

The Turkish translation of the UNIDROIT Principles on Digital Assets and Private Law has been prepared by Professor Dr. K. Berk KAPANCI (MEF University Faculty of Law). All rights reserved.

DİJİTAL VARLIKLAR VE ÖZEL HUKUKA İLİŞKİN UNIDROIT İLKELERİ

Translation into the Turkish language of the official version of the UNIDROIT Principles on Digital Assets and Private Law published by UNIDROIT. The translator gratefully acknowledges permission to translate given by UNIDROIT; Turkish not being an official language of UNIDROIT, UNIDROIT has not reviewed this translation.

UNIDROIT – Via Panisperna, 28 – 00184 Rome (Italy) – www.unidroit.org – publications@unidroit.org

GİRİŞ

I. İLKELERİN OLUŞTURULMA GEREKÇELERİ

- 0.1. Bu İlkeler, İlke 2(2)'de tanımlanan türdeki dijital varlıklarla ilgili işlemleri kolaylaştırmak amacıyla tasarlanmıştır. Bunlar, ticarete sıklıkla kullanılan dijital varlık türleridir.
- 0.2. Bu tür dijital varlıklarla gerçekleştirilen işlemlerin azami verimliliğe ulaşabilmesi için, bu işlemlerin temel unsurlarına uygulanacak açık kuralların bulunması önemlidir (bkz. Açıklama 0.13–0.19). Öngörülebilir sonuçlar olmadan, bu işlemler doğaları gereği verimsizlik gösterecek, maliyetler artacak ve ticari alanda yapılan işlemlerin değeri azalacaktır.
- 0.3. Bu İlkeler, kapsadıkları işlemlerde taraf olan kişilere, bunların danışmanlarına (avukatlar dâhil) ve bu işlemlerin hukuki sonuçlarını değerlendirecek mahkemeler ile diğer kişilere rehberlik sağlamayı amaçlamaktadır. Özetle, bu İlkeler, dijital varlıklarla ilgili olarak uygulayıcıların, yargıçların, hakemlerin, kanun koyucuların ve piyasa katılımcılarının önümüzdeki yıllarda karşı karşıya kalabilecekleri hukuki belirsizlikleri azaltmayı hedeflemektedir.
- 0.4. Devletlerin, bu İlkelere uygun mevzuat kabul etmeleri tavsiye edilmektedir. Bunun çeşitli yararları olacaktır. Bu varlıkları içeren işlemlerin, bu tür işlemlerin gerçekleştiği devletlerde öngörülebilirliği artacaktır. Ayrıca, bu işlemler sıklıkla farklı devletlerdeki kişiler arasında yapıldığından, devletler arasındaki uyum ne kadar büyük olursa, sınır ötesi işlemlerde öngörülebilirlik de o kadar artacaktır. Bu artan öngörülebilirlik hem doğrudan işlem maliyetlerini hem de fiyatlandırmayı kapsayacak şekilde ilgili işlemlerin maliyetlerini azaltacaktır.

II. TARAFSIZLIK VE İLKELERİN ULUSAL HUKUKLA İLİŞKİSİ

- 0.5.** Bu İlkeler, pratik ve işlevsel bir yaklaşım tarzını benimsemektedir. Bunun birkaç önemli sonucu vardır. İlk olarak, bu İlkeler teknolojiye ve iş modellerine karşı tarafsızdır. Yorumlarda yer yer bu İlkelere açıklık getirmek amacıyla blokzincir gibi dağıtık defter teknolojilerine atıf yapılmış ve örnekler verilmiştir. Ancak bu yalnızca İlkelerin uygulanmasını açıklığa kavuşturmak içindir; bu tür teknolojileri kullanan varlıklara öncelik vermek veya başka teknolojileri kullanan dijital varlıklara uygulanabilirliğini değiştirmek ya da zayıflatmak amacı taşımamaktadır. Önemle ifade edilmelidir ki, bu durum İlkelerin teknolojik tarafsızlığını etkilememektedir. Dolayısıyla bu İlkeler, kaydı blokzincir üzerinde tutulsun veya tutulmasın, İlke 2(2)’de tanımlanan tüm dijital varlıklara uygulanacak şekilde tasarlanmıştır. Bu İlkelerin kapsamı ve özellikle temel olarak hedef aldıkları dijital varlık türleri hakkında bkz. Yorum 0.11 ve 0.12 ile İlke 1.
- 0.6.** İkinci olarak, bu İlkeler hukuk sistemi açısından tarafsızdır. Bu nedenle, belirli bir ülkenin terimleri veya hukuk sistemi temel alınarak kaleme alınmamış olup, herhangi bir hukuk sistemi ve kültürü dahilinde uygulanabilir şekilde hazırlanmıştır. Böylece bu İlkeler, Anglo-amerikan hukuku (*common law*) ve Kıta Avrupası hukuku (*civil law*) sistemleri de dâhil olmak üzere tüm hukuk sistemlerinde dijital varlıkların hukuki olarak ele alınmasını kolaylaştırmayı amaçlamaktadır. Örneğin bu İlkelerde kullanılan “kontrol” kavramı, bazı Anglo-amerikan hukuku ülkelerinde kullanılan “kontrol” kavramı ile özdeş anlaşılmamalıdır. Benzer şekilde, Kıta Avrupası hukuk sistemlerinde kullanılan “zilyetlik” kavramına benzemekle birlikte, bu İlkelerdeki “kontrol” kavramı zilyetlik ile de birebir aynı değildir: Kıta Avrupası hukuk sistemlerinde bir kişi bir malı başkası aracılığıyla elinde tutabilirken, bu İlkelere göre bir dijital varlığın, İlke 6 veya temsil hukuku uyarınca öngörülen şartlar karşılanmadıkça (bkz. Açıklama 6.6), başka bir kişi aracılığıyla kontrol edilmesi mümkün değildir.
- 0.7.** Yukarıda açıklandığı üzere bu İlkelerin hukuk sistemi açısından tarafsız olması, bu İlkelerin bir ülkenin hukuk sistemine nasıl dâhil edileceğinin o ülkenin tercihinine bırakıldığı anlamına da gelir. Geleneksel olarak, Anglo-amerikan ve Kıta Avrupası hukuk sistemleri yeni olguların ele alınmasında ve uluslar üstü kuralların benimsenmesinde farklı yaklaşımlar ortaya koyabilirler; bu İlkeler belirli bir yöntemi zorunlu tutmamaktadır. Örneğin, bir hukuk sistemi bu İlkelerin tamamını içeren özel bir yasa

kabul etmeyi seçebilir. Alternatif olarak, başka bir hukuk sistemi bu İlkeleri mevcut olan hukuk düzenlemelerine entegre ederek uygun gördüğü şekilde değiştirebilir. Bu İlkeler, kurallarının bir devletin yalnızca dijital varlıkları konu alan özel yasalarında mı yer alacakları, var olan özel hukuk düzenlemelerine mi dâhil edilecekleri, ya da konunun bu ikisinin karması bir yaklaşım tarzıyla mı ele alınacağı hususlarında herhangi bir tutum belirlemez.

0.8. Üçüncü olarak, bu İlkeler düzenleme tarzı ve yeri anlamında tarafsızdır. Yani, yukarıda ifade edildiği gibi, bir devletin mevzuatının hangi bölümünde yer alacağı konusunda bir tavır ortaya koymaz. Bir devlet bu İlkeleri dijital varlıklara yönelik özel bir yasaya dâhil edebilir, ya da bunların genel olarak özel hukuk, ticaret hukuku veya tüketici hukuku düzenlemeleri çerçevesinde ele almayı göz önünde bulundurabilir. Ancak, İlkelerin düzenleme tarzı ve yeri anlamında tarafsızlığı, bunların kapsam olarak İlkelerde tanımlanandan daha dar şekilde uygulanabileceği anlamına gelmez. Örneğin, bir hukuk sistemi ticaret hukukunun yalnızca girişimcilere/şirketlere uygulanacağını takdir ediyorsa, bu İlkeler yalnızca ticaret hukuku düzenlemeleri altında yer vermemelidir; zira İlkeler tüketicileri kapsam dışı tutmamaktadır. Benzer şekilde, İlkeler sadece tüketici hukuku altında yer vermek de uygun değildir, çünkü bunların kapsamı yalnızca tüketicilerle sınırlı değildir.

0.9. Bu İlkelerin düzenleme tarzı ve yeri bakımından tarafsızlığı, bunların özel hukuk alanı dışında ele alınabilecekleri anlamına da gelmez. Bu İlkeler yalnızca dijital varlıklarla ilgili özel hukuk konularını ve özellikle bunlar üzerinde söz konusu olacak malvarlıksal mutlak hakları kapsar. Dolayısıyla dijital varlıklar üzerindeki tasarruflar, bunların kazanılması ve yine bunlar üzerinde söz konusu olan hakların üçüncü kişilere karşı ileri sürülmesi gibi hususlara odaklanır. Esas itibarıyla, bu İlkeler kamu kurumları tarafından tatbik edilecek, çoğu hukuk sisteminde “düzenleyici kurallar (regülasyon)” olarak adlandırılan kuralları kapsamaz. Örneğin bu İlkeler, dijital varlıkları ilgilendiren faaliyetlerde bulunan bir kişinin faaliyet izni alıp almayacağına dair konulara ilişkin kurallar getirmez. Ancak, hukuk sistemleri, bu İlkeleri tamamlayacak ve bunlarla birlikte uygulama alanı bulacak kamu kurumları aracılığıyla tatbik edilen düzenleyici kuralları benimsemek isteyebilirler. Örneğin, devletler, dijital bir varlığı işlem hayatına sokan kişinin, bu dijital bir varlığın başka bir varlıkla bağlantılı olduğunu (eğer böyle bir durum söz konusu ise) açıklama yükümlülüğünü konu alan kuralları benimseyebilirler (bkz. İlke

4 ve Açıklaması). Bu türden kurallara uyulmadığında, denetleyici konumundaki ilgili kamu kurumu tarafından belirli bir para cezasına hükmedilebilir veya ilgili kişinin faaliyet izni iptal edilebilir. Yine, dijital varlık saklayanların muhafaza ettikleri müşteri dijital varlıklarını kendi dijital varlıklarından ayırma zorunluluğu öngören düzenleyici kurallar da söz konusu olabilir. Bu kurallar, hem saklayanın müşteri varlıklarını nasıl yönetmesi gerektiğine ilişkin usulleri hem de saklayanın iflas sürecine girmesi durumunda, müşterilerin dijital varlıklarının kendi malvarlığına dahil edilerek alacaklılarına dağıtılmasını engellemek amacıyla izlenmesi gereken hukuki yöntemi kapsayabilir. Bkz. İlke 11(3)(d) (özel hukuk yükümlülüğü bakımından), Açıklama 11.8 ve İlke 13(2). Saklayan bu türden kuralları ihlal ederse, denetleyici konumundaki kamu kurumu bu ihlali para cezası uygulayarak veya saklayanın faaliyet iznini iptal ederek yaptırıma tabi tutabilir.

0.10. Ayrıca, bu İlkeler yalnızca özel hukukun belirli bir alanını kapsamayı amaçlamakta olup, bu İlkeler tarafından ele alınmayan birçok özel hukuk konusu mevcut bulunmaktadır. Bunlara örnek olarak, fikrî haklara veya tüketicinin korunmasına ilişkin özel hukuk kurallarını ilgilendiren konular gösterilebilir. Esas itibariyle, ilgili hukuk alanları bu İlkelerin kapsamına dahil edilmemiştir ve dolayısıyla fikrî haklara ve tüketicinin korunmasına ilişkin ulusal düzenlemeler de bu İlkelerden etkilenmemektedir. Yine, bu İlkeler, ulusal özel hukukların sözleşmeler hukuku ve eşya hukuku kısımlarına ilişkin birçok konuyu da kapsamlarına almamaktadır. Bu İlkeler tarafından ele alınmayan konulara örnek olarak şunlar gösterilebilir: Dijital bir varlık üzerindeki malvarlıksal mutlak bir hakkın bir başka kişiye geçerli olarak devredilip devredilmediği, dijital bir varlık üzerinde geçerli bir teminat hakkının kurulup kurulmadığı, dijital bir varlığı devreden ile devralan arasındaki haklar, dijital bir varlık üzerinde teminat hakkı kuran ile bu teminatın lehtarları arasındaki haklar, dijital varlıkların devrinin üçüncü kişiler nezdinde hüküm ifade etmesinin şartları ve hukuki sonuçları, dijital bir varlık üzerindeki teminat hakkının üçüncü kişiler nezdinde hüküm ifade etmesinin şartları ve hukuki sonuçları (bkz. ayrıca İlke 3(3) ve İlke 4). Özetle, bu İlkeler salt olarak belirli temel kavram ve kuralları tesis etmekte olup (bkz. Açıklama 0.13 – 0.19), İlkeler kapsamında ele alınan dijital varlık türlerine ilişkin tüm sözleşmeler hukuku ve eşya hukuku problemlerine çözüm getirme amacını taşımamaktadır. Zira devletlerin geniş kapsamlı farklı hukuk kuralları bulunabileceğinden (yasalar ve yargı kararlarıyla oluşturulan), İlkeler dahilinde,

uygulanabilecek spesifik hukuk düzenlemelerinin belirlenmesine yönelik bir girişim de mevcut değildir.

III. İLKELERİN KAPSAMI

0.11. Bu İlkeler yalnızca belirli bir dijital varlık alt kümesine uygulanır. Bunlar, İlke 2(2)’de belirtildiği şekilde, “kontrol” altına alınabilen dijital varlıklar olarak tanımlanarak diğer dijital varlıklardan ayrılır (bkz. Açıklama 0.15 altında kısaca belirtildiği üzere). Bu İlkeler bakımından bir kişinin şu özellikleri haiz olduğunu ortaya koyabildiği durumlarda “kontrol”den söz açılabilir: (i) Başkalarının dijital varlıktan esaslı ölçüde tüm faydayı sağlamalarını engelleyebilmek bakımından münhasır yetkiye sahip olunması, (ii) dijital varlıktan esaslı ölçüde tüm faydayı elde edebilme yetkisine sahip olunması ve (iii) dijital varlık üzerindeki kontrolü başka bir kişiye devretmek bakımından münhasır yetkiye sahip olunması. Bkz. İlke 6.

0.12. Bazı durumlarda, bu İlkelerin kapsamına giren bir dijital varlığın başka bir varlıkla “bağlantılı” olduğu belirtilebilir. Açıklama 0.10’da da ele alındığı üzere, ulusal hukukla olan ilişki dahilinde, ilgili bağlantının sözleşmeler hukuku ve eşya hukuku açısından etkileri (eğer varsa) bu İlkeler dışında kalan hukuk tarafından belirlenecektir. Bkz. İlke 4.

IV. TEMEL KAVRAMLAR VE KURALLAR

Eşya hukuku boyutuyla ilgili hususlar

0.13. Bu İlkeler, dijital varlıkların (Bkz. İlke 2(2)’deki tanım) malvarlıksal mutlak haklara konu oluşturabileceğini kabul eder, ancak bunların bir devletin diğer hukuk düzenine göre “eşya” sayılıp sayılmadığını düzenlemez. Bkz. İlke 1 ve İlke 3(1). Dijital varlıklar malvarlıksal mutlak hakların konusunu oluşturabildikleri üzere, bu varlıkların kendilerine özgü özellikleri de dikkate alınarak, dijital varlıklara ilişkin masum hak kazanımlarının korunmasını sağlayan ve dijital varlıklar üzerinde teminat haklarının oluşturulmasına imkân tanıyan özel mahiyette kurallar öngörmek yerinde olur (bkz. İlke 8 ve İlke 14).

Milletlerarası özel hukuk

0.14. Dijital varlıkların gayri maddi özellik taşımaları ve birçok işlemin herhangi bir fiziksel yerle bir bağlantı bulunmaksızın gerçekleşmesi hususları düşünüldüğünde ve yine uygulanacak hukukun belirlenmesindeki kesinlik gerekliliği de dikkate alındığında, maddi özellik taşıyan malvarlığı değerleri için geçerli olan klasik bağlama noktalarının dijital varlıklar özelinde kullanılmaya elverişli olmadıkları belirgin biçimde görülmektedir. Bu nedenle İlkeler, tarafların uygulanacak hukuku seçme özgürlüğüne geniş ölçüde yer vermekte ve dijital varlığın kendisi ya da kaydedildiği sistem bakımından söz konusu olabilecek eşya hukuku konularını düzenleme altına alacak hukukun taraflarca belirlenmesine açıkça imkân tanımaktadır. Ayrıca, İlkeler dahilinde, belirli durumlar özelinde başka bazı bağlama noktalarına da yer verilmektedir. Bu noktalar arasında, eğer dijital varlığın bir “ihraççısı” bulunuyorsa (bkz. İlke 5(2)(f)’deki tanım), bu ihraççının kanuni merkezinin bulunduğu yer sayılabilir. İlke 10 ve 13 arasında ele alınan saklama sözleşmesini ilgilendiren konularda ise, ilgili sözleşmede tabi olunacağı belirtilen hukuk uygulama alanı bulacaktır. Bkz. İlke 5.

Kontrol

0.15. Bu İlkeler, bir dijital varlık üzerinde kontrol kurulabilmesi için sahip olunması gereken birtakım fiili yetilerden (özelliklerden) oluşan bir “kontrol” kavramı geliştirmiştir (bkz. Açıklama 0.11). Kontrol kavramı, özellikle masum kazanıma ilişkin kural, üçüncü kişilere karşı ileri sürülebilirlik ve saklama sözleşmesinin tanımı bakımından bu İlkeler dahilindeki kurallar bakımından kritik bir rol oynamaktadır (bkz. İlke 6 ve 7 ile İlke 10).

Devir ve teminat işlemleri

0.16. Bu İlkeler, ticaret hayatındaki en önemli işlemleri kapsar — dijital varlık üzerindeki malvarlıksal mutlak hakkın devri ve dijital varlık üzerinde teminat hakkı tesis edilmesi (bkz. İlke 2(5)). Bu İlkeler, dijital varlıkların ticaret hayatında “gerçek zamanlı” işlemlere konu oluşturduklarını ortaya koyan bazı özel kurallar getirmektedir (devir ve teminat haklarına ilişkin başkaca hususlar ise diğer hukuka bırakılmıştır, bkz. Açıklama 0.10, 1.2 ve 1.3). Bu İlkeler uyarınca, dijital bir varlık üzerindeki kontrolü elde ederek ve belirli ek şartları sağlayarak masum bir kazanımda bulunan, bu varlığı üzerindeki diğer hak

iddialarından arınmış olarak kazanır. Masum kazanımda bulunanın hakları, sonraki devralanlara da, ilgili devralan masum kazanımda bulunan olarak nitelendirilsin veya nitelendirilemesin, bu konuda benimsenen bir “koruma” kuralı kapsamında aynı şekilde intikal eder. Teminatlı alacaklı, dijital varlık üzerindeki kontrolü elde ederek, oluşturulan teminat hakkını üçüncü kişilere karşı da ileri sürebilir. Ayrıca, bir dijital varlık üzerinde kontrolü elde etmiş olan teminatlı alacaklı, aynı varlık bağlamındaki diğer teminatlı alacaklılara göre öncelik hakkına sahip olur. Bu diğer teminatlı alacaklılar, teminat haklarını belirli bir sicile tescil yoluyla üçüncü kişilere karşı ileri sürebilir hale gelenleri de kapsar. Söz konusu haklar, sonraki devralanlara da, ilgili devralan masum kazanımda bulunan bir kişi olarak nitelendirilebilsin veya nitelendirilemesin, yine bu konuda benimsenen bir koruma kuralı kapsamında aynı şekilde intikal eder. “Kontrol” ün tanımı, hem masum kazanımda bulunanın haklarının ele alınması hem de dijital varlık üzerinde kurulan teminat hakkının üçüncü kişilere karşı ileri sürülebilirliğinin temini için özenli biçimde tasarlanmıştır (bkz. İlke 8–9 ve İlke 14–17, Bölüm V: Teminat işlemleri).

Saklayanlar

0.17. Bu İlkelerde ele alınan dijital varlıklar çoğu zaman saklayanlar tarafından muhafaza edilecektir. İlkeler, bir kişinin hangi durumlarda saklayan olarak hareket ettiğini açıkça ortaya koymakta ve saklayanın iflas etmesi halinde, onun müşterileri için muhafaza ettiği dijital varlıkların kendi malvarlığına dâhil edilemeyeceğini düzenlemektedir. İlkeler ayrıca, saklayanların bu varlıklarla ilgili görev ve yetkilerini de konu alır. Eğer bir alt saklayan, bir saklayan adına dijital varlığı muhafaza ediyorsa, İlkeler bu ilişkiyi de saklayan–müşteri ilişkisini düzenleyen kurallara benzer şekilde ele almaktadır (bkz. İlke 10–13, Bölüm IV: Saklama).

Usul hukuku

0.18. Bu İlkeler, usul hukukuna ilişkin konular da dâhil olmak üzere, dijital varlıklarla ilgili hakların icrası gibi konularda esas itibarıyla diğer hukukun uygulama alanı bulacağını öngörmektedir (bkz. İlke 18).

İflasın etkisi

0.19. Bu İlkeler, üçüncü kişilere karşı ileri sürülebilir nitelikteki malvarlıksal mutlak hakların genel olarak iflas idaresine karşı da ileri sürülebileceğini düzenlemektedir (bkz. İlke 19).

V. GEÇİŞ HÜKÜMLERİ

0.20. Eğer bir devlet bu İlkeleri bir yasama faaliyetiyle yürürlüğe koyarsa, İlkelere ilişkin düzenlemeler genel bir kural olarak ileriye etkili biçimde uygulama alanı bulacaktır. Bu sayede önceden hayata geçirilmiş (mevcut) işlemler ve hukuki ilişkiler korunmuş olur. Ne var ki, bazı durumlarda da İlkelerin bir kısmı ancak belirli bir “geçiş süresi” sonrasında mevcut işlemler için de uygulanabilir hale gelebilecektir. Örneğin, teminatlı bir alacaklı, geçiş süresinin devreye girmesinden önce belirli bir dijital varlık üzerindeki teminat hakkını tescil yoluyla üçüncü kişilere karşı ileri sürebilir hale getirmiş, ancak akabinde bu hakkını kontrol yoluyla da üçüncü kişilere karşı ileri sürülebilir hale getirmek için gerekli diğer adımları atmamış olursa (bkz. İlke 15), geçiş süresinin tamamlanmasını takiben aynı dijital varlık üzerinde sonradan kontrolü elde etmek yoluyla hak kazanmış bulunan bir başka teminatlı alacaklıya karşı önceliğini kaybedebilir.

BÖLÜM I: KAPSAM VE TANIMLAR

İlke 1

Kapsam

Bu İlkeler, dijital varlıklarla ilgili özel hukuk kurallarını konu alır.

Açıklama

1.1. Bu İlkeler, devletlerin özel hukuklarını, dijital varlıkların elde tutulması, devri ve teminat olarak kullanılması bakımından en iyi uygulamalar ve uluslararası standartlarla uyumlu hale getirmeleri için, İlke 2(2) belirtildiği üzere, kılavuz kurallar olarak tasarlanmıştır. İlkeler, yalnızca dijital varlıklara ilişkin özel hukuk sorunlarını, özel olarak da malvarlıksal mutlak hakları kapsamına alır. Bu nedenle, İlkeler dahilinde dijital varlıkların el değiştirmesi, kazanılması veya bu varlıklar üzerindeki hakların üçüncü kişilere karşı ileri sürülebilmesi gibi konulara odaklanılır. Esas itibariyle İlkeler, kamu kurumları tarafından tatbik edilecek düzenleyici mahiyetteki (pek çok hukuk sistemi dahilinde “regülasyon” olarak adlandırılan) hukuk kurallarını kapsamazlar. Örneğin, bir kişinin dijital varlıklarla ilgili faaliyetlerde bulunabilmek için faaliyet izni alıp almayacağı gibi konular bu İlkelerin kapsamına girmemektedir. Aynı şekilde bu İlkeler, kişilerin dijital varlıkları nasıl elde tutmaları gerektiğine ilişkin, öngördükleri yükümlülöklere uyumun kamu kurumlarınca zorunlu kılındığı kuralları da kapsamaz.

1.2. Ayrıca bu İlkeler, özel hukukun yalnızca belirli bir alanıyla ilgilenir; fikri haklar veya tüketicinin korunması gibi özel hukuka ilişkin birçok konuya değinmez. Bu alanlarda ulusal hukuk kuralları bu İlkelerden etkilenmeksizin geçerliliklerini sürdürür. Ayrıca bu İlkeler, sözleşme ve eşya hukukuna ilişkin tüm özel hukuk kurallarını düzenlemez; bunun gerekçesi Açıklama 1.3’te belirtilmiştir. Örneğin, bir dijital varlık üzerindeki malvarlıksal mutlak hakkın geçerli şekilde devredilip devredilmediğı, bir dijital varlık üzerinde geçerli bir teminat hakkı kurulup kurulmadığı, devreden ve devralan arasındaki haklar, teminat veren ve teminatlı alacaklı arasındaki haklar, gerçekleştirilen dijital varlık devrinin üçüncü kişilere karşı ileri sürülebilir olmasının sonuçları ve yine dijital varlık üzerinde kurulan teminat hakkının üçüncü kişilere karşı ileri sürülebilir olmasının koşulları ve sonuçları

gibi konular, bu İlkelerin uygulama kapsamı dışındadır. Bu konuda ayrıca bkz. İlke 3 (3) ve İlke 4.

1.3. Bu İlkeler, mevcut (özel) hukukta boşlukların bulunduğu veya geleneksel yaklaşımların yetersiz kaldığı ve değiştirilmesinin gerekli olduğu durumlara çözüm getirmeyi amaçlar. Ancak İlkeler, uygulanabilirliği ve işlevselliği ön planda tutan bir yaklaşım benimsediği için, dijital varlıkların her türlü teknoloji ve hukuk sisteminde özel hukuk kapsamında ele alınmasını kolaylaştırmayı hedefler. Bu şekilde, İlkelerin bu uluslararası mahiyeti sayesinde, farklı hukuk sistemleri tarafından dijital varlıkların elde tutulması, devri ve teminat olarak kullanılmasıyla ilgili birçok hukuki sorun bağlamında ortak bir yaklaşımın geliştirilmesi sağlanabilir. Bu İlkelerin teknoloji, hukuk sistemi, düzenleme yeri ve tarzı bakımından tarafsızlığı hakkında ayrıntılar için bkz. Açıklama 0.5-0.9.

İlke 2

Tanımlar

- (1) “Elektronik kayıt”, elektronik ortamda saklanan ve erişilebilir nitelikteki bilgiyi ifade eder.
- (2) “Dijital varlık”, üzerinde kontrol tesis edilebilen bir elektronik kayıttır.
- (3) “İlkeler hukuku”, bir devletin bu İlkeleri benimsemiş veya onlarla uyumlu olan hukuk kurallarını ifade eder.
- (4) “Diğer hukuk”, bir devletin İlkeler hukukunun dışında kalan hukukunu ifade eder.
- (5) Dijital varlıkların devri ile ilgili olarak:
 - (a) bir dijital varlığın “devri”, ilgili dijital varlık üzerindeki malvarlıksal mutlak hakkın bir kişiden diğerine geçirilmesini ifade eder,
 - (b) “devir” terimi, devreden tarafından türeme yoluyla ortaya çıkan bir dijital varlığın kazanılmasını da kapsar,
 - (c) “devreden”, devri gerçekleştiren kişi; “devralan” ise malvarlıksal mutlak hakkın geçtiği kişiyi ifade eder,
 - (d) “devir” terimi, bir teminatlı alacaklı lehine teminat hakkı tesis edilmesini de kapsar; bu durumda “devralan” terimi de teminatlı alacaklı karşılık gelir.
- (6) “İflasla ilgili süreç”, borçlunun malvarlığı değerleri (varlıkları) veya ilişkileri üzerinde yeniden yapılandırma veya tasfiye amacıyla başlatılan ve aşağıdakilerden en az birini içeren toplu yargısal veya idari işlemleri ifade eder:
 - (a) bunların bir mahkeme veya yetkili otoritenin kontrolü altında olması,
 - (b) borçlunun bunları yönetme veya bunlar üzerinde tasarruf etme kabiliyetinin hukuken sınırlandırılması,
 - (c) borçlunun alacaklılarının bunları ilgilendiren cebri icra süreçlerine başvurma kabiliyetlerinin hukuken sınırlandırılması.
- (7) Aşağıdaki terimlerin anlamı, İlkeler altındaki başkaca yerlerde belirlenmiştir:
 - (a) “ihraççı” (İlke 5(2)(f), İlke 5(1)(c) bağlamında),
 - (b) “kontrol” (İlke 6),
 - (c) “kontrol değişikliği” (İlke 6(2)),

- (d) “türeme yoluyla ortaya çıkan dijital varlık” (İlke 6(2)),
- (e) “malvarlıksal mutlak hakka dayalı talepler” (İlke 8(2)),
- (f) “saklayan”, “alt-saklayan” ve “müşteri” (İlke 10(1)),
- (g) “muhafaza etme” (İlke 10(2)),
- (h) “saklama sözleşmesi” (İlke 10(3) ve 10(4)),
- (i) “noksanlık” (İlke 13(5)).

(8) Tekil hallerinde kullanılan kelimeler bunların çoğul hallerini, çoğul hallerinde kullanılan kelimeler ise bunların tekil hallerini de kapsar.

Açıklama

Elektronik kayıt

2.1. “Elektronik kayıt”, dijital varlıkların bir alt kümesini oluşturduğu (İlke 2(2)’de tanımlandığı üzere) daha geniş bir varlık sınıfını kapsamına alır. Tanımlandığı üzere, elektronik kayıt; elektronik ortamda saklanan ve erişilebilir nitelikteki bilgiye karşılık gelir. “Elektronik ortam”, geniş anlamda anlaşılmalıdır. Yani ilgili tanım manyetik alan kullanan sabit diskler veya malzeme üzerinde fiziksel değişiklikler meydana getiren DVD’ler gibi, doğrudan elektron akışına dayanmayan diğer her türlü dijital teknolojiyi de kapsar. Bilginin erişilebilir olması, bu bilginin aynı zamanda insan tarafından algılanabilir bir biçimde erişilebilir olması gerektiğini de kasteder. Diğer taraftan, kayıt altına alınmayan sözlü iletişim veya yalnızca insan belleğinde tutulan bilgi, bu tanım kapsamında değerlendirmeye alınmaz.

2.2. Bu tanım, pek çok ulusal hukuk düzeninde yer alan ve “bilgi”ye karşılık gelen “elektronik kayıt” tanımıyla uyumludur. Aslında “elektronik kaydın”, “bilgi kaydı” olarak değil de “bilgi” olarak ifade edilmesi (bilginin bir yerde kayıtlı ve erişilebilir olması zımni gerekliliği bir kenara bırakılacak olursa) tuhaf görülebilir. Belki belirli bir kaydın sıfırdan oluşturulması söz konusu olsa idi, “bilgi kaydı” ifadesinin kullanımı anlamlı olabilirdi. Ancak, bu ifade, sadece dijital varlığın tanımlanmasında bir unsur (bileşen) olarak bir yere sahiptir. Açıklama 2.3 ve 2.17’de de belirtildiği üzere, ilgili tanımda asıl belirleyici faktör “elektronik kaydın” “üzerinde kontrol tesis edilebilen” özellikte olmasıdır. Bu çerçevede, “elektronik kayıt” tanımı hangi formül üzerinden verilirse verilsin, aynı sonuca ulaşılmış olacaktır. Dolayısıyla, üzerinde genel bir kabulün bulunduğu tanımlama tercih edilmiştir.

Dijital Varlık

2.3. “Dijital varlık” tanımı, yalnızca üzerinde -İlke 6’da tanımlandığı biçimde- “kontrol” kurulabilecek bir elektronik kaydı kapsamına alır. Örneğin, günlük konuşma dilinde “dijital varlık” tasvir edilebilecek bazı elektronik kayıtlar, bu İlkelere tanımlandığı anlamda kontrol altına alınamaz ve dolayısıyla buradaki anlayış çerçevesinde dijital varlık sayılmaz. Bu konuda ayrıntılı açıklamalar için İlke 6 altındaki açıklamalara göndermede bulunulmalıdır. Çok kısa ifade edilecek olursa, orada ayrıntılı şekilde açıklanan “kontrol”, esasen (ilgili tanımda geçen istisna durumlar saklı kalmak üzere) münhasır kontrole karşılık gelir.

2.4. Basitleştirilmiş bir örnek üzerinden ele alınacak olursa: Üçlü bir bilgi setinden oluşan bir elektronik kayıt düşünölsün. Birinci set “Bilgi Alpha”, ikinci set ise genel anahtar/özel anahtar sisteminde bu bilgiyi kontrol edilebilir kılan “anahtar bilgisi” olsun. Burada anahtar bilgisi doğrudan özel anahtarı içermeyebilir, ama özel anahtar vasıtasıyla kontrol edilebilecek nitelikteki bilgiyi barındırır. Bu iki bilgi seti birlikte “Dijital Varlık Alpha”yı oluşturur. Üçüncü bilgi seti ise “Bilgi Beta” olsun. Bilgi Beta da aynı elektronik kayıta yer alabilir, ancak Dijital Varlık Alpha’nın kontrolünün devri, Bilgi Beta üzerinde bir kontrol devrini sağlamaz. Burada Bilgi Beta kontrol altına alınabilir nitelikte olmadığı varsayılmaktadır. İlgili durum gerçekçi olmaktan uzak değildir. Örnek olarak bir kişinin elinde tuttuğu Bitcoin, harcanmamış işlem çıktısından (*unspent transaction output* - UTXO) oluştuğunda benzer bir durumla karşılaşılır. UTXO, aynı elektronik kaydın parçası olan, örnek olarak bir başlığa dahil edilmiş bilgiler gibi, kontrol edilebilir nitelikte olmayan bilgilerle ilişkilendirilebilir. UTXO’nun harcanması, bu başlık altındaki bilgilerin mutlaka devredilmesi sonucunu doğurmaz. Bir dijital varlıkta yer alan bilgiler ile, Bilgi Beta veya başka malvarlığı değeri (varlık) gibi dijital varlıkla ilişkilendirilmiş bilgiler birbirlerinden ayırt edilmelidir. İlke 4, bu türden, altın ve menkul kıymetler gibi, dijital varlıkla bağlantılı varlıklara değinmektedir. Bu konuda bkz. Açıklama 4.13-4.15 ve 4.21 altındaki tartışmalar.

2.5. Yine bu Açıklama 2.4 altında verilen Dijital Varlık Alpha örneğinden hareketle, İlke 8 uyarınca Dijital Varlık Alpha’yı iyi niyetle edinen bir kişinin (X), bu varlığı çatışan hak iddialarından ari şekilde kazandığı düşünölsün. Bu durum, X’in Bilgi Alpha’yı kazandığı

(örnek olarak X'in Bilgi Alpha üzerinde, uygulanacak hukuk buna izin verse bile, bağımsız bir hakkı kazandığı) anlamına gelmez. X yalnızca Dijital Varlık Alpha içinde anahtar bilgisiyle ilişkilendirilen ölçüde Bilgi Alpha'yı elde etmiş olur. Bilgi Alpha, Dijital Varlık Alpha'nın bir parçası olduğu kadar, ondan ayrı ve bağımsız şekilde de varlığını sürdürebilir. Bilgi Alpha, Bilgi Alpha'dır, yani Bilgi Alpha ne şekilde veya nerede kaydediliyor, var oluyor veya algılanıyor olursa olsun aynı özellikte kalmaya devam eder. Buna karşılık, Dijital Varlık Alpha ondan farklıdır, ne de olsa ortada sadece Bilgi Alpha'dan değil aynı zamanda anahtar bilgisinden de oluşan bir dijital varlık söz konusudur.

2.6. Bilgi Alpha bir görüntü, şiir, kitap, video, şarkı, veri tabanı içeriklerinden veya özel bir değeri bulunmayan "1" ve "0" kombinasyonlarından oluşabilir. İçeriği neden ibaret olursa olsun, İlkeler hukuku bakımından ("İlkeler hukuku"na verilen anlam için bkz. İlke 2(3)), bilgi diğer hukuka tabi olacaktır. Örnek olarak Bilgi Alpha, geçerli bir telif hakkı korumasına tabi olsaydı, telif hakkı sahibinin hakları, Dijital Varlık Alpha'nın oluşturulması, kazanılması veya devredilmesinden özel olarak etkilenmezdi. Diğer taraftan, Bilgi Alpha'nın Dijital Varlık Alpha'ya dahil edilmesi ya da Dijital Varlık Alpha'nın kullanımı, devri veya kazanımı anılan kanunlar kapsamındaki hakları ihlal edebilir veya bunlara doğrudan bir tecavüz oluşturabilir. Bilgi Alpha (veya bir dijital varlığa dahil edilen diğer herhangi bir bilgi) fikri haklar veya diğer kanunlar kapsamında herhangi bir korumaya tabi olmasa da, söz konusu bilginin Dijital Varlık Alpha'nın dışında ve ondan ayrı olarak mevcut olması, kullanılması veya ilgili bilgi üzerindeki haklar, İlkeler hukukundan etkilenmez.

2.7. Dijital varlık bünyesindeki Bilgi Alpha, Bilgi Beta gibi söz konusu varlıkla ilişkilendirebilir bilgilerden de ayırt edilmelidir. Aşağıda İlke 1 (kapsam), İlke 2(1) ("elektronik kayıt" tanımı) ve İlke 2(2) ("dijital varlık" tanımı) çerçevesinde işaret edilen örnek durumlar, dijital varlığın tanımının uygulamasına ve bu İlkelerin kapsamına ilişkin ek örnekler sunar.

2.8. Örnek Durum 1: Bir açık blokzincirdeki (kripto) misli varlık değeri -örnek olarak bitcoin- bir dijital varlıktır. Açık bir blokzincir yapısı dahilinde, bu yapıya temel teşkil eden protokolü (yazılımı) hiç kimse tek başına kontrol edemez. Yazılım dahilinde bulunan ve sistem yapısına tümleşik özellik taşıyan mutabakat mekanizması, kullanıcılar

tarafından gerçekleştirilmek istenen işlemlerin geçerliliğini doğrulamaktadır. Açık blokzincire temel teşkil eden protokolün (sistem) kendisi kontrole (Bkz. İlke 6) elverişli değildir. Bununla birlikte, bireysel kullanıcılar özel anahtarları sayesinde sistem yapısı dahilindeki dijital varlıklar üzerinde kontrol sahibi olabilirler, bu da ilgili kullanıcıya (tanımlandığı şekilde) dijital varlık üzerinde kontrol tesis etme imkânını sağlar (örnek olarak, Bitcoin özelinde UTXO (harcanmamış işlem çıktısı) üzerindeki kontrol düşünülün).

2.9. Her ne kadar diğer açık blokzincirler, uygulama alanı bulan mutabakat mekanizması ve işlem seyri bakımından Bitcoin blokzincirinden farklılık gösterebilir olsa da, yukarıdaki açıklama yine bunlar bakımından da geçerli olacaktır. Bireysel bir kullanıcı tek başına temeldeki protokolü (veritabanı veya blokzincir) kontrol edemez; ancak kendi özel anahtarını kontrol edebilir ve bu sayede ilgili protokol aracılığıyla elde tutulan dijital varlıklar üzerinde (tanımlandığı şekilde) “kontrol” sahibi olabilir. Bir dijital varlığın mevcut olduğu protokolün kendisi, bu İlkeler kapsamında bir dijital varlık olarak değerlendirmeye alınamaz, ancak özel anahtar ile kontrol edilen bir malvarlığı değeri (varlık), bu İlkelerin kapsamında bir dijital varlık olarak kabul edilir.

2.10. Örnek Durum 1’deki analiz, aşağıdaki diğer örnek durumlar için de geçerlidir.

2.11. Örnek Durum 2: Bir CBDC, dijital varlık oluşturabilir. Bir devlet, merkez bankası dijital parası (CBDC) ihraç etmek istediğinde, bunu çeşitli yollarla yapabilir. Olasılıklardan biri, devletin İlke 2(2)’de tanımlanan şekilde bir dijital varlık ihraç etmesidir. Bu durumda, CBDC birimlerinin, İlke 6’da tanımlandığı şekilde kontrol edilebilen bir elektronik kayda karşılık gelmesi mümkündür.

2.12. CBDC’yi ihraç eden egemen devlet (veya parasal birlik) ilgili para mevzuatı, CBDC sahibinin merkez bankası ile arasındaki hukuki ilişkiyi tanımlar. Aynı zamanda CBDC’nin, adı ve nominal değeri üzerinden fiziki para birimine dönüştürülebilir olması da dahil olmak üzere, para birimi olarak hukuki niteliğini belirler. Para hukuku (*lex monetae*), ayrıca CBDC’nin kullanımının herkese açık olup olmayacağını (perakende CBDC) veya yalnızca belirli kurumlarla sınırlı olup olmayacağını (toptan CBDC), ve kendi kullanıcıları arasında yasal ödeme aracı olup olamayacağını, olabiliyorsa da ne ölçüde olacağını tayin eder.

2.13. Bununla birlikte, CBDC'nin tasarım özelliklerine bağlı olarak ve İlke 2(2) çerçevesinde tanımlanan tüm dijital varlıklar bakımından olduğu gibi, bu İlkeler, CBDC ile ilgili malvarlıksal mutlak hakları ilgilendiren sorunlara ve kişiler arasında gerçekleştirilen (bir borcun ifası veya bir teminat hakkının tesisi) devir işlemlerinde uygulanacak özel hukuk kurallarına ışık tutabilir. Dijital varlık şeklinde ihraç edilmiş bir CBDC'ye ilişkin işlemler, fiziki para ile yapılan işlemlerde olduğu gibi masum kazanımların korunmasını da gerekli kılabilir (Bkz. İlke 8 ve Açıklama 8.7).

2.14. Örnek Durum 3: Bir dijital varlık, değerli bir veri kümesi veya veritabanı (örnek olarak bir yapay zekâ sisteminin (artificial intelligence – AI) çalışmasının temelini oluşturan bir veri kümesi düşünölsün), bir görsel veya yazılı bir ifade içeriyorsa, söz konusu bilgi uygulanacak fikri haklar hukukuna tabidir ve dijital varlığın dışında olan bilgi, dijital varlığın bir parçası olarak görölemez. Açıklama 2.6'da tartışıldığı üzere, eğer dijital varlığa dahil edilen bilgi bizzat fikri haklar hukuku kapsamında (bu örnekte telif hakkı) kapsamında koruma altındaysa, elektronik kayda bu bilginin dahil edilmiş olması veya dijital varlığın masum kazanımda bulunana devredilmesi, fikri hak sahibinin haklarını olumsuz şekilde etkilemez. Uygulanacak fikri haklar hukukunun izin verdiği ölçöde, dijital varlığı devralan kişi, bu bilgiden yararlanma ve onu kullanma hakkına sahip olabilir (telif hakkı koruması altındaki bir kitabı hukuka uygun biçimde satın almış olan kişinin durumu düşünölsün). Buna karşılık, eğer bu bilgi veya bilginin işlevselliği patent hukuku dahilinde korunuyorsa, dijital varlığı kazanan kişi ilgili bilgiyi kullanmak suretiyle patent hakkı sahibinin haklarını ihlal edebilir.

2.15. Bu örnek durumda yer verilen olgular, gerçekçi görölmeyebilir veya genel uygulamayı yansıtmayabilir, ancak örnek duruma değinilme amacı, İlkeler hukuku ve dijital varlıklara ilişkin diğer hukukun uygulanacak fikri haklar hukukuna tabi olması gerektiğinin gösterilmesi ve vurgulanmasıdır. Bu aynı zamanda daha geniş bir noktaya da işaret eder: Dijital varlık, bilginin kontrol edilebilir olmasını mümkün kılan bir bilgi paketinden ibarettir. Açıklama 2.4 ve 2.5'te belirtildiği üzere, dijital varlığa dahil edilen ve onun dışında, ondan ayrı ve bağımsız biçimde varlığını sürdüren bilgi, dijital varlığın bir parçasını oluşturmaz.

2.16. Örnek Durum 4: Şifre ile erişilen bir sosyal medya sayfası, dijital varlık teşkil etmez.

Sosyal medya veya sosyal ağ platformları hakkında bir genellemede bulunmak zordur. Bununla birlikte, sosyal medya platformları genellikle kullanıcılarla yapılan lisans sözleşmeleri üzerinden faaliyet gösterir ve bu sözleşmeler, kullanıcılarına ilgili “sayfalar” veya platform üzerine tutulan veriler üzerinde bir hak sahipliği kazanma olanağını vermez. İlgili durum, kullanıcıların günlük konuşma dilinde “kendi” sayfalarından ve “kendilerine ait” bilgilerden söz etmelerine rağmen geçerlidir. Genel olarak bu platformlar kullanıcılara, İlke 6’da tanımlanan “kontrolün” gerektirdiği nitelikte münhasır yetkiler sağlamaz. Dolayısıyla bunların bu İlkeler kapsamında değerlendirmeye alınacak dijital varlıklar olduğu söylenemez.

2.17. Örnek Durum 5: Şifre korumalı bir Excel veya Word dosyası bir dijital varlık olarak

dikkate alınabilecek olsa da, İlkelerin bu varlıklar özelinde esaslı bir işlev veya etkiyi meydana getiremeyebilir. Word, Excel veya benzeri bir veri dosyası, İlke 2(1)’deki tanım dahilinde bir elektronik kayıt oluşturur. Dosya içeriğine erişim bir şifre ile korunuyorsa da, aynı zamanda hem bu şifreyi bilen hem de ilgili dosyanın kayıtlı olduğu sabit diske doğrudan erişimi olan kişi, İlke 6 kapsamındaki kontrolün tesisinde gerekli olan münhasır yetkileri haiz olabilir. Bu durumda ilgili dosya kontrol edilebilir özellik göstereceğinden, İlke 2(2) anlamında bir dijital varlık teşkil eder ve İlkelerin kapsamına girer. Bununla birlikte, eğer bu dijital varlık, üzerinde kazanımda ve tasarrufta bulunulmasını kolaylaştıran bir protokol ile ilişkilendirilmemişse, İlkeler hukuku ilgili varlık özelinde esaslı bir işlev veya etkiyi meydana getirmez. Örneğin, sabit bir diskte saklanan şifre korumalı bir Word dosyasının kontrolünü devretmek için yalnızca dosyanın şifresini değil, aynı zamanda dosyanın kayıtlı olduğu sabit diski de devretmek gerekir. Dosya üzerinde kontrol sahibi olan bir kişi, bunu bir e-posta ekinde başka bir kişiye gönderip şifresini de beraberinde aktarırsa, ilgili durumda bir kontrol değişikliğinden söz açılmaz. Zira e-posta alıcısı tarafından elde edilen dosya, ilk dosyayla tam olarak aynı bilgiyi içerse de, tümüyle yeni bir elektronik kayıt teşkil edecektir. Ayrıca Açıklama 2.6’da ifade edildiği üzere, dosya üzerindeki kontrol uygulanacak fikri haklar hukuku kapsamında mevcut bulunan hakları ortadan kaldırmaz. Sözü edilen durum karşısında, İlkelerin kapsamının aşırı geniş olduğu düşünülebilir. Ancak bu durum normal şartlarda üzerinde tasarruf edilemeyecek dijital varlıklara ilişkin bir örnek oluşturmaktadır. Dolayısıyla, ilgili durumda İlkelerin öngördüğü hukuk rejimden yararlanılabilmesi veya bu rejime ihtiyaç duyulabilmesi olasılığı düşük kalır. Diğer taraftan, dijital varlık tanımını, bu türden varlıkları dışlayacak

biçimde daraltma yönünde bir girişim, İlkelerden yarar sağlama potansiyeli olan varlıkların kapsam dışı kalması riskini de beraberinde getirebilir.

İlkeler hukuku ve diğer hukuk

2.18. İlke 1 uyarınca, bu İlkeler dijital varlıklarla ilgili özel hukuk meselelerini kapsar. Buna göre, dijital varlıkların saklanması, devri ve bunlar üzerinde teminat haklarının tesis edilmesi gibi konularda kurallar getirir. İlke 2(3) uyarınca, bir devletin hukuk sistemine bu İlkeler uyarınca dâhil edilen veya bunlarla uyumlu hale getirilen tüm kurallar “İlkeler hukuku” sayılır. Ayrıca, İlke 5’te düzenlenen milletlerarası özel hukuk kuralları da bir devletin iç hukukuna aktarıldığında İlkeler hukuku kapsamında değerlendirilir. Bu İlkeler, söz konusu kuralların dijital varlıklara ilişkin özel bir kanunla mı, genel kanunlara yapılacak çeşitli ilavelerle mi, yoksa anılan her iki yaklaşımın bir arada tatbik edilmesiyle mi düzenleme altına alınması konusunda bir zorunluluk öngörmez. İlkelerin, teknoloji, hukuk sistemi, düzenleme yeri ve tarzı bakımından tarafsızlıkları özelinde daha geniş bilgi için bkz. Açıklama 0.5-0.9.

2.19. Bir hukuk sistemindeki mevcut özel hukuk kuralları zaten bu İlkelerle uyumlu olabilir veya olmayabilir. Eğer ilgili hukuk sistemlerindeki genel mahiyetli özel hukuk kuralları İlkelerle uyumluysa bunlar da dijital varlıklar bakımından İlkeler hukuku olarak değerlendirmeye alınabilir. Ancak bu durum, genel mahiyetli özel hukuk kurallarının getirdikleri düzenlemelerin sadece dijital varlıkları ilgilendirdiği ölçüde geçerli olur.

2.20. İşlevsellik ve tarafsızlık ilkeleri gereği, bu İlkeler dijital varlıkların mutlaka belli bir hukuki kategoriye dâhil edilmesini zorunlu kılmaz. Bununla birlikte, İlke 3(1) uyarınca dijital varlıkların malvarlıksal mutlak haklara konu oluşturabilmesi lazım gelir. Bu da bazı ülkelerde dijital varlıkların “eşya”, “mal”, “şey” veya benzeri türden başka bir kategoriye dahil edilmesini zorunlu kılabilir. Bu konu, doğrudan doğruya uygulanacak hukuka tabi olup yapılacak tercih tümüyle ilgili devletin takdirine bırakılmış bulunmaktadır. Eğer bir devletin hukukunda, malvarlıksal mutlak hakların konusunu oluşturabilecek farklı malvarlığı değeri kategorileri mevcutsa ve bu kategorilerden her biri için farklı sonuçların uygulanması söz konusu ise, ilgili devlet hukukunun dijital varlıkların hangi kategoriye dahil edileceğini açıkça belirlemesi önerilir. Bu şekilde, dijital varlıklar malvarlıksal mutlak hakların konusunu oluşturabilirler. İlgili durumda, gerekirse yeni bir malvarlığı

değeri kategorisinin oluşturulması gerekebilir, ancak bu husus da her bir devletin kendi takdirine bırakılmıştır.

2.21. Daha genel olarak, eğer belirli bir devlette, dijital varlıklara uygulanacak genel kurallar konusunda bir belirsizlik varsa, bu hususun açıklığa kavuşturulması önerilir. Bu, özellikle dijital varlık üzerindeki malvarlıksal mutlak hakkın kazanılması veya devriyle ilgili durumlarda önem taşır. Yine benzer şekilde, dijital varlıklar üzerinde teminat hakkı kurulmasına ilişkin olarak hangi kural ve standartların geçerli olacağı hususu da ilgili devlet tarafından netleştirilmelidir. Ancak bu durum, bir devlet hukukunun dijital varlıklara uygulanacak her bir kural ve standardı teker teker listelenmesini de zorunlu kılmaz. Böyle bir listeleme yalnızca gereksiz bir karmaşıklık yaratmakla kalmaz, aynı zamanda lüzumsuz da olur; sonuçta bu İlkeler yalnızca özel hukuk kurallarıyla alakalı bulunmakta, spesifik olarak da malvarlıksal mutlak hakları ilgilendiren düzenlemeler getirmektedir. Ayrıca bkz. Açıklama 3.1–3.4.

2.22. Bir devletin hukukunda “İlkeler hukuku” kapsamına girmeyen tüm hukuk kuralları bu İlkeler tahtında “diğer hukuk” olarak sınıflandırılmış bulunmaktadır (bkz. İlke 2(4)). Burada tanımlandıkları halleriyle “İlkeler hukuku” ve “diğer hukuk”, birlikte “hukukun bütünü” oluşturur. Diğer hukuk, idari düzenlemeleri, yargı kararlarıyla oluşturulmuş kuralları ve kanunları bir arada içerir.

Devir

2.23. Burada tanımlanan anlamda “devir”, yani dijital varlık üzerindeki malvarlıksal mutlak hakkın bir kişiden başka bir kişiye geçirilmesi, İlke 6(2)’de tanımlanan kontrol değişikliği ile karıştırılmamalıdır. Bir dijital varlığın kontrolünün değişmesi, duruma göre malvarlıksal mutlak hakkın da devredilmesiyle üst üste gelebilir veya gelmeyebilir (Bu konuda bkz. Açıklama 2.26). Bazı durumlarda, uygulanacak hukuk çerçevesinde, kontrol değişikliği bir hak değişikliğini meydana getirmeyebilir. Örnek olarak bir saklayan (İlke 10(1)’de tanımlandığı üzere), müşterisi adına bir dijital varlık üzerindeki kontrolü elde edebilir ama bu onun dijital varlık üzerindeki malvarlıksal mutlak hakkı kazandığı anlamına gelmez. Diğer taraftan, çoğu durumda dijital varlık üzerindeki hakkın devri, bir kontrol değişikliğini de beraberinde getirir, ancak her zaman böyle olmak zorunda

değildir. Bir devletin hukukunda, belirli durumlarda dijital varlık üzerindeki malvarlıksal mutlak hak bir başkasına geçse bile, kontrol devreden elinde kalabilir.

2.24. İlke 2(5)'teki “devir” tanımı, yalnızca bir dijital varlığın başkasına geçişini değil, aynı zamanda devreden tarafından, bu tür bir varlıktan türeme yoluyla ortaya çıkan ve ondan farklılık arz eden bir dijital varlığın kazanılmasını da kapsar (Ayrıca bkz. 6(2)). Bu duruma örnek olarak Bitcoin işlemlerindeki UTXO (*unspent transaction output* / harcanmamış işlem çıktısı) gösterilebilir. Ethereum platformundaki işlemler özelinde söz konusu olan ether hesap bakiyesi düzenlemeleri de yine aynı mantıkla değerlendirmeye alınabilir; burada da elden çıkarılan varlık ile edinilen varlık misli mahiyettedir, dolayısıyla bunlar “aynı” olmak zorunda değildir.

2.25. Bu İlkelerde geçen “devir” terimi, teminat hakkı kurulmasını, “devreden” terimi teminat veren, yine “devralan” terimi de teminatlı alacaklıları kapsayacak şekilde geniş anlamda kullanılmıştır. Ancak bu kullanım, sadece tanımlama yapılmasında kolaylık sağlanması bakımındandır, yoksa bunun ötesinde İlkeler kapsamında dijital varlık üzerinde kurulacak teminat hakkının, uygulanacak hukuk çerçevesinde dijital varlık üzerindeki malvarlıksal mutlak hakkın bütünüyle devrini gerektireceği söylenemez. Yine örnek olarak bkz. 5 Temmuz 2006 tarihli Aracı Nezinde Tutulan Menkul Kıymetlere İlişkin Belirli Haklara Uygulanacak Hukuk Üzerine Milletlerarası Antlaşma (*Convention of 5 July 2006 on the Law Applicable to Certain Rights in Respect of Securities held with an Intermediary* (“*Hague Securities Convention*”)) madde 1(1)(h)'de “tasarruf” “mülkiyet hakkının tamamen veya teminat amacıyla devri ile zilyetliğe dayalı veya zilyetliğe dayalı olmayan teminat haklarının tesisini içeren her türlü işlem” olarak tanımlanmaktadır.

2.26. Bu İlkeler, dijital varlık üzerindeki malvarlıksal mutlak hakkın bir başka kişiye geçerli şekilde devredilmesinin koşullarını düzenlemez. Her ne kadar İlke 3(1) dijital varlıkların malvarlıksal mutlak haklara konu olabileceğini, İlke 8 de masum kazanımda bulunan sıfatının haiz olunabilmesi için kontrolün elde edilmesi gerektiğini öngörse de; bu İlkeler dijital varlığın geçerli suretle devrinin tüm koşullarını belirlemez. Örneğin bir kontrol değişikliğinin, malvarlıksal mutlak hakkın devri için gerekli olup olmadığı konusu diğer hukuka bırakılmıştır. Ayrıca bkz. İlke 3(3).

2.27. “Devreden” terimi, “devri başlatan kişi” ye karşılık gelir. Duruma göre bu kişi, sahip olduğu haklardan fazlasını devralana geçirebilecek bir yetkiye sahip olabilir. Örneğin, kontrol sahibi bir kişi, dijital varlık üzerinde malvarlıksal mutlak hakka sahip olmasa da bu varlığı masum kazanımda bulunana devredebilir. Bkz. İlke 8(4) ve Açıklama 8.9.

İflasla İlgili Süreç

2.28. Burada kullanılan “iflasla ilgili süreç” ifadesi, iflas süreçleriyle ilgili genel bir tanım vermeye yönelik bir amaç taşımaz, yalnızca bu İlkeler bağlamında kullanılabilirliği haizdir. UNCITRAL İflas Hukuku Rehberi gibi kaynaklarda genel tanımlar bulunabilir. “İflas süreçleriyle” ilgili daha genel mahiyette bir tanım, UNCITRAL İflas Hukuku Üzerine Yasama Rehberi (*Legislative Guide on Insolvency Law*) ve yine bunu takip eden iflasla ilgili hukuk metinlerinde bulunabilir. İlke 2(6)’da ise, borçlunun kötüleşen mali durumu nedeniyle başlatılan ve hukuki sonuç doğuran her türlü toplu, yargısal veya mahkeme dışı süreci kapsayan geniş bir tanım benimsenmiş ve ilgili sürecin başlama anına hukuki bir etki atfedilmiştir. Bu tanım, genellikle “karma” olarak sınıflandırılan ve hem mahkeme huzurunda yürütülen resmi iflas süreçlerini hem de mahkeme dışı sözleşmeye dayalı kolektif yeniden yapılandırma çözümlerinin unsurlarını bir arada barındıran yeni nesil iflas süreçlerini kapsamına alır. Dolayısıyla İlke 2(6)’da yer verilen “iflasla ilgili süreç” terimi, tümüyle mahkeme huzurunda yürütülen süreçleri, borçlunun malvarlığını olağan ticari faaliyetleri dışında yönetme ve/veya bunlarla ilgili tasarruf yetkisinin kısıtlandığı süreçleri ya da sadece borçlunun malvarlığına yönelik icra takiplerinin geçici olarak durdurulmasını tetikleyen ve iş faaliyetinin devamını sağlamayı amaçlayan süreçleri de kapsayacak biçimde geniş anlamda kullanılmaktadır. Bu nedenle İlkeler bağlamında, 2009 UNIDROIT Aracı Nezinde Tutulan Menkul Kıymetlere İlişkin Maddi Hukuk Kuralları – Cenevre Menkul Kıymetler Antlaşması (*Convention on Substantive Rules For Intermediated Securities (“Geneva Securities Convention”)*) madde (1)(h) ve benzeri hukuk metinlerinden farklı olarak, borçlunun malvarlığı üzerine mahkeme veya idari bir makamın doğrudan denetimi veya gözetimi bulunmasa da, borçlu kendisini “iflasla ilgili bir süreç” içinde bulabilir.

2.29. İlke 2(6)(a)’daki “kontrol” kelimesi, bu İlkelerdeki İlke 6 anlamında değil, iflas hukukundaki genel anlamıyla değerlendirmeye alınmalıdır.

Diğer Tanımlar

2.30. İlke 2(7), atıf kolaylığını sağlamak üzere, İlkelerde geçen ama anlamı başka maddelerde açıklanan terimlerin listesine yer vermektedir.

Yorum Kuralı

2.31. İlke 2(8), İlkelerin tamamına uygulanacak genel bir yorum kuralı getirir. Örnek olarak dijital varlığın misli mahiyet taşıdığı durumlarda, “bir dijital varlık” ve “ilgili dijital varlık” ifadeleri, aynı nitelikteki belirli bir miktar dijital varlığı da kapsamına almaktadır (bkz. Açıklama 11.6).

İlke 3

Genel İlkeler

- (1) Bir dijital varlık, malvarlıksal mutlak haklara konu olabilir.**
- (2) İlke hukuku, diğer hukukla çeliştiği durumlarda öncelikli olarak uygulanma kabiliyetini haizdir.**
- (3) Bu İlkeler tarafından aksi belirtilmedikçe, aşağıdaki tüm hususlarda diğer hukuk uygulanır:**
 - (a) bir kişinin bir dijital varlık üzerinde malvarlıksal bir mutlak hakka sahip olup olmadığı,**
 - (b) bir dijital varlık üzerindeki malvarlıksal mutlak hakkın başka bir kişiye geçerli olarak devredilip devredilmediği,**
 - (c) bir dijital varlık üzerinde geçerli bir teminat hakkının kurulup kurulmadığı,**
 - (d) bir dijital varlığı devreden ile devralan arasındaki hakları,**
 - (e) bir dijital varlık üzerinde teminat hakkı tesis eden ile lehine bu hak tesis edilen teminatlı alacaklı arasındaki hakları,**
 - (f) bir dijital varlığın devrinin üçüncü kişilere karşı ileri sürülebilir olmasının hukuki sonuçları,**
 - (g) bir dijital varlık üzerinde teminat hakkının üçüncü kişilere karşı ileri sürülebilmesi için aranan koşullar ve yine bunun hukuki sonuçları.**

Açıklama

İlke 3(1)

3.1. İlke 1’de belirtildiği üzere, bu İlkeler dijital varlıklarla ilgili özel hukuk konularını ve özellikle bunlar üzerinde söz konusu olan malvarlıksal mutlak hakları kapsar. Bu nedenle İlke 3(1) (İlke 2(3)’te tanımlandığı üzere) İlkeler hukukunun, dijital varlıkların malvarlıksal mutlak haklara konu olabileceği yönünde bir kabullenmede bulunması gerektiğini belirtir. Öyle ki, bu İlkelerde yer alan tüm düzenlemeler sözü geçen temel varsayım üzerine inşa edilmiştir. Ancak dijital varlıkların malvarlıksal mutlak haklara konu oluşturabilip oluşturamayacağı pek çok hukuk sistemi dahilinde tartışmalıdır. Bazı mahkemeler önemli (gündem oluşturan) davalarda dijital varlıkların malvarlıksal mutlak

haklara konu oluşturabileceğine karar vermiş, alanında yetkin birçok yazar da benzer yönde görüş bildirmiştir. Bu yüzden işbu İlkeler, devletlere bu hususta hukuki belirliliği artırmalarını ve açıkça dijital varlıkların malvarlıksal mutlak haklara konu olabileceğini düzenlemelerini tavsiye etmektedir. “Malvarlıksal mutlak hak” terimiyle neyin kastedildiği, Açıklama 3.4’te ele alınmaktadır.

3.2.Dijital varlıkların malvarlıksal mutlak haklara konu olabilmesi (bir hukuki sonuç) ile dijital varlıkların hangi malvarlığı değeri (varlık) kategorisi altında sınıflandırılacağı, birbirinden farklı meselelerdir. İlke 2(3)’ün açıklamasında belirtildiği üzere, bu İlkeler dijital varlıkların mutlaka belirli bir kategori altında sınıflandırılmasını zorunlu kılmaz. İlke 3(1)’in öngördüğü şekilde dijital varlıkların malvarlıksal mutlak haklara konu oluşturabilmesi, bazı ülkelerde bunların “mal”, “eşya”, “şey” veya benzeri bir kategorinin altına yerleştirilmesini gerektirebilir. Bunun nasıl yapılacağı uygulanacak hukuka tabidir, ve ilgili konudaki tercih de ilgili devlete bırakılmıştır. Eğer bir devlet hukukunda malvarlıksal mutlak haklara konu oluşturabilecek malvarlığı değeri (varlık) kategorileri arasında bir ayırım yapıyorsa ve ilgili ayırım çeşitli sonuç farklılıklarına vücut veriyorsa, dijital varlıkların hangi kategoriye dahil olduğunun ilgili devlet hukukunda açıkça belirlenmesi tavsiye edilir. Bu şekilde, ilgili devletin hukukunda dijital varlıkların malvarlıksal mutlak haklara konu oluşturabilmesi de temin edilmiş olur. Duruma göre ve gerekirse, yeni bir malvarlığı değeri (varlık) kategorisi bile yaratılabilir; ancak bu konudaki tercih ilgili devlete bırakılmıştır.

3.3.İlke 3(1), bir kişinin bir dijital varlık üzerinde malvarlıksal mutlak hakka sahip olup olmadığı veya bu hakkın geçerli şekilde bir başkasına devredilip devredilmediği gibi hususları ise diğer hukuka bırakır (bkz. İlke 2(4)). İlke 3(1)’de dijital varlıkların malvarlıksal mutlak haklara konu oluşturabilmesi varsayımı üzerinden hareket edilmekle birlikte, bu hakkın nasıl doğacağı veya nasıl geçerli biçimde devredileceği gibi hususlara değinilmemiştir. Bunlar diğer hukuka bırakılmıştır. Bkz. ayrıca İlke 3(3) ve Açıklama 3.8–3.12.

3.4.Bu İlkelerde “malvarlıksal mutlak hak” ifadesi geniş anlamda kullanılmaktadır. İlgili ifade, hem doğrudan bu tür bir mutlak hakkı hem de benzer yaratan etkiler yaratan diğer hakları kapsar. Bu geniş tanım, İlkelerin farklı hukuk sistemlerinde uygulanabilirliğini sağlamak amacıyla takip edilen işlevsel yaklaşımı da yansıtır. Ayrıca bu tanım, kişilerin

dijital varlıklar üzerinde -kendileriyle herhangi bir sözleşmesel ilişkinin bulunmadığı- üçüncü kişilere karşı da ileri sürebilecekleri hak veya menfaatlere sahip olabileceklerini ifade eder. Bu nokta, özellikle iflas bağlamında önem arz edebilir. İlgili durumda iflas idaresi, iflas edenin malvarlığı dahilinde bulunan dijital varlıklar üzerindeki malvarlıksal mutlak hakları üçüncü kişilere karşı ileri sürebilir ya da üçüncü kişiler de iflas idaresine karşı ilgili dijital varlıklar üzerinde sahip oldukları bu özellikteki haklar bakımından, hak iddiasında bulunabilirler.

İlke 3(2)

3.5.3Bu İlkeler, dijital varlıkların yapısını gözeterek ilgili varlıkların elde tutulması, devri ve teminat olarak kullanılması ile ilgili özel kurallar getirir. Bu nedenle bu İlkeler, devlet hukuklarını tamamlayabilir veya onlardan sapma gösterebilir. İlke 3(2), bu kuralların tam olarak uygulanabilmesi için, devlet hukuklarıyla çeliştiği durumlarda, İlkeler hukukunun öncelikli olacağını belirtir. Dolayısıyla bir devlet bu İlkeleri kendi hukuku olarak kabul edip uygulamaya koyduğunda, artık İlkeler hukuku (bkz. İlke 2(3)) diğer hukuka (bkz. İlke 2(4)) üstün gelir.

3.6.Yukarıda da belirtildiği gibi, bu İlkeler devletlerin dijital varlıklarla ilgili özel bir kanun yapmasını, ilgili kuralları genel kanunlarına entegre etmesini veya mevcut hukuk sistemi dahilinde bu sistemle uyumlu şekilde uygulanmasını veya da bu yaklaşımlardan birkaç tanesine birlikte yer verilmesine yönelik bir yaklaşım tarzını zorunlu kılmaz. Ancak, İlkeler hukuku (İlke 2(3)'teki tanım dahilinde) diğer hukukla (İlke 2(4)'teki tanım dahilinde) çatışması durumunda önceliklidir (Ayrıca bkz. Açıklama 2.18–2.22, özellikle Açıklama 2.19). Bu sonuca, özel kanunların genel kanunlardan daha önce ya da sonraki kanunların önceki kanunlardan daha önce uygulama alanı bulmasına ilişkin yürürlük kurallarıyla da ulaşılması mümkün olabilir. Yine devletler, bu düzenlemenin tam anlamıyla uygulanabilmesi için, hangi kanun bölümlerinin veya hükümlerinin değişmesi veya yürürlükten kalkması gerektiğini de belirleyebilir.

3.7.Bir devlet, İlkelerden bile daha özel mahiyette bir kanunu benimseyebilir; örneğin salt belirli bir bağlantılı dijital varlık türüne ilişkin özel kurallar getirebilir (bkz. İlke 4). Böyle bir durumda, devlet, mümkün olduğunca İlkeler hukuku ile bu özel kanunun uyumlu olmasını sağlamalıdır. Örneğin devlet, bu varlık türü için biraz daha farklı bir masum

kazanım kuralı öngörebilir (bkz. Açıklama 8.7) veya o varlık türünün teminat aracı olarak kullanılmasında belirli kuralların özel olarak uygulanmasını uygun bulabilir (bkz. Açıklama 14.4). Düzenlemeler arasında herhangi bir çatışmanın varlığı dahilinde, özel kanun İlkeler hukukuna üstün gelecektir. Bu türden bir özel kanuna, UNCITRAL Elektronik Devredilebilir Kayıtlar Model Kanunu (*Model Law on Electronic Transferable Records*) örnek gösterilebilir; ilgili kanun, elektronik belgelerin kâğıt (fiziki) muadilleriyle (eşdeğerleriyle) aynı işlevsel etkiye sahip olmasını sağlar. Böyle bir elektronik kayıt, İlke 2(2)'de tanımlanan bir dijital varlık özelliği taşıyabilir (bkz. Açıklama 4.22). UNCITRAL Elektronik Devredilebilir Kayıtlar Model Kanunu'nu benimseyen bir devlette, söz konusu özel kanun ve yine aynı devlet hukukunda bunların işlevsel kâğıt (fiziki) muadillerini (eşdeğerleri) düzenleme altına alan kanun, İlkeler hukuku ile çelişirse öncelikli olur. Ancak yine de devletlerin bu şekilde söz konusu olabilecek olası uyumsuzlukları mümkün olduğunca önlemek üzere gerekli adımları atmaları tavsiye edilir.

İlke 3(3)

3.8. İlke 3(3), diğer hukukun (bkz. İlke 2(4)'teki tanım dahilinde) dijital varlıklarla ilgili olarak geçerli olmaya devam ettiğini açıkça ifade eder. Bu kapsamda İlke 3(3), örnek olarak eşya hukukuna veya sözleşme hukukuna ilişkin bazı konuları listelemektedir. Bu konular, bu İlkelerin kapsamına girmediği ve değiştirilmesinin özel olarak amaçlanmadığı konulardır. İlgili liste sınırlandırıcı bir mahiyet taşımaz. Ayrıca, bu İlkelerin yalnızca özel hukuka dair kurallar getirdiği ve kamu kurumlarınca tatbik edilecek düzenleyici mahiyetteki kuralları (regülasyon) kapsamadığı tekrar vurgulanmalıdır. Bunun yanında, bu İlkeler yalnızca özel hukukun belli bir alanına odaklanmıştır; fikri haklar veya tüketicinin korunması hukuku gibi diğer alanları etkilemez. Dolayısıyla fikri haklar ve tüketicinin korunmasına ilişkin ulusal kanunlar geçerliliğini korur. İlke 3(3)'te listelenen örnekler, bu İlkelerin düzenlemediği ve devlet hukukuna tabi olan önemli konulara işaret etmektedir. Teknik olarak bakıldığında “bu İlkeler tarafından bertaraf edilmediği ölçüde” ifadesi gereksizdir; çünkü zaten İlke 2(4)'te tanımlanan diğer hukuk, İlkelerin kapsamına girmeyen kuralları ifade eder. Ancak herhangi bir tereddüde yer bırakmamak adına ilgili ifade eklenmiştir. Bu ifade, belirli bir devlet hukukunun yalnızca bu İlkelerin (İlkeler hukukundan farklı olarak) o hukuku açıkça devre dışı bırakmadıkça uygulanacağı anlamına gelmez. Her ne kadar İlke 2(5), “devir” terimini (bu İlkelerde kullanıldığı

haliyle) teminatlı alacaklı lehine bir teminat hakkının sağlanmasını kapsayacak biçimde tanımlasa da İlke 3(3)'teki listede devirlere ve teminat haklarının tesisine ayrı ayrı yer verilmiştir. Burada amaç açıklığın sağlanmasıdır, ilgili durum İlke 3(3)'ün diğer hukukun uygulanacağı konuları listelemiş olmasından ileri gelmektedir.

3.9. İlke 3(3)'te, diğer hukuk tarafından düzenlenmeye devam eden konulara ilişkin örnekler şu şekilde sınıflandırılabilir: İlke 3(3)(a)'da sayılan örnek, bir kişinin dijital varlık üzerinde malvarlıksal mutlak hakka sahip olup olmadığını belirlemeye odaklanmaktadır; bu statik (durağan) bir durumdur. İlke 3(3)(a) uyarınca, böyle bir hakkın üçüncü kişilere karşı ileri sürülebilmesi için gereken koşullar diğer hukuk tarafından belirlenir. Bu nedenle, örneğin bir kişinin dijital varlık üzerinde geçerli bir malvarlıksal mutlak hakka sahip olup olmadığı konusu, İlkeler tarafından düzenleme altına alınmamıştır.

3.10. İlke 3(3)(b) ve 3(3)(c) ise, devreden ve teminat veren açısından dijital varlıkların devri veya teminat olarak kullanılmasıyla ilgili dinamik durumlara işaret eder. Bir kişinin dijital varlığı geçerli şekilde devredip devretmediği ya da bu varlık üzerinde geçerli şekilde bir teminat hakkının kurulup kurulmadığı hususları, İlke 3(3)(b) ve 3(3)(c)'de açıkça belirtildiği üzere, esas itibarıyla diğer hukuka tabidir. Bununla birlikte bu İlkeler, dijital varlığın devri ve tesis edilen teminat hakkının üçüncü kişilere karşı ileri sürülebilirliğiyle ilgili bazı özel kurallar öngörür. Örneğin İlke 15, dijital varlık üzerinde kontrolü elde etmenin (İlke 6'da tanımlandığı haliyle), hakkın üçüncü kişilere karşı ileri sürülebilir olma özelliğinin kazanılmasında bir yöntem olarak kullanılabileceğini belirtir. Ancak diğer hukuk, ilgili bağlamda başka yöntemleri de ayrıca tanıyabilir. İlke 8, masum kazanımda bulunan kişiyi korur; İlke 12 de saklayan tarafından müşteri adına muhafaza edilen dijital varlıklar bakımından benzer biçimde bir koruma sağlar. Mevcut genel kuralların dijital varlıklara uygulanıp uygulanmadığı konusunda belirsizlik olduğunda veya İlkeler hukuku diğer hukukla çatıştığında, devletlerin bu konuyu açıkça düzenlemesi önerilir.

3.11. İlke 3(3)(d) ve 3(3)(e), sırasıyla devreden ile devralan ve teminat hakkı veren ile teminatlı alacaklı arasındaki hak ilişkilerini, diğer hukuk kapsamında ve temel olarak bu İlkelerin kapsamı dışında bırakır. Bazı hukuk sistemlerinde bu ilişkiler, sözleşmeye dayalı bir mahiyet arz eder. İlke 3(3)(d) ve 3(3)(e), sırasıyla devreden ile devralan ve teminat hakkı veren ile teminatlı alacaklı arasındaki hak ilişkilerinin, taraflar arasındaki ilişki nasıl nitelendirilecek olursa olsun, diğer hukuk tarafından ele alınacağını öngörmektedir.

3.12. Yukarıda açıklandığı üzere, İlke 3(3)(d) ve 3(3)(e) devreden ile devralan ve teminat veren ile teminatlı alacaklı arasındaki (sözleşmesel) ilişkileri ilgilendirir. Bunlar sözleşme tarafları arasındaki *inter se* ilişkileri ilgilendirir. Buna karşılık İlke 3(3)(f) ve 3(3)(g), üçüncü kişilerle olan *erga omnes* ilişkileri düzenler. Bir dijital varlığın devrinin veya bu varlık üzerinde tesis edilen teminat hakkının üçüncü kişilere karşı ileri sürülebilir olup olmayacağı, temel itibariyle diğer hukuk tarafından belirlenir. Bazı hukuk sistemlerinde, üçüncü kişilere karşı ileri sürülebilir olma özelliği, “etkililik” kavramıyla ifade edilir. İlke 3(3)(f) ve 3(3)(g), bağlam ne olursa olsun ve hangi terminoloji kullanılırsa kullanılsın, üçüncü kişilere karşı ileri sürülebilirliğin veya etkililiğin koşullarının da, İlkeler tarafından da aksi özel olarak belirtilmedikçe, temel itibariyle diğer hukuk tarafından düzenleneceğini belirtir (bkz. Açıklama 3.10 ve İlke 15).

İlke 4

Bağlantılı Varlıklar

Bu İlkelerin uygulandığı dijital varlıklar, başka bir malvarlığı değeriyle (varlıkla) bağlantılı olan dijital varlıkları da kapsar. Söz konusu diğer malvarlığı değeri (varlık), maddi özellik gösteren veya göstermeyen (başka bir dijital varlık dâhil olmak üzere) bir malvarlığı değeri (varlık) olabilir. Dijital varlık ile bu diğer malvarlığı değeri (varlık) arasındaki bağlantının mevcudiyeti, ilgili bağlantının kurulabilmesinin hukuki gereklilikleri ve sonuçları, dijital varlığın devrinin bağlantılı bulunduğu diğer malvarlığı değeri (varlık) üzerindeki etkileri de dâhil olmak üzere, diğer hukuk tarafından belirlenir.

Açıklama

4.1. İlke 4'te öngörüldüğü üzere, bir dijital varlık başka bir malvarlığı değeri (varlık) veya değerleriyle bağlantılı olabilir. İlkeler hukuku, bu bağlantının yeterince kurulup kurulmadığı veya bu bağlantının hukuki sonuçlarının neler olduğu konusunda tarafsız bir duruş sergiler. Bu konular bağlamındaki hususlar, ilgili devlet nezdinde uygulama alanı bulacak diğer hukuka (düzenleyici kurallar (regülasyon) da dahil olmak üzere) bırakılmıştır. Bağlantının işleyiş yapısı, o devlet dahilinde yürürlükte bulunan mevcut hukuk kurallarına ya da bağlantılı varlıklara özgü olarak yeni geliştirilecek kurallara bağlı biçimde değişkenlik gösterebilir. Dolayısıyla dijital varlık ile diğer malvarlığı değeri (varlık) arasındaki bağlantının nasıl işlerlik göstereceği, uygulama alanı bulacak diğer hukuka göre farklılık gösterebilir.

4.2. Dijital bir varlığın başka bir malvarlığı değeriyle (varlıkla) bağlantılı olarak tasarlanmasının yaygın nedeni, dijital varlığın devriyle birlikte söz konusu diğer malvarlığı değeri (varlık) üzerinde işlem yapılmasını mümkün kılınmasıdır. Bağlantının kurulmasındaki amaç, dijital varlığı elinde bulunduran kişinin, diğer malvarlığı değeri (varlık) üzerindeki hakların veya o varlığı ihraç eden kişiyle ilişkili hakların değiştirebilmesini sağlamak olabilir. Dijital varlığın devriyle birlikte diğer malvarlığı değeri (varlık) üzerindeki hakların da devredilmesi amaçlanabilir.

4.3. İlke 4’te bahsedilen “diğer malvarlığı değeri (varlık)”, maddi ya da maddi olmayan mahiyette bir malvarlığı değeri (varlık), başka bir dijital varlık ya da hisse senedi, tahvil gibi diğer hukuka göre oluşturulmuş bir malvarlığı değeri (varlık) da olabilir. Bu diğer malvarlığı değeri (varlık), dijital varlıkla eşzamanlı olarak var olur fakat ondan bağımsızdır. İlke 6(2)’de tanımlanan “türeme yoluyla ortaya çıkan bir dijital varlık”, diğer bir deyişle de önceden var olan bir dijital varlığın kontrolündeki değişim sonucu meydana gelen dijital varlık, bu kapsama girmez.

Bağlantının Varlığı ve Etkisi

4.4. Bağlantılı varlıkların işleyiş yapısı iki temel soruya bağlıdır: (1) Dijital varlık ile diğer varlık arasında gerçekten bir bağlantı bulunmakta mıdır? (2) Bu bağlantı, tarafların diğer varlık üzerindeki haklarına herhangi bir hukuki etki doğurmakta mıdır? Her iki soru da ilgili devlet nezdinde uygulama alanı bulan diğer hukuk tarafından cevaplanır.

4.5. Bağlantının gerçekten mevcut olup olmadığı esasen bir olgusal bir durumdur. Böyle bir durumun varlığı, somut olayı çevreleyen tüm koşullara ve dijital varlığı meydana getiren tarafların iradesine bağlı bulunur. İlgili bağlantı, dijital varlığın kodlamasından, ilgili sistem protokollerinden ya da yayımlanmış teknik dokümanlardan (örneğin teknik rapor (*white paper*) veya ihraç şartları) anlaşılabilir. Ayrıca, ilgili devletin diğer hukukunda (düzenleyici kurallar da dahil olmak üzere) bu bağlantının var olduğunun tanınması için asgari hukuki standartlar da belirlenmiş olabilir. Bu standartları karşılayamayan bir bağlantı, tarafların amacı ne olursa olsun etkisiz kalabilir.

4.6. Dijital varlık ile diğer malvarlığı değeri (varlık) arasındaki bağlantının fiili varlığı tatmin edici biçimde kanıtlansa bile, bunun hukuki etkisi yine diğer hukuka bağlı bulunur. Buradaki “hukuki etki” ifadesi de geniş anlamda değerlendirilmelidir. Bu ifade özellikle dijital varlıkla yapılan bir işlemin diğer malvarlığı değerini (varlığı) ilgilendiren haklara etkisini veya iflas halinde bu bağlantının sonuçlarını kapsamına almaktadır. Hukuki etki tanınması halinde buna bağlı olarak oluşabilecek bir sonuç, dijital varlık ve diğer malvarlığı değerini (varlığı) ilgilendiren hakların senkronize şekilde devredilebilir olmasıdır. Ayrıca dijital varlık sahibi ile diğer malvarlığı değeri (varlık) sahibi arasındaki sözleşmesel haklar da bu bağlantı sayesinde değişme gösterebilir.

4.7.Bu İlkenin öngördüğü şekilde diğer hukukun önceliği gözetildiğinde, dijital varlığı ihraç eden veya üzerinde işlem yapan taraflar, ilgili bağlantıya diğer hukukta izin verilenin ötesinde bir hukuki etki atfedemezler. Örnek olarak sadece taraflar arası bir sözleşmeyle, dijital varlığın devrinin mutlaka diğer malvarlığı değeri (varlık) üzerindeki malvarlıksal mutlak hakkın da devredilmesi sonucunu meydana getireceği hükme bağlanamaz. Böyle bir etkinin ilgili devletin diğer hukukunca da kabul görmesi gerekir. Taraflar arasındaki sözleşme, yalnızca o sözleşmenin tarafları için geçerli olacak sonuçlar doğurabilir.

Kayıt Sistemleriyle Karşılaştırma

4.8.Bağlantılı dijital varlıklarla yapılan işlemler, her zaman, hukuken oluşturulmuş bir kayıt sisteminde kaydedilen menkul kıymetler gibi geleneksel malvarlığı değerleriyle (varlıklarla) yapılan işlemlerle aynı hukuki etkiye sahip olmayabilir. Dijital varlığın kayıtlı hak sahipliğinde yapılan bir değişiklik, ilgili bağlantıya hukuki bir sonuç tanınmadığı sürece, diğer malvarlığı değeri (varlık) bakımından hukuken herhangi bir etki meydana getirmeye elverişli değildir. Diğer hukuk tarafından böyle bir hukuki sonuç öngörülüyorsa, bunun sonucu olarak dijital varlık ile diğer malvarlığı değeri (varlık) üzerindeki hak devrinin eşzamanlı olması söz konusu olabilir.

4.9.Geleneksel bir menkul kıymet siciline kaydedilen devir işlemi, ilgili malvarlığı değeri (varlık) üzerindeki hakkı devredilmesini sağlar. Bunun sebebi diğer hukuk çerçevesindeki mevzuatın sicil sistemine hukuki bir etki atfetmesidir. Benzer şekilde, bir devletin diğer hukuku da dijital varlık devrinin, onunla bağlantılı diğer bir malvarlığı değeri (varlık) üzerindeki hakkın da devredilmesini sağlayacağını öngörebilir. Bunun sebebi, diğer hukukun bağlantıyı, dijital varlığın devrinin doğrudan tarafların diğer malvarlığı değeri (varlık) devredilebilmesini sağlamak üzere öngörmesidir.

Diğer Hukuk

4.10. Hukuki etki, mevcut diğer hukuk kurallarıyla belirlenebileceği gibi, devletler bağlantılı varlıklara özgü yeni kurallar da getirebilir. Diğer hukuk, bağlantının varlığını kabul etmekle birlikte, dijital varlığın devrinin diğer varlık üzerindeki haklara hiçbir etkisi olmayacağını da düzenleyebilir. Bu durumda, bağlantılı varlık üzerindeki hak sahipliği durumunu değiştirmek için ayrı bir hukuki işlem gerekebilir. Dolayısıyla bağlantılı

varlıkların elde tutulması ve devri, bu İlkeler ile diğer hukukun bir arada uygulanması suretiyle yürütülür.

Masum Kazanım

4.11. Bir devletin diğer hukuku, İlke 8'e uygun şekilde dijital varlık için öngörülen masum kazanım kuralının, bağlantılı diğer varlık için de geçerli olacağını düzenleyebilir. Ancak bu İlkeye göre, dijital varlık ile diğer varlık arasındaki bağlantının ispatı, diğer hukukun önceliği düşüncesiyle de tutarlı biçimde, otomatik olarak diğer varlık bakımından masum kazanımı sağlamaz. Bunun için diğer hukukta ilgili sonuca yol açabilecek bir düzenleme bulunmalıdır (bkz. Açıklama 4.29–4.32, Örnek Durum 8).

4.12. Dijital varlık ile diğer varlık arasındaki bağlantının farklı hukuki etkilerini göstermek amacıyla aşağıda sekiz örnek duruma işaret edilmiştir.

4.13. Örnek Durum 1. Yürürlükte bulunan diğer hukuk kuralları, tarafların dijital varlıkla yaptıkları işlemler için uygulama alanı bulabilir ve bağlantılı diğer varlık üzerindeki hukuki etkileri belirleyebilir.

4.14. Örnek olarak, tokenize edilmiş altının alınıp satılması için bir sistem kurulabilir. Bir yatırımcı, belirli miktardaki altın üzerinde hakkını temsil eden dijital bir tokeni elinde bulundurabilir. Bu tokenin devri, satıcının altın üzerindeki aynı hakkını devretmeye yeterli olur mu sorusu, ilgili devletin diğer hukukuna bağlıdır. Bazı sistemlerde, token devrine tarafların altın üzerindeki aynı hakkını devretme niyetinin dışı yansıması olarak muamele edilebilir. Böylece alıcı, token ile birlikte altın üzerindeki hakkı da kazanır. Bunun için ilgili devletin ayrıca bir düzenleme yapmasına gerek olmaz (Burada şöyle bir parantez açılabilir: İlgili devletin diğer hukuku bu sonuca izin verse bile, ilgili durum tarafların dijital tokenden bağımsız olarak doğrudan altın üzerinde işlem yapmalarına mutlak olarak engel olmaz. Ancak taraflar bu şekilde doğrudan altın üzerinde de işlem yapmaya devam ederlerse, dijital varlık ve altın üzerindeki hakların senkronizasyonu (uyumu/eşzamanlılığı) bozulabilir).

4.15. Bazı devletlerde ise üzerindeki hak sahipliğinin alıcıya geçişi için satıcının ilgili altını fiilen teslim etmesi zorunlu olabilir; bu durumda token devri altın üzerindeki aynı hakkı

karşı tarafa geçirmez. Dolayısıyla dijital varlık ile diğer malvarlığı değeri (varlık) arasındaki hak devrinin uyumlu hale getirilebilmesi için yeni bir düzenlemenin yapılmasına ihtiyaç olabilir.

4.16. Örnek Durum 2. Bir dijital varlık başka bir dijital varlıkla bağlantılı olabilir ve bu bağlantının hukuki etkisi, bu varlıkları ellerinde bulunduranlar arasındaki ilişkiden kaynaklanabilir.

4.17. Örneğin, bir ihraççı başka bir protokoldeki (sistemdeki) dijital varlığın “sarmalanmış” (*wrapped*) versiyonunu yaratabilir. Sabit (stabil) kripto varlıklarda olduğu gibi, diğer varlığa karşılık gelen yalnızca bir tane sarmalanmış dijital varlık oluşturulabilir. Teknik raporda (*White paper*) sarmalanmış dijital varlık sahibinin diğer dijital varlığı geri alma (bozdurma) hakkı olduğu belirtilmiş olabilir. Bu durumda devralan, sarmalanmış varlığın karşılığı olan varlığı geri alabilir (bozdurabilir). Belirtilen 1:1 oranlı yapının etkisi, sarmalanmış dijital varlığın değerinin diğer varlıkla aynı olmasını sağlar. Sarmalanmış dijital varlık devredildiğinde, devralan, diğer dijital varlık doğrudan devredilmiş olsaydı elde edeceği değerin aynısını elde etmelidir. Bu iki varlık üzerindeki hak sahipliği durumu, bağlantıya atfedilen hukuki etkiye bağlı bulunacaktır. İhraççı ile sarmalanmış dijital varlığı elinde bulunduran arasındaki sözleşmenin hükümleri, dijital varlığı elinde bulunduran kişinin diğer varlık üzerindeki kontrolü yeniden elde edebilip edemeyeceğini, ilgili bağlamda da sarmalanmış dijital varlığın “yakılıp” (burn) yok edilip edilmeyeceğini belirleyecektir. Ayrıca 2, 6 ve 7 numaralı örnek durumlar dahilinde yer verilen “ihraççı” teriminin, İlke 5(2)(f)’de belirtilen sınırlı anlamda kullanılmadığına dikkat çekilmelidir.

4.18. Örnek Durum 3. Yürürlükteki diğer hukuk, dijital varlığa bağlı bir varlığın tüm malvarlıksal mutlak hak boyutlarını tarafların amaç ve beyanlarından bağımsız olarak düzenleyebilir.

4.19. Örneğin, Alpha isimli kişi açık ve izinsiz bir blokzincir üzerinde bir müzik eseriyle ilgili telif haklarını temsil eden bir gayri misli dijital varlık (*non-fungible digital asset - NFT / A-NFT*) meydana getirdiğini ilan edebilir. Ayrıca Alpha, diğer bir kişi (Beta) ile yaptığı sözleşmede, A-NFT devredilince bunun üzerindeki telif hakkının da Beta’ya geçeceğini kararlaştırabilir. Beta da ilgili telif haklarını A-NFT’yi devrederek tekrar devir konusu yapabilir. Ancak bu bağlantının hukuken geçerli olup olmayacağı, Alpha’nın telif

haklarını tokenize etme amacından bağımsız biçimde, telif hakkına uygulanacak hukuka bağlıdır. Benzer şekilde Beta'nın daha sonra bu telif hakkını üçüncü kişilere A-NFT'yi devrederek tekrar devretmesine de, yine telif hakkına uygulanacak hukuka göre bir sonuç bağlanabilir.

4.20. Örnek Durum 4 ve 5. Devlet, token ile diğer varlık arasındaki bağlantıyı hukuken geçerli kılacak özel bir mevzuatı yürürlüğe sokabilir.

4.21. Örneğin, bir şirket blokzincir üzerinde borçlanma (tahvil) senetleri ihraç ederek yatırımcılardan kaynak toplayabilir. Her bir yatırımcı, elinde şirkete karşı olan alacak haklarını temsil eden devredilebilir tokenler bulundurur. İhraç koşulları, borçlanma senetlerini ihraç eden şirketten ödeme alma hakkını tanıyabilir. Dolayısıyla, söz konusu token blokzincir üzerinden devredildiğinde, ilgili alacak hakkı da devredilmiş olur. Şirket, borcunu ilgili tokeni elinde bulundurana ödeyerek borcundan kurtulabilir. Eğer mevcut sistem bu sonucu, alacağın devri, yenileme veya menkul kıymet devri gibi hukuki kurgular üzerinden sağlamıyorsa, anılan sonuca ulaşılmasında özel bir mevzuata ihtiyaç duyulabilir.

4.22. Benzer şekilde, bir devlet kıymetli evrakın dijital muadillerini (eşdeğerlerini) yaratacak bir mevzuatı yürürlüğe koyabilir. Bu kanun, dijital varlık üzerindeki kontrol değişikliğinin, kıymetli evrakın zilyetliğinin devriyle aynı etkiyi doğuracağını öngörebilir. Böylece devralan, ilgili devletin diğer hukuku dahilinde, dijital varlık üzerinden bunun temsil ettiği bir alacak hakkını veya bir ayni hakkı elde edebilir. Söz konusu özel mevzuat, dijital varlığın, devletin mevcut diğer hukukunda yer alan kıymetli evrakın muadili (eşdeğeri) olarak bir etki gösterebilmesi için gerekli olan asgari kriterleri belirleyecektir.

4.23. Örnek Durum 6. Bir dijital varlık ile başka bir varlık arasındaki bağlantının hukuki etkisi, diğer hukuktan olduğu kadar, sistem kodlaması, protokoller ve belgelerde somutlaşmış taraf amaçlarına da bağlı bulunulabilir. Dolayısıyla bir dijital varlığın ihraç edilmesine eşlik eden teknik raporun (*White paper*) hükümleri, dijital varlık sahibinin diğer varlıkla ilgili olarak sahip olması amaçlanan hakkın niteliğini ve değerini belirlemede etken oluşturabilir.

4.24. Örneğin, sabit (stabil) kripto varlık ihracı sırasında, bu varlıklar Amerikan Doları gibi bir para birimine endekslenebilir. İhraç edilen her 1 Amerikan Doları sabit (stabil) kripto varlık karşılığında, ihraççı, Amerikan Doları türünden likit varlıklardan oluşan 1:1 oranında bir rezerv meydana getirir. Bu rezerv, ihraççının kendi varlıklarından ayrı olarak bir aracı tarafından tutulur. Teknik rapor (*White paper*), herhangi bir sabit (stabil) kripto varlık sahibinin bu kripto varlığı ihraççıya Amerikan Doları cinsinden bir nominal para değeri üzerinden tekrar satma hakkına sahip olduğunu öngörebilir. Bu tekrar satma hakkı, kripto varlığın ödeme işlemlerinde dolaşım halindeki devir değeri bakımından istikrarın sağlanmasında etki gösterir.

4.25. Sabit (stabil) kripto varlık devrinin ve bu devrin ihraççıya karşı doğurabileceği hakların etkisi, hem teknik raporda (*White paper*) öngörülen koşullara hem de diğer hukukun alacak devri veya yenilemeye ilişkin kurallarına bağlı bulunabilir. Teknik rapor (*White paper*), sabit (stabil) kripto varlık sahibinin öncelikle ihraççıya karşı sözleşmesel bir hakka sahip olmasının amaçlandığını gösterebilir. Yine bu varlığın devri, alacak devri ve yenileme hukuki mahiyeti taşıyabilir. Diğer hukuk veya teknik raporun (*White paper*) hükümleri üzerinden, token sahibinin sabit (stabil) kripto varlık üzerinde malvarlıksal mutlak bir hakkı olsa dahi bu kişinin rezervde tutulan diğer varlıklar üzerinde herhangi bir malvarlıksal mutlak hakka sahip olmadığı sonucuna varılabilir. Söz konusu hakkın ihraççıya karşı ileri sürülebilecek başka talepler karşısında hangi ölçüde önceliğe sahip olacağı ise, uygulanacak hukukun iflasa ilişkin kuralları tarafından belirlenir.

4.26. Örnek Durum 7. Dijital varlıklar, blokzincir dışında var olan başka varlıklar bakımından söz konusu olacak devredilebilir değer paylarının oluşturulması için de kullanılabilir. Dijital varlıkla diğer varlık arasındaki bağlantının varlığı açık olsa bile, bunun doğuracağı hakların etkisi ilgili devletin diğer hukukuna bağlıdır. Tarafların bağlantı kurma niyeti, diğer hukukun bu varlıklar bakımından öngördüğü etkileri bertaraf edemez.

4.27. Örnek olarak bir ihraççı, sahibine bir taşınmazla ilgili talep hakkı vereceği öngörülen dijital varlıkları satabilir. Bu varlıkla blokzincir üzerinden devredilebilir niteliktedir. Ancak daha yakından incelendiğinde, tokenize edilmiş taşınmaz paylarının çoğunluğu üzerindeki aynı hakların kurulacak bir şirkete devredilmesinin planlandığı görülür. İşbu şirketin hisseleri tokenize edilir ve blokzincir üzerinden devredilebilir hale getirilir. Ancak

tokenlerin devri, hukuken şirket hisselerinin veya taşınmaz payları üzerindeki hakların devri için yeterli olmayabilir. Bu hususların, şirketin kurulduğu veya taşınmazın bulunduğu yerdeki diğer hukuka göre değerlendirilmesi gerekebilir. Dijital varlık burada şu hususları göstermek açısından önemlidir: (i) Tokeni elinde bulunduran kişiyle şirket hisseleri ve taşınmazla ilgili hukuki ilişkileri; (ii) tokeni devralan kişinin şirket hisse defteri veya taşınmazın kayıtlı bulunduğu tapu sicilinde tutulan kayıtların güncellenmesi bakımından atılması gerekli bulunan adımları göstermek bakımından önem taşır.

4.28. Bu örnek, bir tokenin kişiler arasında devredilmesinin tek başına şirket hisselerinin ve taşınmazların devrini gerçekleştirmeyebileceğini göstermektedir. Benzer şekilde, bir kişinin token üzerinde sağladığı kontrol, hisselerin veya taşınmazların, token üzerinde gerçekleştirilecek herhangi bir işlemde bağımsız olarak devredilmesini engellemek bakımından yeterli olmayabilir.

4.29. Örnek Durum 8. Bir devletin diğer hukuku, dijital varlıkla arasında bağlantı kurulan diğer varlıklar için de bir masum kazanım kuralı öngörebilir. Böyle bir durumda, masum kazanım hem dijital varlık hem de diğer varlık bakımından bir etki meydana getirebilir.

4.30. Örnek olarak, Açıklama 4.13 – 4.15’te olduğu gibi, tokenize edilmiş altın ticareti için bir sistem kurulabilir ve bir yatırımcı, ilgili altının belirli bir payı üzerindeki aynı hakkı temsil eden bir dijital varlığı elinde tutabilir. Anılan durumda bir bilgisayar korsanının, hukuka aykırı biçimde token üzerindeki kontrolü ele geçirdiği ve bunu satış yoluyla masum bir alıcıya aktardığı düşünülün. Böyle bir durumda alıcı, token üzerinde, önceki hak sahibi konumunda bulunan yatırımcının haklarından arınmış bir hakkı elde eder. Bununla birlikte masum alıcının, “bağlantılı” altın payı üzerinde de önceki yatırımcının taleplerinden arınmış bir hakkı kazanabilip kazanamayacağı, ilgili devletin diğer hukukuna tabi olacaktır.

4.31. Bir devletin diğer hukuku teminat hakkı konusu oluşturan bir bağlantılı varlık bakımından da benzer sonuçları öngörebilir. Belirli bir altın payını temsil eden bağlantılı varlık üzerinde bir teminat hakkı tesis edilebilir. İşbu teminat hakkının ilgili altın payını da etkileyip etkilemediği diğer hukuka tabi olan bir konudur. Açıklama 4.20 – 4.22’deki örnek geliştirilerek, diğer hukukun böyle bir tokeni altın üzerindeki paya ilişkin aynı hakkı gösteren bir hak sahipliği belgesi olarak değerlendirmeye aldığı düşünülebilir. Böyle bir

durumda token üzerinde tesis edilen teminat, altın payı bakımından da etki gösterir. Bu türden bir sistem, tüm hakların token dahilinde “yer almasını” sağlamak amacıyla, bağlantılı varlık üzerindeki hakların nasıl düzenleneceğini dikkatli biçimde ele almalıdır.

4.32. Eğer diğer hukuk, diğer varlığın masum kazanımı bakımından benzer bir sonucu öngörüyorsa, masum alıcı hem dijital varlığı hem de diğer varlığı başka haklardan arınmış olarak kazanabilir. Diğer hukukun önceliği dahilinde, masum kazanımda bulunanın hakları, dijital varlığa ilişkin İlkeler hukuku kurallarından daha farklı kurallar dairesinde belirlenmiş olabilir. Dolayısıyla devletlerin, masum kazanımda bulunan üçüncü kişilerin dijital varlık ve diğer varlık üzerindeki haklarının birbirine paralel kalmasını sağlamak için özel bir mevzuatı yürürlüğe sokması gerekli bulunabilir.

BÖLÜM II: ULUSLARARASI ÖZEL HUKUK

İlke 5

Uygulanacak Hukuk

(1) Aşağıdaki fıkra (2) saklı kalmak üzere, bir dijital varlıklar bağlamındaki malvarlıksal mutlak haklarla ilgili konularda uygulanacak hukuk, aşağıda işaret edilen şekilde belirlenir:

(a) dijital varlık üzerinde açıkça belirtilen devletin ulusal hukuku ve eğer varsa yine dijital varlık üzerinde açıkça belirtilen İlkeler; veya bunların yokluğunda,

(b) dijital varlığın kaydedildiği sistemde açıkça belirtilen devletin iç hukuku ve varsa bu sistemde açıkça belirtilen İlkeler; veya bunların yokluğunda,

(c) ihraççısı olan bir dijital varlık bağlamında, aynı nitelikte bulunup bir ihraççısı olan dijital varlıklar da dahil olmak üzere, ilgili yasal merkezin kamuya açık şekilde kolayca tespit edilebiliyor olması şartıyla, ihraççının yasal merkezinin bulunduğu devletin ulusal hukuku; veya bunların yokluğunda,

(d) yukarıdaki bentlerin hiçbirinin uygulanmaması hâlinde:

Seçenek A:

(i) uyuşmazlığın görüldüğü mahkemenin bulunduğu yerdeki (forum) devletin(in) izin verdiği ölçüde, bu devletin ulusal hukukunun ilgili yönleri veya hükümleri;

(ii) (d)(i) bendi kapsamına girmeyen hususlar bakımından, forum devletinin belirlediği ölçüde İlkeler;

(iii) (d)(i) ve (d)(ii) bentleri kapsamına girmeyen hususlar bakımından, forum devletinin uluslararası özel hukuk kuralları uyarınca belirlenecek ulusal hukuk;

Seçenek B:

(i) forum devletinin belirlediği ölçüde İlkeler;

(ii) (d)(i) bendi kapsamına girmeyen hususlar bakımından, forum devletinin uluslararası özel hukuk kuralları uyarınca belirlenecek ulusal hukuk.

(2) Fıkra (1)'in yorumlanması ve uygulanmasında şu hususlar dikkate alınır:

(a) dijital varlıklar bağlamındaki malvarlıksal mutlak haklara ilişkin sorunlar, özellikle bunların kazanılması ve bunlar üzerinde yapılacak tasarruflar her zaman bir hukuk sorunu olarak değerlendirmeye alınır;

(b) uygulanacak hukukun dijital varlık dahilinde veya bu varlığın kaydedildiği sistemde belirtilip belirtilmediği değerlendirilirken, dijital varlığa ve bu varlığın kaydedildiği sisteme eklenmiş olan ya da bunlarla bağlantılı bulunan kayıtlar da, ilgili kayıtların dijital varlıkla işlem yapan kişiler tarafından kolayca incelenebilir olmaları şartıyla, özellikle dikkate alınmalıdır;

(c) bir dijital varlığı devralan, kazanan veya bu varlıkla ilgili işlemlerde bulunan kişi, (1)(a), (1)(b) veya (1)(c) bentleri uyarınca belirlenen hukuku kabul etmiş sayılır;

(d) fıkra (1) uyarınca belirlenen hukuk, aynı nitelikteki tüm dijital varlıklara uygulanır;

(e) bir dijital varlığın ilk kez ihracından veya meydana getirilmesinden sonra, (1)(a), (1)(b) veya (1)(c) bentleri uyarınca uygulanacak hukukun değişecek olursa, ilgili değişiklikten önce kazanılmış malvarlıksal mutlak haklar bu durumdan etkilenmez;

(f) (1)(c) bendinde bahsi geçen “ihraççı”,

(i) belirli bir dijital varlığı veya aynı türden dijital varlıkları, belirli bir değer karşılığında ticaret akışına sunan, ve

(ii) aşağıdaki bilgileri herkes tarafından kolayca tespit edilebilir biçimde açıklayan bir kişiye karşılık gelir:

(A) kendi ismini,

(B) yasal merkezini,

(C) belirli bir dijital varlığı veya aynı türden dijital varlıkları belirli bir değer karşılığında ticaret akışına sunan kişi olduğunu.

(3) Bir sözleşmenin saklama sözleşmesi niteliğinde olup olmadığı da dahil olmak üzere, İlke 10 ile İlke 13 arasında düzenlenen konular bakımından uygulanacak hukuk, ilgili sözleşmede açıkça belirtilmiş olan devletin ulusal hukuku veya eğer aynı sözleşmede başka bir ulusal hukuk tüm bu konular için geçerli olarak açıkça belirtilmişse, o ulusal hukuk olur.

(4) Fıkra (1) ve (2), fıkra (3) hükümlerine tabidir.

(5) Aşağıdaki hususlar bakımından uygulanacak hukuku belirleme yetkisi diğer hukuka aittir:

(a) dijital varlık üzerinde, kontrol dışında başka bir yöntemle üçüncü kişilere karşı ileri sürülebilir hâle getirilen bir teminat hakkının bu özelliğine uygulanacak hukuk,

(b) kontrol dışında başka bir yöntemle üçüncü kişilere karşı ileri sürülebilir hâle getirilen ve konuları itibariyle birbirleriyle çatışma içinde olan teminat hakları arasındaki öncelik sırasına uygulanacak hukuk.

(6) İflasla ilgili bir sürecin açılmasından bağımsız olarak ve fıkra (7) saklı kalmak üzere, bu İlke uyarınca belirlenen hukuk, iflas sürecinin başlamasından önce gerçekleşen durumlar bağlamında dijital varlıkları ilgilendiren tüm malvarlıksal mutlak hak sorunları bakımından uygulama alanı bulur.

(7) Fıkra (6), iflasla ilgili bir süreç nedeniyle uygulama alanı bulacak bir maddi hukuk veya usul hukuku kuralının uygulanmasını etkilemez, buna şu örnekler gösterilebilir:

(a) alacak kategorilerinin sıralamasına ilişkin kurallar,

(b) bir işlemin imtiyazlı sayılması veya alacaklıları yanıltmak amacıyla yapılan devirlerin iptaline ilişkin kurallar,

(c) iflas idaresinin kontrol veya denetimi altındaki bir malvarlığı değeri (varlık) üzerindeki hakların kullanılmasına ilişkin kurallar.

Açıklama

Genel

5.1. Bir kanunlar ihtilafı kuralının hiçbir zaman tam anlamıyla mükemmel olamayacağı, genel olarak kabul edilir. Bu nedenle İlke 5'in amacı, kanunlar ihtilafı konusuna ilişkin açıklığı ve hukuki öngörülebilirliği mümkün olan en yüksek düzeye çekmektir.

5.2. İlke 5, malvarlıksal mutlak haklara ilişkin hususlarda uygulanacak hukuku genel olarak ele almakta olup, yalnızca bu İlkeler kapsamında düzenlenenlerle de sınırlı değildir. Hangi

hususların “malvarlıksal mutlak haklara ilişkin hususlar” olarak nitelendirilecekleri, yargılama yerinin hukuku tarafından belirlenecektir. İlke 5’in bu geniş kapsamı, kapsam itibarıyla sınırlı olan bu İlkeler tarafından düzenlenen hususların, bu İlkeler kapsamı dışında kalan ancak onlarla yakından bağlantılı bulunan malvarlıksal mutlak haklara ilişkin hususları düzenleyen hukuktan farklı bir hukuka tabi olmasını önlemeyi amaçlamaktadır. Örnek olarak bkz. İlke 3(3)’te sayılan hususlar.

5.3. İlke 5 yalnızca uygulanacak hukukun seçimine ilişkin hususları düzenlemekte olup, herhangi bir yargı merciinin taraflardan biri veya uyuşmazlık konusu bakımından yargı yetkisine sahip olup olmadığı hususunu ele almamaktadır.

5.4. İlke 5, kanunlar ihtilafı kurallarında genellikle kullanılan bağlama noktalarının (örneğin kişilerin, işyerlerinin, faaliyetlerin veya malvarlığı değerlerinin bulunduğu yer) dijital varlıklar üzerindeki malvarlıksal mutlak haklara ilişkin hususlarda çoğu zaman faydalı bir rol oynamadığını kabul etmektedir. Gerçekten de, dijital varlıkların fiziki bir özelliğe sahip olmayan gayri maddi nitelikte varlıklar olmaları nedeniyle, bu tür bağlama noktalarının benimsenmesi (tanımlanabilir bir ihraççının bulunduğu sınırlı durum hariç olmak üzere, bkz. İlke 5(1)(c)) tutarsız olacak ve sonuca da elverişsiz mahiyet arz edecektir. Bunun yerine söz konusu İlke, yeni dijital varlıklar yaratan ya da mevcut dijital varlık sistemlerini yöneten kişilere, uygulanacak hukuku dijital varlığın kendisinde veya ilgili sistemle bağlantılı olarak belirlemeleri yönünde bir teşvik sağlamayı amaçlamaktadır. Bu yaklaşım, dijital varlıkların kendilerine özgü özelliklerini ve bu varlıklara ilişkin olarak ortaya çıkabilecek malvarlıksal mutlak hak sorunlarını dikkate almaktadır.

İlke 5(1)(a) ve 5(1)(b)

5.5. İlke 5(1), uygulanacak hukukun belirlenmesi için “kademeli” bir bağlama noktaları yapısı öngörmektedir. İlke 5(1)(a) uyarınca, uygulanacak hukuk, dijital varlığın üzerinde belirtilen devletin ulusal hukuku ve yine bu varlıklar üzerinde belirtilen İlkelerden oluşur. İlke 5(1)(a) uygulanamıyorsa, uygulanacak hukuk, dijital varlığın kaydedildiği sistemde belirtilen devletin hukuku ve yine bu sistemde belirtilen İlkelerden oluşur (İlke 5(1)(b)) (“sistem” kavramına ilişkin açıklamalar için bkz. Açıklama 5.6). İlke 5(1)(a) ve 5(1)(b)’deki kanunlar ihtilafı kuralları, Açıklama 5.4’te açıklanan nedenlerin yanı sıra, İlke 5(2)(c)’nin, bir dijital varlıkla işlem yapan ve malvarlıksal mutlak hakka ilişkin bir sorunun

çözümünden etkilenebilecek her bir kişinin İlke 5(1)'deki kanun seçimi kurallarını kabul etmiş sayması nedeniyle taraf iradesine dayanmaktadır (ayrıca bkz. Açıklama 5.16). Bu kişiler, uygulanacak hukukun belirlenmiş olduğunu bileceklerdir; zira bu husus, bu kişiler tarafından incelenmesi kolayca mümkün olan kayıtlarda yer alacaktır (bkz. İlke 5(2)(b) ve Açıklama 5.16). Ayrıca, günümüzde birçok dijital varlık veya sistem uygulanacak hukuku belirtmemekle birlikte, İlke 5(1)(a) ve 5(1)(b)'deki kurallar, böyle bir belirlemenin yapılması yönünde bir teşvik oluşturmaktadır. Taraf iradesine bu şekilde dayanılması, Uluslararası Ticari Sözleşmelerde Hukuk Seçimine İlişkin Lahey Konferansı İlkeleri'nin ("Lahey Konferansı İlkeleri") 3. maddesiyle uyumludur. Ayrıca, bir dijital varlık veya sistem, UNIDROIT İlkeleri'nin tamamının ya da bir kısmının (gerektiği ölçüde belirtilen ulusal hukukla tamamlanmak suretiyle) malvarlıksal mutlak haklara ilişkin hususlarda uygulanacak hukuk olduğunu da belirleyebilir.

5.6. İlke 5(1)(b)'de yer alan "sistem" kavramı, teknolojik açıdan tarafsız bir biçimde, geniş ve işlevsel olarak anlaşılmalıdır. Bu kavram, dijital varlıkların kaydedilmesine imkân tanıyan kapasiteye sahip olduğu ölçüde her türlü protokolü, platformu, uygulamayı, devir düzenlemesini ve ağı kapsamaktadır. Ağların genellikle katmanlı olarak inşa edildiği (örneğin fiziksel katman, veri bağlantı katmanı, ağ katmanı, taşıma katmanı, oturum katmanı, sunum katmanı ve uygulama katmanı) dikkate alındığında, bir dijital varlık, bir protokol üzerinde işleyen bir platforma dayanan bir uygulama içerisinde kaydedilebilir. Farklı katmanlar için farklı uygulanacak hukukların belirlenmiş olması mümkündür. Bu durumdan doğabilecek belirsizliği gidermek amacıyla, bir devlet ilgili hallerde hangi hukukun uygulanacağını belirleyen özel bir kural kabul etmeyi değerlendirebilir. Böyle bir kurala örnek olarak, dijital varlığa daha yakın özellikteki katman tarafından belirlenen hukukun üstün sayılması gösterilebilir. Hangi katmanın dijital varlığa daha yakın özellik taşıdığı, yetkili mahkeme tarafından tespit edilmesi gereken maddi bir olgudur. Bununla birlikte, uygulanacak hukukun dijital varlığın kendisinde belirtilmiş olması hâlinde (İlke 5(1)(a)), bu paragrafta ifade edilen belirsizlik ortaya çıkmayacaktır.

5.7. Yukarıda belirtildiği üzere, İlke 5(1), uygulanacak hukukun belirlenmesi için kademeli bir bağlama noktaları yapısı öngörmektedir. İlke 5(1)(a) uyarınca uygulanacak hukuk, dijital varlığın üzerinde belirtilen devletin ulusal hukukudur. Dijital varlık, uygulanacak hukuk olarak İlkelerin tamamını veya bir kısmını da belirleyebilir; bu durumda, belirtilen İlkeler, belirtilmiş olan ulusal hukuka üstün gelecektir (bkz. İlke 3(2)). Bununla birlikte, İlkelerin

tamamı belirtilmiş olsa dahi, İlkeler uyarınca başka bir hukuka tabi olan hususlar bakımından uygulanmak üzere bir ulusal hukukun da belirtilmesi gerekir. İlke 5(1)(a) uygulanamazsa, uygulanacak hukuk, dijital varlığın kaydedildiği sistemde belirtilen devletin ulusal hukuku ile birlikte, belirtilmişse İlkelerin tamamı veya bir kısmı olacaktır. Ne dijital varlığın kendisinde ne de kaydedildiği sistemde bir hukuk seçimi yapılmışsa, İlke 5(1)(c) uyarınca ihraççının devletin hukuku uygulanır. Bu şekilde belirlenen hukuk, yani ihraççının hukuku, yalnızca somut uyuşmazlığa konu olan belirli dijital varlığa değil, aynı zamanda “aynı tanıma sahip” tüm dijital varlıklara da uygulanır (bkz. İlke 5(2)(d)). “Aynı tanıma sahip” ifadesi, bu İlkeler bağlamında, piyasa katılımcıları tarafından misli olarak kabul edilen dijital varlıkları ifade eder. Ayrıca bkz. Açıklama 11.6.

İlke 5(1)(c)

5.8. İlke 5(1)(c), yani İlke 5 tarafından öngörülen kademeli yapının üçüncü basamağı, sınırlı bir uygulama alanına sahiptir. Bu sınırlılık, ilk olarak, tüm dijital varlıkların bir ihraççısının bulunmamasından kaynaklanmaktadır (İlke 5(2)(f)’de tanımlandığı üzere; bkz. Açıklama 5.10). Bu tür durumların tamamında bu kural uygulanmaz ve uygulanacak hukuk İlke 5(1)(d) uyarınca belirlenir. Bununla birlikte, tipik olarak ihraç edilen dijital varlıklara ilişkin örnekler için bkz. Açıklama 4.23–4.28.

5.9. İkinci olarak, ihraççıya dayanan bağlama noktası birden fazla şekilde nitelendirilmiştir. Özellikle, İlke 5(1)(c), ihraççının yasal merkezinin bulunduğu devlete atıfta bulunmaktadır. Bir ihraççının yerinin belirlenmesi gerektiğinde, yasal merkez, üçüncü kişiler tarafından en kolay şekilde tespit edilebildiği için en yüksek düzeyde hukuki kesinlik sağlayan bağlama noktasıdır. “Merkezi yönetim yeri”, “esas işyeri” veya “asli menfaat merkezi” gibi diğer olası bağlama noktaları aynı derecede kesinlikle tespit edilemez ve bu nedenle gereksiz bir belirsizlik yaratır. İlke 5(1)(c) uyarınca, ihraççının yasal merkezinin “kamu tarafından kolayca tespit edilebilir” olması gerekir. Örneğin, ihraççı, adi ortaklık gibi yasal merkezi bulunmayan gayri resmî bir yapı ise, İlke 5(1)(c) anlamında kamu tarafından kolayca tespit edilebilir bir yasal merkez mevcut olmayacaktır. Ayrıca, belirli bir dijital varlığın farklı kişiler tarafından veya farklı katmanlarda ihraç edilmesi nedeniyle hangi ihraççı tarafından ihraç edildiğinin belirsiz olması hâlinde bu dijital varlığın ihraççısının kanuni merkezi kamu tarafından kolayca tespit edilebilir

olmayacaktır. Bu tür durumların tamamında İlke 5(1)(c) uygulanmaz ve uygulanacak hukuk İlke 5(1)(d) uyarınca belirlenir.

5.10. Üçüncü olarak, “ihraççı” kavramı İlke 5(2)(f)’te tanımlanmış olup, bir kişinin ihraççı olarak nitelendirilebilmesi için en az beş kümülatif ölçütü sağlaması gerekir. İlk olarak, bir kişinin ihraççı olarak kabul edilebilmesi için tüzel kişi olması gerekir. Bu nedenle gerçek kişiler, bu İlkeler kapsamında “ihraççı” olarak nitelendirilemez. Bu ölçüt, İlke 5(1)(c)’de ihraççının yasal merkezine atıfta bulunulmasından da çıkarılabilir; zira yasal merkez kavramı mantıken yalnızca tüzel kişiler bakımından söz konusu olabilir. Ayrıca, İlke 5(1)(c), İlke 5(2)(f)’nin giriş kısmıyla birlikte değerlendirildiğinde, ilgili ihraççı tüzel kişi niteliğini taşımıyorsa (örneğin, adi ortaklığın uygulanacak hukukta tüzel kişilik olarak tanınmaması hâlinde), İlke 5(1)(c)’nin uygulanamayacağı sonucuna varılmalıdır. Buna benzer tüm durumlarda uygulanacak hukuk İlke 5(1)(d) uyarınca belirlenir. İkinci olarak, ihraççı, İlke 5(2)(f)(i) uyarınca dijital varlığı veya aynı tanıma sahip dijital varlıkları bedel karşılığında ticari dolaşıma sokmuş olmalıdır. Bu ölçüt, bir kişinin dijital varlığı yaratmasına rağmen onunla ilgili herhangi bir ticari menfaatinin bulunmadığı durumları kapsam dışı bırakmayı amaçlamaktadır. “Aynı tanıma sahip” kavramı hakkında bkz. Açıklama 5.17 ve Açıklama 11.6. Üçüncü olarak, ihraççı sayılabilmek için kişinin, İlke 5(2)(f)(ii)(A) uyarınca, adını kamu tarafından kolayca tespit edilebilir şekilde açıkça belirtmiş olması gerekir. Bu, ihraççının adının üçüncü kişiler tarafından kolayca tanımlanabilir olması gerektiği anlamına gelir. Dördüncü olarak, ihraççı, İlke 5(2)(f)(ii)(B) uyarınca kanuni merkezini kamu tarafından kolayca tespit edilebilir şekilde belirtmiş olmalıdır. Bu ölçüt, kendiliğinden anlaşılabilir açık bir mahiyet taşımaktadır. Son olarak, ihraççı, İlke 5(2)(f)(ii)(C) uyarınca, dijital varlığı veya aynı tanıma sahip dijital varlıkları bedel karşılığında ticari dolaşıma sokan kişi olduğunu kamu tarafından kolayca tespit edilebilir şekilde beyan etmiş olmalıdır. Bu, ihraççının yalnızca fiilen dijital varlığı bedel karşılığında ticari dolaşıma sokmuş olmasının (İlke 5(2)(f)(i) anlamında) yeterli olmayacağı; aynı zamanda kendisini bu sıfatla açıkça tanımlamış olmasının da gerektiği anlamına gelir. Bir kişi, İlke 5(2)(f) uyarınca ihraççı olarak nitelendirilebilmek için gerekli ölçütlerin herhangi birini (ya da tamamını) sağlamıyorsa, uygulanacak hukuk İlke 5(1)(d) uyarınca belirlenir.

İlke 5(1)(d)

5.11. Kademeli yapının en alt basamağında, İlke 5(1)(a) ve İlke 5(1)(b)’de öngörüldüğü üzere dijital varlıkta veya sistemde bir hukuk seçimi yapılmamış olması ve İlke 5(1)(c)’nin de uygulanmaması hâlinde, İlke 5(1)(d), ilgili devlete, o devlet bünyesinde faaliyet gösteren bir yargı mercii bakımından uygun kuralları belirleme konusunda geniş bir takdir yetkisi tanımaktadır. Bu bağlamda temel bir husus, birçok durumda dijital varlığın herhangi bir devletle anlamlı bir bağlantısının bulunmayabileceği gerçeğidir. Dijital varlıklar üzerindeki malvarlıksal mutlak hak sorunlarında yargı merciinin uygulayacağı tek tip ve her duruma uyan bir yaklaşımın İlke 5(1)(d)’de öngörülmesi mümkün değildir. Bu nedenle İlke 5(1)(d), iki alternatif seçenek (Seçenek A ve Seçenek B) öngörmektedir; her iki seçenek de, bu tür sorunlara yargılama yeri devleti tarafından belirlenecek ölçüde İlkelerin tamamının veya bir kısmının uygulanmasını içerir. Bu İlkeler, uluslararası düzeyde tarafsız ve dengeli bir kurallar bütünü olarak genel kabul gördüğünden, kademeli yapının en alt basamağında uygulanmaları uygundur (bkz. Lahey Konferansı İlkeleri’nin 3. maddesi; bu madde, tarafların yalnızca bir devlet hukukunu değil, aynı zamanda devlet dışı kaynaklardan doğan “hukuk kurallarını” da seçebilmelerine imkân tanımaktadır). Vurgulanmalıdır ki, her bir seçenek özelinde uygulanacak İlkeler, yalnızca yargılama yeri devleti tarafından açıkça belirlenenlerdir.

5.12. İlke 5(1)(d) kapsamındaki her bir seçenek içinde, İlke 5 kabul edilirken devlet tarafından yapılan belirlemelere dayanan alt kademeli bir yapı öngörülmektedir.

Seçenek A

5.13. Seçenek A, bir devletin, kendi ülkesinde faaliyet gösteren yargı merciinin, dijital varlıklar üzerindeki malvarlıksal mutlak haklara ilişkin hususlarda kendi ulusal hukukunun bazı yönlerini uygulamasını uygun görmesi hâlinde tercih edilmeye elverişlidir. Bu durum, örneğin devletin dijital varlıklar üzerinden malvarlıksal mutlak haklara ilişkin hususları özel olarak düzenleyen bir mevzuatı kabul etmiş olması hâlinde söz konusu olabilir. Buna somut bir örnek, devletin bu İlkelerin bazı bölümlerini ulusal hukukunun bir parçası olarak benimsemiş olmasıdır. Yargılama yeri devleti tarafından belirtilen bu ulusal hukuk hükümleri, kademeli yapının ilk basamağını oluşturur (Seçenek A kapsamında İlke 5(1)(d)(i)). Kademeli yapının ikinci basamağı (Seçenek A kapsamında İlke 5(1)(d)(ii)),

Seenek A'nın İlke 5(1)(d)(i) hükmüyle düzenlenmeyen hususlara ilişkindir ve yargılama yeri devletinin tercihine ve buna baėlı olarak yaptığı belirlemeye göre İlkelerin tamamından, bazı İlkelerden veya İlkelerin bazı yönlerinden oluşur. Kademeli yapının üçüncü basamağı (Seenek A kapsamında İlke 5(1)(d)(iii)) ise, diėer hükümlerle düzenlenmeyen ölçüde, yargı merciinin kendi milletlerarası özel hukuk kuralları uyarınca uygulanacak hukuku tatbik etmesini gerektirir.

Seenek B

5.14. Seenek B, Seenek A'da öngörülen kademeli yapının ikinci ve üçüncü basamaklarından oluşmaktadır. Bu nedenle Seenek B, dijital varlıklar üzerindeki malvarlıksal mutlak haklara ilişkin hususların, maddi hukuk kuralı mahiyetindeki ulusal hukuk kurallarına herhangi bir atıf yapılmaksızın, yalnızca İlkeler veya bunların belirli bölümleri uyarınca çözümlenmesi gerektiğine karar veren bir devlet bakımından uygun bir seçenektir. Bu durum, özellikle devletin dijital varlıklar üzerindeki malvarlıksal mutlak haklara ilişkin hususları özel olarak düzenleyen bir mevzuat kabul etmemiş olması hâlinde söz konusu olabilir. Bu bağlamda da uygulanacak İlkeler, yargılama yeri devleti tarafından belirtilen İlkelerdir. Kademeli yapının üçüncü basamağı ise, Açıklama 5.13'te açıklandığı şekilde uygulanır.

5.15. Bu İlkelere yapılan atıf yoluyla, İlke 5(1)(d), İlke 5(1)(a), 5(1)(b) veya 5(1)(c)'nin uygulanamadığı durumlarda, yargılama yerinin yetkisi altındaki kişiler ve hususlar bakımından İlkeleri benimsemesine imkân tanıyan yenilikçi bir yöntem sunmaktadır. İlke 5'in kabulü, yargılama yerinin bu gibi durumlarda İlkeleri uygulama yönündeki iradesini karşılayacaktır. Özellikle yargılama yeri, normalde yargılama yeri devletinin maddi hukukunun uygulanacağı hâllerde dahi, uygulanması gereken yerel özel hukukun esaslı biçimde değiştirilmesini gerektirecek potansiyel gecikme ve karmaşıklıklara yol açmaksızın İlkeleri uygulayabilecektir. Nitekim bir yargılama yeri devleti bu yaklaşımı, İlkeleri benimsemenin birincil yolu olarak veya tam anlamıyla kabul edilmesine kadar geçici bir çözüm olarak tercih edebilir. Elbette, ilgili dijital varlık veya sistem, yargılama yeri devletinin maddi hukukunu belirtmişse (ve bu hukuk İlke 5(1)(a) veya 5(1)(b) uyarınca uygulanacaksa), yargılama yeri devletinin bu İlkelerde örneklenen nitelikte kabul edilebilir maddi kuralları benimsemiş olduğu makul biçimde varsayılabilir. İlke 5, bir devlete, kendi

politika tercihleriyle uyumlu ve ulusal hukuku ile bağdaşan kanunlar ihtilafı kuralları oluşturma konusunda geniş bir esneklik tanımaktadır.

İlke 5(2)

5.16. İkinci fıkra, İlke 5(1)'in yorumlanması ve uygulanmasına ilişkin ilave rehberlik sağlamaktadır. İlke 5(2)(a), malvarlıksal mutlak haklara ilişkin hususların; (i) ilgili ağdaki katılımcıların herhangi bir hukukun uygulanmasını reddederek münhasıran koda dayanmak istemeleri ve (ii) teknolojinin niteliği veya ağın uluslararası karakteri nedeniyle hukukun uygulanmasının aşırı derecede karmaşık olduğu, belirsiz sonuçlar doğurduğu veya ağın işleyişini bozduğu iddia edilse dahi, hukuka tabi olduğunu teyit etmektedir. İlke 5(2)(b), dijital varlıkta veya sistemde uygulanacak hukukun belirlenmesinin, dijital varlığa veya sisteme eklenmiş ya da bunlarla bağlantılı olan kayıtların (elektronik veya diğer yollarla kaydedilmiş bilgiler anlamında) incelenmesi suretiyle yapılabileceğini açıkça ortaya koymaktadır; ancak bu kayıtların, dijital varlıkla ilgili işlem yapan kişiler bakımından kolayca erişilebilir olması şarttır. Bu kayıtları inceleyebilecek durumda olan ve dijital varlıkla ilgili işlem yapan kişiler, bu işlem yapma olgusunun sonucu olarak, belirtilen uygulanacak hukuka rıza göstermiş sayılırlar; bu sonuç İlke 5(2)(c) hükmünden doğmaktadır.

5.17. İlke 5(2)(d) ve İlke 5(2)(e)'nin birlikte etkisi, belirlenen uygulanacak hukukun, dijital varlığın meydana getirildiği veya ihraç edildiği andan itibaren aynı tanıma sahip tüm dijital varlıklara uygulanması; ancak bu hukukun daha sonraki bir tarihte değişiklik göstermesi hâlinde, dijital varlık üzerindeki mevcut hakların bundan etkilenmemesinde kendilerini gösterir. Aynı tanıma sahip tüm dijital varlıkların aynı uygulanacak hukuka tabi olması özellikle önemlidir. Uygulanacak hukukta değişikliklerden mümkün olduğunca kaçınılmalıdır. Böyle değişikliklerin ortaya çıkması hâlinde ise, tüm bu dijital varlıkların her zaman aynı hukuka tabi olmasını güvence altına alan geçiş hükümlerinin kabul edilmesi zorunlu olacaktır. İlke 5(2)(f), Açıklama 5.10'da ele alınmıştır.

İlke 5(3) ve İlke 5(4)

5.18. İlke 5(3) ve İlke 5(4), İlke 5(1)'in, bir saklayan ile müşterisi arasındaki ilişkiye uygulanacak hukuku belirlemediğini açıkça ortaya koymaktadır. Bu husus, İlke 5(3)'te yer

alan kanunlar ihtilafı kuralı uyarınca belirlenir; buna göre uygulanacak hukuk, saklama sözleşmesinin bu sözleşmeye uygulanacağını açıkça belirttiği hukuktur veya, eğer farklı ise, İlke 10 – 13’te düzenlenen hususlara uygulanacağı açıkça belirtilen hukuktur. Bu kural, söz konusu hususlar bakımından genellikle tek bir hukukun uygulanması sonucunu doğuracaktır. İlke 5(1)(a) ve 5(1)(b) kapsamında farklı dijital varlıklarda veya farklı sistemlerde farklı hukukların belirlenebilmesi ihtimaline karşılık, saklama ilişkisine tek bir hukukun uygulanması uygun görülmektedir.

5.19. İlke 5(3)’te öngörülen özel kanunlar ihtilafı kuralı, bir saklayan ile müşterisi arasındaki ilişkide uygulanacak hukuku belirlemekte olup, kapsamı sınırlıdır. Bu kural yalnızca, sözleşmenin bir saklama sözleşmesi olup olmadığı da dâhil olmak üzere, İlke 10 – 13’te ele alınan hususlara ilişkindir. İlke 13, bir saklayanın iflasla bağlantılı bir usule tâbi olması hâlinde ortaya çıkan hususları düzenlemektedir. İlke 5(6) ve İlke 5(7)’de de görüldüğü üzere, İlke 5(3)’teki kanunlar ihtilafı kuralı, İlke 10 – 13’te düzenlenen sözleşmesel ve malvarlıksal mutlak haklara ilişkin hususlar bakımından uygulanmakta; buna karşılık iflas hukukuna ilişkin hususlar, uygulanabilir iflas hukuku tarafından yönetilmektedir.

5.20. İlke 5(3)’te yer alan kanun seçimi kuralı kapsamındaki hususlar, genel çerçevede özel hukuka ilişkin hususlar olarak kabul edilmektedir. Bu nedenle söz konusu kural, saklayan – müşteri ilişkisini ilgilendirebilecek herhangi bir düzenleyici mahiyetteki hukuk kuralının (regülasyon) uygulanmasını bertaraf etmez. Bu türden düzenleyici kurallara örnekler için bkz. Açıklama 10.21. Ayrıca, bir saklayan düzenleyeci kurallara tabi bir kuruluş olabilir ve düzenleyici otoriteler, saklama sözleşmesi veya İlke 10 – 13’te ele alınan hususlar bakımından saklayanın hukuk seçimini sınırlandırmak isteyebilir. İlke 5(3), saklayanın hukuk seçimini kısıtlayan bu tür düzenleyici hukuk kurallarını ortadan kaldırmamaktadır.

5.21. Saklama ilişkisinin İlke 5(1) ve İlke 5(2)’nin uygulanma alanı dışında bırakılması, bu İlkelerin, bir saklayanın bir dijital varlığı kazanımı veya elden çıkarması gibi malvarlıksal mutlak haklara ilişkin hususlarda uygulanmayacağı anlamına gelmemektedir.

İlke 5(5)

5.22. İlke 5(5), İlke 5(1)’de benimsenen yaklaşımın, bir rehin veya teminat hakkına ilişkin kayıt sistemini yöneten hukukun belirlenmesi bakımından uygun olmadığını kabul

etmektedir. Zira böyle bir sistem, sicili inceleyen üçüncü kişiler tarafından tespit edilebilecek nesnel göstergelere (örneğin teminat verenin bulunduğu yer) dayanmalıdır.

5.23. Açıklama 5.22’de belirtilen gerekçeyle, İlke 5(5), bir dijital varlık üzerindeki teminat hakkının, üçüncü kişilere karşı kontrol dışındaki bir yöntemle ileri sürülebilir hâle getirildiği durumlarda, üçüncü kişilere karşı ileri sürülebilirliğe uygulanacak hukukun başka hukuk tarafından (bu bağlamda, başka hukukun içerdiği kanunlar ihtilafı kuralları aracılığıyla) belirleneceğini öngörmektedir. Ayrıca, bu tür teminat hakları arasında öncelik meselesinin de aynı hukuka tâbi olması gerektiğinden, İlke 5(5), birden fazla çatışan teminat hakkı arasındaki önceliğin belirlenmesine uygulanacak hukukun da yine başka hukuk tarafından belirleneceğini düzenlemektedir. Buna karşılık, çatışan teminat haklarından biri, üçüncü kişilere karşı kontrol yoluyla ileri sürülebilir hâle getirilmişse (aynı zamanda kontrol dışındaki bir yöntemle de ileri sürülebilir hâle getirilmiş olsa dahi), uygulanacak hukukun belirlenmesi bakımından İlke 5(1) uygulanacaktır. Ayrıca bkz. Açıklama 16.5.

Bağlantılı Varlıklar

5.24. Bir dijital varlığın başka bir varlıkla bağlantılı olması veya bağlantılı olduğu iddiasında bulunulması hâlinde, dijital varlık ile diğer varlık arasındaki bağlantının varlığının, şartlarının ve hukuki etkilerinin belirlenmesine uygulanacak hukuk, başka hukuk tarafından (bu bağlamda, başka hukukun içerdiği kanunlar ihtilafı kuralları aracılığıyla) belirlenir. Bu hususlar, İlke 4 uyarınca başka hukuk tarafından tayin edilir.

İlke 5(6) ve İlke 5(7)

5.25. İlke 5(6), iflasla bağlantılı bir yargılama sürecinde, iflas sürecinin açılmasından önce meydana gelen olaylara ilişkin olarak dijital varlıklar bakımından ortaya çıkan malvarlıksal mutlak haklara ilişkin hususlarda İlke 5’in uygulanacağını açıkça ortaya koymaktadır. İlke 5(7) ise, iflasa uygulanacak hukuka öncelik tanıyan olağan istisnaları düzenlemektedir. Bu istisnalar, Açıklama 19.9 – 19.12’de ele alınmıştır. İlke 5(7)(c)’de geçen “kontrol” teriminin, İlke 6’da tanımlanan anlamda değil, geniş anlamda kullanıldığına dikkat edilmelidir (bkz. Açıklama 19.4).

BÖLÜM III: KONTROL VE DEVRİ

İlke 6

Kontrol

(1) Aşağıdaki koşullar bir arada sağlandığında, bir kişinin bir dijital varlık üzerinde “kontrol” sahibi olduğu kabul edilir:

(a) fıkra (2) ve (3) saklı kalmak üzere, eğer söz konusu dijital varlık veya ilgili protokol ya da sistem, o kişiye:

(i) başkalarının bu dijital varlıktan esaslı biçimde tüm yararları elde etmelerini engelleme münhasır yetkisini;

(ii) bu dijital varlıktan esaslı biçimde tüm yararları elde etme yetkisini; ve

(iii) (i) ve (ii) alt bentlerindeki yetkileri, başka bir kişiye devretme münhasır yetkisini veriyorsa; ve

(b) dijital varlık veya ilgili protokol ya da sistem, bu kişinin yukarıda bent (a)’da sayılan yetkilere sahip olduğunu tanımlamasına imkân veriyorsa.

(2) “Kontrol değişikliği”nden, bir dijital varlık üzerindeki (1)(a) bendindeki yetkilerin başka bir kişiye devri anlaşılır ve bu ifade dijital varlığın değiştirilmesini, yok edilmesini, iptal edilmesini veya ortadan kaldırılmasını, ayrıca bunun sonucunda ortaya çıkan ve başka bir kişinin kontrolü altına giren yeni bir dijital varlığın (“türeme yoluyla ortaya çıkan dijital varlık”) meydana getirilmesini de kapsar.

(3) (1)(a) bendinde öngörülen yetkilerin aşağıda sayılan durumlarda münhasır özellikte olmaları aranmaz:

(a) dijital varlık veya ilgili protokol ya da sistem, dijital varlığı kullanımını sınırlandırıyor ya da kontrol değişikliği veya kaybı da dahil olmak üzere dijital varlık üzerinde değişiklikler meydana getirmeye programlanmış ise;

(b) kontrol sahibi konumunda bulunan kişi, sayılan yetkilerini bir veya birden fazla kişiyle paylaşmayı kabul etmiş yahut da ilgili duruma açıkça veya örtülü olarak rıza göstermiş ise.

Açıklama

Genel

6.1. Bu İlkeler dahilinde “kontrol” kavramı son derece büyük bir önemi haiz bulunmaktadır. İlke 6, dijital varlık üzerindeki kontrolün ayrıntılı bir tanımını içerir. Kontrol, esasen olgusal (fiili) bir durumdur ve malvarlıksal mutlak haktan bağımsızdır; bununla birlikte İlkeler kapsamında belirli hukuki sonuçların doğması için kontrol aranır (örnek olarak masum kazanımda bulunanın korunması veya üçüncü kişilere karşı ileri sürülebilirlik özelliğinin kazanılması için durum böyledir). İlke 6(1)(a)’daki münhasır yetkiler (İlke 6(3) ile esnetildiği ölçüde), malvarlıksal mutlak hakların ayrılmaz unsuru olan “başkalarını dışlama” özelliğini yansıtır.

6.2. İlke 6(1)(a)’daki münhasır yetkiler, kontrolün taşınır mallardaki “zilyetlik” kavramına işlevsel bir denklige sahip olduğunu farz etmektedir. Ancak burada “zilyetlik” hukuki değil, yalnızca fiili bir durum olarak kabul edilir. Dijital varlık maddi olmayan bir öge teşkil ettiğinden, bu denkliğin yalnızca dijital varlık üzerindeki hâkimiyet boyutunu kapsadığı ve fiziksel yer boyutunu içermediği belirtilir. Kontrolün var olup olmadığı olgusaldır, hukuki yorumda bulunulmasını gerektirmez. Ancak kontrolün varlığı belirli hukuki sonuçları meydana getirir. Dijital varlıkları kazananlar, bu varlık üzerinde münhasır yetkilere (istisnalar saklı kalmak üzere) sahip olacaklarına inanır ve bunu bekler.

6.3. Kontrol kavramının bu İlkeler dahilindeki anlamı, bazı hukuk sistemlerinde “zilyetlik” olarak adlandırılan kavramıninkinden farklıdır. Bazı hukuk sistemlerinde zilyetlik hukuki bir statüdür ve başkası aracılığıyla kullanılabilir. Oysa burada kontrol, tamamen fiili bir durumdur ve İlke 6’da yer verilen ölçütler sağlanmadıkça bir kişi dijital varlık üzerinde kontrol sahibi sayılmaz. Saklama ilişkisi bakımından ayrıca bkz. İlke 10.

6.4. Dijital varlıkları düzenleme altına alan bir hukuk sisteminde kontrol kavramı, bir dijital varlığı masum kazananın (saklama ilişkisi kapsamındaki müşteri haricinde) korunmasında, üçüncü kişilere karşı ileri sürülebilirlik özelliğinin kazanılmasında ve teminat hakları arasındaki önceliğin belirlenmesinde işlev gösteren bir ölçüttür. Devletler, daha genel olarak malvarlıksal mutlak hakların üçüncü kişilere karşı ileri sürülebilir olmasının sağlanması bakımından kontrol kavramını kullanmayı tercih edebilir. Kontrol

(İlke 6’da tanımlandığı haliyle), aynı zamanda dijital varlığın tanımlanmasında kullanılan bir unsur olma özelliğini gösterir. İlke 2(2) uyarınca, kontrol altına alınabilir olmayan bir elektronik kayıt, İlkeler çerçevesinde “dijital varlık” sayılmaz.

6.5. Kontrolün bir kişiden bir başkasına aktarılması ile dijital varlık üzerindeki malvarlıksal mutlak hakkın devri birbirinden ayrıdır. Bkz. “devir” kavramını tanımlayan İlke 2(5). Bir dijital varlık üzerindeki malvarlıksal mutlak hakkın geçerli şekilde devredilip devredilmediği hususu, diğer hukuk çerçevesinde belirlenir ve bu İlkelerin kapsamına girmez (bkz. İlke 3(3) ve Açıklama 2.26). Çoğu durumda malvarlıksal mutlak hakkın devri, kontrol değişikliğiyle birlikte gerçekleşse de, bazı durumlarda böyle olmayabilir. Örnek olarak bir devletin hukuku, belirli koşullar altında bir dijital varlık üzerindeki malvarlıksal mutlak hakkın (uygulanacak ulusal hukukta tanımlandığı haliyle) bir başkasına aktarılabilceğini, ancak kontrolün devredende kalmaya devam edebileceğini de öngörebilir. Tam tersine, bazı hallerde ve uygulama alanı bulacak diğer hukuk çerçevesinde, kontrol değişikliği malvarlıksal mutlak hakların devredilmesi sonucunu meydana getirmeyebilir. Örneğin bir saklayan (İlke 10(1)’de tanımlandığı şekilde), bir müşterisi için dijital varlığı kontrol edebilir ama hukuken o dijital varlık üzerindeki malvarlıksal mutlak hakka (uygulanacak ulusal hukukta tanımlandığı haliyle) sahip olmayabilir. Bu açıklama, dijital varlık üzerindeki kontrolün zilyetliğin işlevsel dengini teşkil eden bir kavram olduğu düşüncesini yansıtır. Kontrol değişikliği ile malvarlıksal mutlak hakların devri arasındaki bu ayrımı vurgulamak amacıyla bu İlkelerde “teslim”, “kontrolün teslimi” veya benzeri ifadelerle yer verilmemiş, bunun yerine “kontrol değişikliği” ifadesinin kullanılması tercih edilmiştir. “Kontrol değişikliği” İlke 6(2)’de tanımlanmış olup, bu kavramla ilgili iki örnek duruma Açıklama 6.14-6.17 altında yer verilmiştir.

6.6. Bir temsilci (örneğin bir çalışanın işveren adına kontrol sağlaması gibi) dijital varlık üzerinde kontrol sağladığında, bu İlkelerde temsil hukukunun bir uygulama sonucu olarak kontrolün asıl kişide olduğu kabul edilir. Kontrol, aynı zamanda dijital varlıkların saklanması bakımından da önem taşır. İlke 10’da düzenlendiği üzere, saklama sözleşmesi kapsamındaki hizmet sağlayan (saklayan), müşterileri için dijital varlıklar üzerinde kontrolü kendinde tutabilir ya da bir alt saklama sözleşmesi üzerinden alt saklayanın dijital varlıkları kendisi için kontrol etmesini sağlayabilir, bu suretle de dijital varlıkları muhafaza etme yükümlülüğünü yerine getirmiş olur. Bu durum da, malvarlıksal mutlak

hak ile kontrolün ayrılabileceğinin tipik bir örneğidir. Bir dijital varlığı çalan (haksız biçimde elde eden) bir kişi de benzer şekilde kontrolü ele geçirebilir, ama bu şekilde o dijital varlık üzerindeki malvarlıksal mutlak hakkı kazanmış olmaz. Bu da kontrol ve malvarlıksal mutlak hakkın ayırt edilmesinde başka bir örnek oluşturur.

Kontrol sahibinin “yetkisi”

6.7. İlke 6’da “erk” terimi yerine “yetki” terimi tercih edilmiştir. Bu iki terim benzer anlamları taşısa da, “yetki” fiili bir duruma daha iyi işaret eder; “erk” kelimesinin ise daha çok “hukuki” bir çağrışımının bulunduğu söylenebilir. İlgili yetkilerin münhasırlık özelliği bakımından ayrıntılar için bkz. Açıklama 6.10–6.12.

6.8. İlke 6(2), kontrol değişikliğinin, türev bir varlıkla ilgili olduğu durumu ele almaktadır, zira bu türev dijital varlık kontrolünün bırakıldığı dijital varlıktan farklıdır. Bu türden bir türev dijital varlığa örnek olarak Bitcoin’i ilgilendiren işlemlerde işlem sonucunda ortaya çıkan harcanmamış işlem çıktısı (UTXO) gösterilebilir. Bir diğer örnek ise, Ethereum platformunda ether işlemleri sonucunda hesap bakiyeleri üzerinde yapılan ayarlamalardır. İlgili durumda kontrol, farklı misli varlıklar üzerinde bırakılıp yeniden kazanılmaktadır.

6.9. Yukarıda da ifade edildiği üzere, İlke 6(1)(a)’daki münhasırlık (İlke 6(3) ile esnetildiği ölçüde), malvarlıksal mutlak haklarına içkin başkalarını dışlama unsurunu yansıtır. Ancak bir kişinin (meşru biçimde kontrolü elinde tutan bir kişiden farklı olarak) meşru kontrol sahibinin rızası olmaksızın bu yetkileri elde etmesi de mümkündür, örneğin bir özel anahtarın bu anahtarın kayıtlı bulunduğu aygıtın (cihazın) bilgisayar korsanlığı, bulunma veya hırsızlık yoluyla ele geçirilmesi gibi olasılıklar düşünölsün. Bu durum, kontrol değişikliğinin malvarlıksal mutlak hak devrinden ayrı olduğunu gösterir. Kontrol, masum kazanım (İlke 8) ve üçüncü kişilere karşı ileri sürülebilirlik (İlke 15) için bir koşul oluşturması ve bir kişinin dijital varlık üzerindeki kontrolü elinde bulunduran kişinin duruma göre bu varlık üzerinde malvarlıksal mutlak hak sahibi konumunda bulunmasının bir zorunluluk arz etmemesi yönlerinden zilyetlikle işlevsel denklik gösterir, ancak iki kavram arasında ciddi farklılıklar bulunmaktadır.

Yetkilerin münhasırlığı

6.10. İlke 6(1)(a)(i) ve 6(1)(a)(iii)’te öngörülen münhasır yetkiler, dijital varlıklar için güvenilir bir sistemin bu yetkileri ve bunların münhasırlığını sağlayabildiği varsayımına dayanır. Ancak böyle bir sistemin kötü niyetli bir bilgisayar korsanlığı girişiyle -böyle bir girişim gerçekleşmiş olsa bile- bozulması ihtimali münhasırlığı ortadan kaldırmaz. Söz konusu ihtimal, dijital varlıkların doğasında bulunan -ne yazık ki talihsiz- bir risktir (tıpkı fiziksel bir eşyanın zilyetliğinin bir başkası tarafından haksız olarak ele geçirilmesi durumunda olduğu gibi). Uygulamada, böyle bir bilgisayar korsanlığı girişimi, genelde kötü niyetli kişinin hızlıca kontrolü devralmasıyla sonuçlanır. Bkz. Açıklama 7.2. Ayrıca, bir başka kişi meşru kontrol sahibinin rızası olmadan bu yetkileri elde etse bile, meşru kontrol sahibi gerekli yetkileri kaybetmediği sürece kontrolü elinde tutar. Meşru kontrol sahibi, diğer kişi bu yetkileri (örneğin bir dijital varlıkla ilgili özel anahtarı ele geçirerek) elde etse bile, kontrol onun (diğer kişi) tarafından bir başkasına devredilmedikçe kontrolde kalmaya devam edecektir. Diğer kişi, bu yetkileri masum bir şekilde ve kontrolü devretme yönünde herhangi bir amacı ve sebebi olmadan elde etmiş olabilir. Buna karşılık ilgili yetkileri hukuka aykırı biçimde elde eden kişi, meşru kontrol sahibinin dijital varlık üzerinde işlem yapma yetkisini korumasına seyirci kalmaz. Yani dijital varlığı bu şekilde hukuka aykırı olarak elde eden kişinin kontrolü derhal bir başkasına devretmesi kuvvetle muhtemeldir. Meşru kontrol sahibi, diğer kişinin bu yetkileri elde ettiğini öğrendiğinde ise, duruma göre ya çıkarlarını korumak amacıyla kontrolü bir başkasına devredecek ya da kişinin kendisiyle birlikte kontrolde olmasını örtülü olarak kabullenecektir. Bu nedenle, meşru kontrol sahibinin açık veya zımni onayı olmadan diğer bir kişiyle paylaşılan “birlikte kontrol” durumu ancak çok kısa bir süre için devam edebilir.

6.11. İlke 6(3), İlke 6(1)(a)’daki münhasırlık şartlarının bazı durumlarda esnetilmesine imkân tanır. İlke 6(3)(a), kontrol değişikliği de dahi olmak üzere, dijital varlığın veya içinde bulunduğu sistemin özellikleri gereği kendiliğinden ortaya çıkan sınırlamaları ve kontrol sahibinin sahip olduğu yetkilerin münhasırlığına istina oluşturan değişikliklere yol veren durumları ele almaktadır. İlke 6(3)(b) ise kontrol sahibinin, güvenlik veya başka amaçlarla yetkilerini başka kişilerle paylaşabileceğini kabul eder. Örneğin çoklu imza (*multi-sig*) kurgularında, bir kişi İlke 7(1)(b) uyarınca kimliğini belirleyebiliyorsa, ilgili yetkiler bir başkasıyla paylaşılsa bile yine de kontrol sahibi olabilir. Bu durum, diğer kişinin fiili, ilgili bir yetkinin kullanılmasının koşulu olsa bile geçerlidir. Bkz. Açıklama 6.13’teki Örnek

Durum 1. Bir diğerk örnek ise, özel anahtarın birkaç parçaya bölündüğü ve herhangi bir işlemin gerçekleştirilebilmesi için tüm parçaların bir arada gerekli olduğu çok taraflı hesaplama (*multi-party computation – MPC*) yöntemidir.

6.12. İlke 6(1)(a)(ii) bendinde belirtilen yetkinin mutlak suretle münhasır olması şart değildir. Kontrol sahibi kişi, başkalarının dijital varlıktan (belirli şekillerde) yararlanmasına izin verse bile, esaslı faydayı sağlama hakkı devam eder. Bu durum zaten İlke 6(3)(b)’de belirtilen yetki paylaşma istisnasının kapsamına da girebilir. Durum böyleyken İlke 6(1)(a)(ii) bendinde belirtilen yetkinin mutlak suretle münhasır olması ciddi bir sonucu beraberinde getirmeyecektir. Ayrıca kontrol sahibi, İlke 7’de ve ilgili Açıklamada görüleceğı üzere, olumsuz bir olguyu ispat etmekle yükümlü tutulmaz.

Birlikte kontrol

6.13. Örnek Durum 1: Birlikte kontrol ve çoklu imza kurguları. Bir yatırımcı, bir halka açık blokzincir platformunda tutulan misli bir dijital varlık üzerindeki malvarlıksal mutlak hakkı kazandığı düşünölsün. Yatırımcı, kontrol değışikliğinin gerçekleşmesi için üç özel anahtardan ikisinin -yatırımcının özel anahtarı ile yatırımcı tarafından güvenilir üçüncü kişiler X ve Y’nin özel anahtarları- gerekli olduğu bir çoklu imza düzeneğini kullanır. Yatırımcı, İlke 6(1)(a)’da belirtilen tüm yetkilere sahip olduğu ve İlke 6(1)(b) uyarınca kimliğini tanımlayabildiğı olasılıkta, dijital varlık üzerinde kontrol sahibidir. Yatırımcı, İlke 6(1)(a)(ii)’de belirtilen kontrol değıştirme yetkisini X veya Y ile paylaşmak suretiyle birlikte kullanıyor olsa ve onun ilgili yetkiyi kullanabilmesi için X veya Y’nin işlem yapması gerekse de, ortada İlk 6(3)(b) ve 6(1)(a)(iii)’ün münhasırlık koşulu bakımından öngörölmüş bir istisnanın varlığı söz konusudur.

Kontrol değışikliği

6.14. Örnek Durum 2: PKI (açık anahtar altyapısı) üzerinden kontrol değışikliği. Alpha adlı halka açık, izinsiz, dağıtık bir ağ, veritabanında (Alpha-DB) üzerinde kayıtlar (Beta) oluşturmayı ve kullanmayı mümkün kılan bir sanal makineyi (Alpha-VM) destekler. Alpha, her Beta’nın bir açık anahtarla ilişkilendirildiğı ve yalnızca buna karşılık gelen özel anahtar tarafından doğrulanan uygun talimatları Alpha-VM’ye gönderen bir kişi tarafından kullanılabileceğı bir açık anahtar kriptografi sistemini kullanır. Alpha ve

Alpha-VM, Betalar için iki farklı kullanım şeklini desteklemektedir: İlkinde, bir kişi bir Beta'yı çalıştırarak Alpha-DB'ye küçük bir görüntü dosyasını kalıcı olarak kaydedebilir ve her Beta yalnızca bir kez çalıştırılabilir. İkincisi, bir kişi bir Beta'nın ilişkilendirildiği açık anahtarı değiştirebilir; bir Beta yeni bir açık anahtarla ilişkilendirildikten sonra, o Beta'yı kullanmak için buna karşılık gelen bir özel anahtarın devreye sokulması gerekir.

6.15. Bir Beta, İlke 2(2) ve İlke 6'daki tüm koşulları sağladığı için dijital varlık kabul edilir.

Kişi A, yalnızca kendisinin özel anahtarını bildiği bir açık anahtardan Beta'nın bağlantısını kesip, onu yalnızca kişi B'nin özel anahtarını bildiği bir açık anahtarla ilişkilendirerek Beta'nın kontrolünün kişi B'ye devretmektedir.

6.16. Örnek Durum 3: OTP cihazıyla kontrol değişikliği. Özel, izinli, dağıtık bir ağ (Gamma), veritabanında (Delta-DB) elektronik kayıtların (Delta) oluşturulmasını ve korunmasını sağlayan bir sanal cihazı (Gamma-VM) destekler. Deltalar, yalnızca biçimlendirilmemiş metin depolayabilen kayıtlardır. Gamma, her Delta'nın, rastgele tek kullanımlık parolalar (OTP) üreten elde taşınabilir bir cihazla eşleştirildiği bir donanım güvenliği yöntemi uygulamaktadır (OTP cihazı). Bir Delta'da depolanan metni okumak, düzenlemek ve silmek için, söz konusu Delta ile eşleştirilmiş OTP cihazı tarafından üretilmiş tek kullanımlık bir parola gerekir.

6.17. Bir Delta, İlke 2(2) ve İlke 6'daki tüm gereklilikleri karşıladığından bir dijital varlık özelliğini gösterir. Kişi A, söz konusu Delta ile eşleştirilmiş OTP cihazını fiziksel olarak kişi B'ye vererek Delta'nın kontrolünü kişi B'ye devreder.

İlke 7

Bir Dijital Varlık Üzerinde Kontrol Sahibi Olan Kişinin Tanımlanması

(1) Bir kişinin bir dijital varlık üzerindeki kontrolünün tartışma konusu olduğu herhangi bir yargılamada:

(a) bu kişinin, İlke 6(1)(b)'de bahsi geçen tanımlanma şartının, İlke 6(1)(a)'da belirtilen yetkiler bakımından sağlandığını göstermesi yeterlidir;

(b) eğer bu kişi, İlke 6(1)(a)(i) ve İlke 6(1)(a)(iii)'te yer alan yetkilere sahip olduğunu kanıtlarsa, bu yetkilerin münhasır özellikte olduğu varsayılır.

(2) İlke 6(1)(b)'de bahsi geçen tanımlama, makul görülebilecek herhangi bir yöntemle yapılabilir. Sınırlı sayıda olmayan bu yöntemlere şu örnekler verilebilir: Söz konusu tanımlama aracı, kişinin ismini veya gerçek kimliğini açıkça göstermese bile, bir tanımlama numarası, kriptografik bir anahtar, bir ofis veya bir hesap numarası.

Açıklama

7.1. Yalnızca bir dava (geniş anlamda ele alındığında) bağlamında, İlke 7'de belirtilen ölçütleri içeren bir dijital varlıklar hukuku kapsamında, belirli bir dijital varlık üzerinde hangi kişinin kontrole sahip olduğu sorunu gündeme gelebilir. Eğer bir kişinin kontrole sahip olup olmadığı tartışmalı hale geldiğinde, varsayımlı kontrol sahibinin, tanım gereği izin verilen kişiler dışında hiç kimsenin ilgili yetkileri haiz bulunmadığını mutlak suretle ispat etmesi imkânsız olurdu. İlke 7(1)(a), dijital varlık üzerinde kontrol iddia eden bir kişinin, İlke 6'da belirtilen yetkilere sahip olduğunu göstermesiyle bir karinenin oluşacağını açıkça (zaten her durumda örtülü olarak böyle olsa da) ortaya koyar. Yani, o kişi başka kimsenin bu yetkilere sahip olmadığını ayrıca ispatlamak zorunda değildir. İlke 7(1)(b) de benzer şekilde, bu yetkilerin münhasır olduğu konusunda bir karine getirir; anılan karinenin hükümleri uygulanacak usul hukukuna tabi bulunmaktadır. Tabii ki, önceden kontrol sahibi olmuş bir kişi, ilgili devletin usul hukuku kurallarına göre kontrol değişikliğinin hukuka aykırı şekilde gerçekleştiğini ispat ederek daha üstün mahiyette bir malvarlıksal mutlak hakka sahip olduğunu ortaya koyabilir. Bu karine, ilgili devletin usul hukuku kuralları çerçevesinde yeterli görülecek bir ispat faaliyetiyle çürütülebilir.

7.2.Uygulamada, başka bir kişinin varsayımlı kontrol sahibinin rızası bulunmaksızın, ilgili münhasır yetkilere sahip olduğunu iddia ederek bir çekışmeli yargı sürecine dahil olma olasılığı oldukça düşüktür. Öngörülen ölçütler dairesinde, böyle bir kişinin kontrol sahibi olduğu da söylenemez. Bu türden bir kişinin (örnek olarak bir bilgisayar korsanı, hırsız veya dijital varlığı bularak elde eden kimse) ortaya çıkıp böyle bir iddiada bulunması konusundaki endişeler yersiz görünmektedir. Ayrıca, tecrübeler göstermektedir ki, ilgili yetkiler hukuka aykırı biçimde elde edildiğinde, ilgili yetkiler çok hızlı bir biçimde kullanılmakta ve dijital varlıklar önceki kontrol sahibinin uhdesinden çıkarılmaktadır. Bu durum, dijital varlıklara içkin bir dizi riski yansıtmaktadır.

İlke 8

Masum Kazanım

- (1) Bir devralanın masum kazanımında bulunan sayılabilmesi için:*
- (a) bir dijital varlık üzerinde kontrol elde etmesi; ve*
 - (b) ilgili devlet tarafından belirlenen ve iyiniyetle kazanım kurallarına denk düşen gerekliliklere uyması gerekir.*
- (2) Masum bir kazanımında bulunan, dijital varlığı, kendi hakkıyla çatışma gösterecek malvarlıksal mutlak haklardan ari olarak kazanır.*
- (3) Bir dijital varlık üzerindeki malvarlıksal mutlak haklara dayalı hiçbir talep, o dijital varlık üzerinde masum olarak hak kazanımında bulunana karşı ileri sürülemez.*
- (4) Masum kazanımında bulunan, dijital varlık üzerindeki malvarlıksal mutlak hakkı, dijital varlığın kontrolü, haksız şekilde hareket eden ve dijital varlık üzerinde malvarlıksal mutlak bir hakka sahip olmayan bir devreden tarafından değiştirilmiş olsa bile kazanabilir.*
- (5) Bu İlkeler, İlke 5(1) uyarınca uygulandığında, (1)(a) bendindeki gerekliliğe ek olarak, bir dijital varlığı devralanın masum kazanımında bulunan sayılabilmesi için aşağıdaki şartların da ayrıca gerçekleşmesi gerekir:*
- (a) Bir dijital varlığı devralan, bu dijital varlığı devraldığı sırada başka bir kişinin söz konusu dijital varlık üzerinde hak sahibi olduğunu ve kendisine yapılan bu devrin bu kişinin haklarını ihlal ettiğini fiilen bilmediği veya bilmesi gerekmediği sürece masum kazanımında bulunan olarak dikkate alınır.*
 - (b) Bir kişinin bir hakkı veya durumu bilip bilmediğinin veya bilmesi gerekip gerekmediğinin değerlendirilmesinde:*
 - (i) ilgili dijital varlık piyasasının özellikleri ve gereklilikleri dikkate alınmalıdır;*
 - (ii) devralanın genel olarak bir araştırma veya soruşturmada bulunma yükümlülüğü yoktur.*
 - (c) Bir hakkın veya durumun, belirli bir kurum bünyesinde bulunan sorumlu kişi tarafından fiilen bilindiği veya bu kişiye makul biçimde bildirilmiş olması gerektiği andan itibaren, ilgili kurumun da bu hakkı veya durumu bildiği veya bilebilecek durumda olduğu varsayılır.*

(d) Eğer dijital varlık bağışlama yoluyla veya herhangi bir teminat hakkının kurulması da söz konusu olmadan başka bir şekilde karşılıksız olarak devredilmişse, devralan masum kazanımda bulunan olarak sayılmaz.

(6) İlke 9’da belirtilen durumlar hariç olmak üzere, bir devralan fıkra (1) veya uygulanabilir ise fıkra (5) altında sayılan şartları sağlamıyorsa, bu kişinin hak ve yükümlülükleri diğer hukuk tarafından belirlenir.

Açıklama

Genel

8.1. İlke 9 ve bu ilkeye ilişkin açıklamalarda da belirtildiği üzere, dijital varlıklar bakımından da *nemo dat quod non habet* (kimse sahip olmadığı bir hakkı devredemez) temel ilkesi geçerlidir. Ancak İlke 8’deki masum kazanım kuralı, bu temel ilkeye bir istisna getirir. İlke 8(2) ve 8(3) uyarınca masum bir kazanımda bulunan, dijital varlığı çatışan malvarlıksal mutlak hak iddialarından ari olarak devralır ve bu kişiye karşı böyle bir malvarlıksal mutlak hak iddiasına dayanılarak hak ileri sürülemez.

8.2. Masum kazanımda bulunanlara tanınan bu haklar, dijital varlıkların, birçok Kıta Avrupası ve Anglo-amerikan hukuk sistemindeki tedavül kabiliyeti olan kıymetli evrak veya menkul kıymetler gibi tedavüle elverişli nitelikler kazanmasını sağlar.

8.3. Masum kazanım kuralı nedeniyle, bazı durumlarda haksız bir fiilden zarar gören malvarlıksal mutlak hak sahibi kişi, masum kazanımda bulunana karşı herhangi bir hak iddiasında bulunamayabilir. Bu mağdur, haksız fiili gerçekleştiren kişiye karşı dava açabilir, fakat bu çoğu zaman etkili olmayacaktır. Masum kazanım kuralı, bu noktada Açıklama 8.4 ve 8.5’de belirtileceği üzere, piyasaların etkinliği ve hukuki güvenlik açısından masum kazanımda bulunan lehine bir politika dengesini gözetmektedir.

8.4. Dijital varlıklar, çoğunlukla blokzincir veya benzeri elektronik ağlarda çok hızlı şekilde el değiştirir. Piyasaların bu akışkanlığının yanı sıra, devreden konumundaki kişilerin genelde takma adlar kullanmaları veya farklı ülkelerde bulunmaları hususları da dikkate alındığında, devir sırasında çatışma gösterebilecek hak sahipliklerini araştırmak pratikte

pek de mümkün görünmemektedir. Bu nedenle, dijital varlık üzerinde halihazırda malvarlıksal mutlak hakka sahip olan bir kişinin, hakkını korumak için gerekli önlemleri alması, devralana kıyasla daha kolaydır. Masum kazanım kuralı, piyasada işlemlerin süratle ve hukuki belirlilik içinde yapılabilmesine imkân tanır. Böyle bir kural olmadığında, üçüncü kişilerin malvarlıksal mutlak hak iddiası riski, alıcıların dijital varlık için ödeyecekleri bedeli veya teminatlı alacaklıların varlığa atfedecekleri değeri düşürecektir. Masum kazanım kuralı, dijital varlıkları saklayanlar ve onların müşterileri açısından da faydalıdır (bkz. İlke 12 ve bu İlke altında verilen Açıklama). Bu türden bir masum kazanım kuralının varlığı, maliyetleri azaltır ve işlemleri hızlandırır. Kıymetli evrak ve menkul kıymet piyasalarında da benzer masum kazanım kuralları, bu piyasaların etkin ve güvenli biçimde işlerlik göstermesini temin etmektedir. Dijital varlıklar, mevcut ekonomide önemli bir rol oynamaktadır, zaman içinde bu rolün öneminin daha da artması beklenmektedir.

8.5. Ayrıca dijital varlıklar, programlama yoluyla fiilen tedavül kabiliyeti sınırlı olacak şekilde tasarlanabilir. Örneğin, bir dijital varlık, potansiyel alıcıları olası çelişkili taleplerin varlığı konusunda doğrudan veya dolaylı suretle bilgilendirecek biçimde programlanabilir. Bir dijital varlığın meta verilerinde, meşru hak sahibinin kimliğinin açıkça belirtecek ve ilgili varlığı devralmak isteyen herhangi bir kimseye bu kişiyle işlem yapılması gereğini açıkça bildirecek şekilde programlama yapılması böyle bir sonuca yol verebilir.

8.6. İlke 8'in masum kazanım bağlantılı varlıklara uygulanması hakkında bkz. Açıklama 4.11 ve 4.29 – 4.32.

İlke 8(1) – 8(3)

8.7. İlke 8(1), bir devralanın masum kazanımda bulunan sayılması için gerekli olan koşulları ortaya koyar. İlk koşul, devralanın İlke 6'da tanımlandığı şekilde dijital varlık üzerindeki kontrolü elde etmesidir. İkinci koşul, masum kazanımda bulunanın ilgili devletin (yani iç hukuk uygulanacak hukuk olarak dikkate alınacak devletin) belirlediği gerekliliklere uyulmasıdır. İlke 8(1)(b)'de işaret edildiği üzere, bir devlet, dijital varlıkların masum kazanımında öngörülecek koşulların kesin çerçevesinin belirlenmesinde esnek hareket edebilme kabiliyetini haizdir, sonuçta öngörülecek koşulların, o devletin hukukundaki diğer iyiniyetli kazanım koşullarıyla uyum içinde olması gerekir. Bir devlet, dijital varlık

türüne göre farklı masum kazanım kurallarını benimsemeyi tercih edebilir (Ayrıca bkz. Açıklama 3.7).

8.8. İlke 8(2) ve 8(3), Açıklama 8.1 ve 8.2 altında belirtildiği üzere, masum kazanımda bulunanın haklarına ilişkin sonuçları ortaya koyar.

İlke 8(4)

8.9. İlke 8(4), örnek olarak bir hırsız ya da bilgisayar korsanı tarafından gerçekleştirilen bir kontrol değişikliği yoluyla bir dijital varlığın kontrolünü haiz olan bir kişinin dahi, masum kazanımda bulunan olarak nitelendirilebileceğini açıkça ortaya koyulması temel amacını taşımaktadır. Ayrıca bkz. Açıklama 6.6, 6.9 ve 6.10.

İlke 8(5)

8.10. İlke 8(5), bir devralanın masum kazanımda bulunan olarak kabul edilebilmesi için gerekli temel koşulları belirtmektedir. Söz konusu koşullar, şu iki durumda yarar sağlanmak üzere öngörülmüştür: Birincisi, İlke 5(1)(a), 5(1)(b) veya 5(1)(d) uyarınca bir devlet mahkemesinin bu İlkeleri uygulamasının gerekmesidir. İkincisi ise, söz konusu devletin dijital varlıklar için uygulanacak masum kazanım kurallarını henüz benimsememiş olmasıdır. Eğer devlet bu konuda kendi özel kurallarını benimsemişse, ilgili kurallar İlkeler Hukuku olarak uygulama alanı bulacaktır. İlke 8(5), büyük ölçüde Cenevre Menkul Kıymetler Antlaşması'ndaki (*Geneva Securities Convention*) masum kazanım kuralından esinlenilerek meydana getirilmiştir.

İlke 8(6)

8.11. İlke 8(6), İlke 3(3) ile uyumlu şekilde, bu İlkeler tarafından düzenlenmeyen hususlarda diğer hukuk kurallarının geçerli olduğunu vurgular; ancak bu uygulama İlke 9'da belirtilen istisnalara tabidir.

İlke 9

Devralanın Hakları

- (1) İlke 8'e tabi olmak kaydıyla, bir kişi bir dijital varlık üzerinde varsa sahip olduğu malvarlıksal mutlak hakkından fazlasını devredemez.***
- (2) Bir dijital varlık üzerindeki malvarlıksal mutlak hakkı devralan kişi, kural olarak devredenın sahip olduğu veya devretme yetkisine sahip olduğu malvarlıksal mutlak hakkı tümüyle devralır; meğerki devralan bu konuda belirli bir sınırlama dahilinde hareket etmiş olsun, böyle bir durumda devralan ancak ilgili sınırlama ölçüsünde hak sahibi olabilir.***

Açıklama

İlke 9(1): nemo dat kuralı

9.1.İlke 9(1), *nemo dat quod non habet* (kimse sahip olmadığı bir hakkı devredemez) temel ilkesini ortaya koyar. Bununla birlikte, İlke 9(1), İlke 8'de düzenlenen masum kazanım kuralına tabidir; bu kural, *nemo dat* ilkesinin sonuçlarına bir istisna getirir. İlke 8, devredene kendisinde olmayan hakları devretme yetkisi vermez; fakat bu hakları devredebilme imkânını tanır. Bu nedenle masum kazanımda bulunan, dijital varlığı çelişen malvarlıksal mutlak hak iddialarından arı şekilde devralır ve ona karşı herhangi bir hak iddiasında bulunulamaz.

İlke 9(2): Koruma İlkesi

9.2.İlke 9(2), takip edilen koruma ilkesini ifade eder: bir devralan, devredenın devrettiği veya devretme yetkisine sahip olduğu tüm malvarlıksal mutlak hakları devralır. Ancak İlke 9(2), devreden daha dar kapsamlı bir hak devrini gerçekleştirmişse, devralanın da yalnızca devredilen bu ölçüde bir hak kazanımında bulunacağına açıkça işaret etmektedir.

9.3.İlke 9(2) uyarınca, bir dijital varlık üzerindeki malvarlıksal mutlak hakkı masum kazanım yoluyla devralan ve ondan sonraki tüm devralanlar, bu masum kazanımda bulunanın haklarını -yani çatışan hak iddialarından arınmış ve bunlara karşı koruma sağlayan hakları- kazanır. Anılan durum, sonraki devralanın kendisinin doğrudan masum

kazanında bulunabilme koşullarını taşımadığı hallerde dahi geçerlidir (Örnek olarak kazanında bulunacak kişinin, uygulama alanı bulduğunda, İlke 8(5)(a) kapsamındaki bilgileri devir sırasında bilmesi gerekse bile durum değişmez).

BÖLÜM IV: SAKLAMA

İlke 10

Saklama

(1) Bu İlkelerde:

- (a) “Saklayan”, aşağıda fıkra (3) ve (4)’te tanımlandığı şekilde bir saklama sözleşmesi uyarınca bir müşteriye hizmet sağlayan kişiye karşılık gelir ve bu sıfatla hareket eder;*
- (b) “alt saklayan”, fıkra (3) ve (4)’te tanımlandığı şekilde bir saklama sözleşmesi uyarınca başka bir saklayana hizmet sağlayan kişiye karşılık gelir ve bu sıfatla hareket eder;*
- (c) “müşteri”, fıkra (3) ve (4)’te tanımlandığı şekilde bir saklama sözleşmesi uyarınca bir saklayanın hizmet sağladığı kişiye karşılık gelir.*

(2) Aşağıdaki durumlarda saklayanın bir dijital varlığı müşteri için muhafaza ettiği kabul edilir:

- (a) Saklayan dijital varlığın kontrolüne sahip bulunuyorsa; veya*
- (b) Saklayan, İlke 11 (4)’te belirtilen koşulların varlığı dahilinde, dijital varlıkla ilgili olarak bir alt saklayan ile fıkra (3)’te tanımlandığı şekilde bir saklama sözleşmesi ilişkisine girerse.*

(3) Fıkra (4) düzenlemesi saklı kalmak üzere, bir dijital varlıkla ilgili olarak bir müşteriye verilen hizmetler için yapılan bir anlaşma aşağıdaki durumlarda bir “saklama anlaşması” olarak kabul edilir:

- (a) ilgili hizmetin bu hizmet sağlayanın olağan faaliyeti dahilinde sunuluyorsa;*
- (b) hizmet sağlayıcı, müşteri için dijital varlığı elde etmek (henüz böyle bir durum söz konusu değilse) ve muhafaza etmekle yükümlü bulunuyorsa; ve*
- (c) Müşteri, İlke 6(2) anlamında dijital varlık üzerinde kontrol değişikliği meydana getirme konusunda münhasır yetkiyi haiz bulunuyorsa.*

(4) Fıkra (3)’ün uygulama alanı bulduğu bir anlaşma, hizmet sağlayıcının iflasla ilişkili bir sürece girmesi durumunda, dijital varlığın hizmet sağlayıcının alacaklıları tarafından başvurulabilecek malvarlığı değerleri (varlıkları)

arasında yer alacağı yapılan anlaşmadan açıkça anlaşılıyorsa, bu anlaşma bir saklama anlaşması olarak değerlendirmeye alınamaz.

(5) Saklayan ile müşteri arasındaki ilişki, müşterinin ilgili dijital varlık özelinde üçüncü bir kişi adına herhangi bir sıfatla hareket ediyor olmasına bakılmaksızın mevcut olabilir.

Açıklama

Genel Bakış

10.1. Bölüm IV'ün amacı, dijital varlıkların saklanmasıyla ilgili özel hukuk ilkelerinin ortaya koyulmasıdır. Düzenleyici mahiyetteki hukuk kuralları (regülasyon) da dahil olmak üzere başka kanunlar da saklama hizmetlerinin sağlanması için uygulama alanı bulabilir. Saklama ilişkisi, genel olarak bakıldığında, bir kişinin (genellikle belirli düzenleyici kurallar çerçevesinde oluşturulmuş bir tüzel kişi olabilir), bir dijital varlığı, bu varlık üzerinde yetkisiz tasarruflarda bulunulmasına ve dijital varlığı muhafaza eden saklayanın iflasına karşı özel koruma sağlanacak şekilde, başka bir kişi için, yani bir müşteri (bu son kişi başka bir saklayan da olabilir) adına ve yararına muhafaza etmesini konu alır. Anılan durum, yalnızca saklama hizmeti veren kişinin bunu kendi işinin olağan akışı içinde yaptığı durumlarda geçerlidir. Müşteri için söz konusu olacak özel korumanın, özel hukukta müşterinin varlık üzerinde bir tür malvarlıksal mutlak hakka sahip olmasıyla sağlanması muhtemeldir, ancak bu korumanın tam olarak hangi yöntem üzerinden sağlanacağı ilgili hukuk sisteminin özel hukukuna göre değişkenlik gösterecektir. Daha önce Açıklama 6.5 ve 6.6'da belirtildiği üzere, saklama, bir kişi (saklayan) dijital varlık üzerindeki kontrolü (İlke 6'da tanımlandığı biçimde) elinde tutarken, diğer bir kişinin (müşteri) bu varlık üzerinde malvarlıksal mutlak hakkı haiz olduğu durumlara somut bir örnek oluşturur.

10.2. Aynı hizmet sağlayıcının müşterileri için veya kendi adı ve hesabına dijital varlık alım-satımı yapmak, bir pazar yeri ("borsa" veya "alım-satım platformu") işletmek vb. dahil olmak üzere saklama dışında çeşitli faaliyetler yürütmesi oldukça yaygındır. İlke 10, bu hizmeti sağlayan kişi tarafından yürütülen diğer faaliyetlerden bağımsız olarak ve ilgili hizmet sağlayıcının düzenleyici hukuk kuralları (regülasyon) çerçevesindeki hukuki statüsüne bakılmaksızın yalnızca saklama hizmeti bakımından uygulama alanı bulur. "Saklayan" terimi, salt olarak bir kişi saklayan sıfatıyla hareket ettiği sürece o kişiye atıfta

bulunulur. İlke 10'da saklayanlar hakkında belirtilen hususlar, sadece saklama hizmeti için geçerlidir, bu kişiler tarafından sağlanan diğer hizmetler için uygulama alanı bulmaz.

10.3. Bir hizmet sağlayıcı tarafından sunulan hizmetlerin saklama hizmeti olarak değerlendirmeye alınabilip alınamayacağı, hizmet sağlayıcı ile müşterisi arasındaki anlaşmanın bir saklama anlaşması olup olmadığına bağlı olacaktır. İlke 10(3), saklama anlaşmasını tanımlar. İlke 10(1) ise, saklama anlaşması bağlamında önem arz eden tarafların tanımını yapmaktadır. Dijital varlığın kontrolünü elinde tutan kişi, duruma göre bir saklayan (bu durumda dijital varlık saklayan konumunda olmayan bir “müşteri” için kontrol edilmektedir) veya bir “alt saklayan” (bu durumda da dijital varlık saklayan konumunda olan bir “müşteri” için kontrol edilmektedir) olabilir. İlke 10(1)'deki tanım kapsamında, alt saklayan da saklayan konumunda bulunmaktadır.

Dijital bir varlığın muhafaza edilmesi

10.4. İlke 10(2)'nin amacı, İlke 6'da tanımlanan (olgusal/maddi fiil niteliğindeki) “kontrol” kavramından daha geniş bir içeriği haiz olan, dijital varlığı “muhafaza etme” kavramının ortaya koyulmasıdır. “Muhafaza etmek” terimi, saklayanın bir dijital varlığı müşterisi için “muhafaza ettiği” iki durumu kapsayacak şekilde tanımlanmıştır. Bu durumlardan ilki, saklayanın İlke 6 anlamında doğrudan bir dijital varlığın kontrolünü elinde tuttuğu durumdur. İkincisi, saklayanın saklama hizmetini alan kişi konumunda olduğu, yani başka bir saklayanın (alt saklayan), ilk saklayan için dijital varlığın kontrolünü elinde bulundurduğu durumdur. Alt saklayanın devreye sokulduğu olasılıklarda hem saklayan hem de alt saklayan dijital varlığı “muhafaza eden” kişi konumunda bulunur. Anılan durumda, saklayan ile alt saklayan arasında bir saklama anlaşması akdedilir ve saklayan da alt saklayanın müşterisi konumunda olur. Dolayısıyla saklayan bu anlaşma kapsamında alt saklayan karşısında çeşitli hakları haizdir. Duruma göre birden fazla katmandan oluşan saklama anlaşması yapılarıyla da karşılaşılabılır. Örnek olarak üç katmanlı bir yapı dahilinde, alt saklayanın kendisi saklayan için dijital varlığı “muhafaza eder”, çünkü üçüncü bir saklayan da bu alt saklayan için ilgili varlığı kontrol etmekle yükümlüdür.

Saklama anlaşması

10.5. İlke 10(3) ve 10(4) bir anlaşmanın saklama anlaşması olup olmadığını belirlemek için bir yöntem sunmaktadır. İki işlevi yerine getirirler.

10.6. İlk olarak, İlke 10(3)'ün (a), (b) ve (c) bentleri bir saklama anlaşmasının ve dolayısıyla saklama ilişkisinin tanımı olarak işlev görür. Bent (a), bir hizmet sağlayıcının saklayan olarak kabul edilebilmesi için, saklayanın iş faaliyetinin olağan akışı içinde hareket etmesi gerektiğini açıkça ortaya koymaktadır. Bent (b) saklayanın temel yükümlülüğüne işaret etmektedir (ayrıca bkz. İlke 11(1)). Bu yükümlülük, üç durumu kapsar. Belirtilen durumlardan ilki, müşteri ile bir saklama anlaşması imzalamış olan saklayanın sözleşme konusu olan dijital varlığın kontrolünün henüz saklayanda olmadığı durumdur: Örnek olarak, eğer (a) müşteri henüz bir dijital varlığı saklayana devretmemişse ya da saklayan ilgili varlığı henüz müşteri için devralmamışsa, (b) saklayan sahip olduğu kullanım hakkını kullanmaktaysa (bkz. İlke 11(1)) ya da (c) saklayan yükümlülüklerini ihlal ediyorsa ve saklama anlaşmasının konusu olan dijital varlığı kontrolünü elinde bulundurmuyorsa. Verilen bu örneklerin her birinde, saklayan öncelikle anlaşmanın konusu olan dijital varlığı elde etmekle yükümlüdür. Dijital varlık, misli bir mahiyette ise (bkz. Açıklama 11.6), yükümlülük sözleşmede belirtilen tanıma uyan bir dijital varlık elde etmek yönünde olacaktır. İkinci durum, saklayanın dijital varlığın kontrolünü elinde tuttuğu durumdur; bu durumda saklayan, müşteri tarafından aksi yönde talimat verilene kadar ya da varsa kullanım hakkını devreye sokana kadar dijital varlığı kontrol etmeye devam etmekle yükümlüdür (bkz. İlkeler 11 (I)(a) ve 11 (I)(b)). Üçüncü durum, saklayanın dijital varlığı doğrudan kontrol etmeyip kendisinin de bir saklama hizmeti alan kişi olduğu, yani bir alt saklayanın dijital varlığı saklayan için kontrol ettiği durumdur. İkinci ve üçüncü durumlarda saklayan, dijital varlığı İlke 10(2)'de tanımlandığı şekilde “muhafaza eder”. İlke 10(3)(c)’e göre, müşterinin dijital varlığın kontrolünü değiştirme yetkisine münhasır olarak sahip olduğu durumlarda, taraflar arasındaki anlaşma saklama anlaşması niteliğini taşımaz (“kontrol değişikliğinin” anlamı için bkz. İlke 6(2)). Bu duruma Açıklama 10.14-10.19 arasında da değinilmektedir. İlke 10(3)(c)'de atıfta bulunulan münhasır yetki, İlke 6(1)(a)(iii)'de atıfta bulunulan yetkidir ve bu nedenle İlke 6(3)'te belirtilen “münhasırlık” kavramının esnetildiği olasılıklar burada da işlerlik gösterir.

10.7. İlke 10(3) ve 10(4)'ün ikinci işlevi, saklama anlaşması ile hizmet sağlayıcının iflasla ilgili bir sürece tabi olması halinde, hizmet sağlayıcı tarafından muhafaza edilen dijital varlığın onun alacaklılarına dağıtılabilecek varlıkların bir parçasını oluşturduğu bir anlaşma (anılan türde bir anlaşmaya Açıklama 10.20'de değinilmektedir) arasındaki sınırı ortaya koymaktır. Bu son anlaşma, saklama anlaşmasına benzer özellikler gösterebilir, çünkü her iki anlaşmada da müşteri dijital varlık üzerinde kontrolü haiz bulunmamakta ve hizmet sağlayıcı müşterinin haklarının kaydını tutmaktadır (müşteri haklarının bir kaydı, saklama anlaşması kapsamında da tutulur (veya tutulmalıdır), bkz. İlke 11 (3)(a)). Ancak, bu tür bir (saklama ilişkisi haricinde kalan) anlaşma kapsamında müşteri, hesap sağlayıcının iflas riskine katlanmak durumunda olur. Böyle bir riski üstlenen bir müşteri, ilgili durumun farkında olmalıdır, oysa bu türden risk bir saklama anlaşması kapsamında (saklayan dijital varlığı muhafaza etme yükümlülüğünü yerine getirdiği sürece) söz konusu olmaz. Bu nedenle, müşterinin dijital varlıklarının kontrolünü elinde bulundurmadığı bir anlaşmanın, hizmet sağlayıcının tarafından iflasla ilgili bir sürece girmesi durumunda ilgili varlıkların hizmet sağlayıcının alacaklılarına dağıtılabilecek bir parçasını oluşturduğu anlaşmada açıkça belirtilmediği sürece, bir saklama anlaşması olduğu karine olarak kabul edilir. (bkz. İlke 13(2)). İlgili durumun müşteriler açısından açık olması yeterli gelir, bundan başka belirli bir ifadenin veya özel kelime grubunun kullanılmasına gerek yoktur. İlke 10(4), hizmet sağlayıcıları yapacakları anlaşmaların hukuki niteliğini açıkça ortaya koymaya teşvik etmek üzere tasarlanmıştır.

10.8. Bir devlet, müşteriye, onun hizmet sağlayıcının iflas riskine katlanmak zorunda kaldığı saklama haricindeki anlaşmalara karşı korumak isteyebilir. Bu türden düzenleyici hükümlerle sağlanan koruma düzeneklerine ilişkin örnek durumlara Açıklama 10.21'de değinilmektedir.

İlke 10(5)

10.9. İlke 10(5), saklama ilişkisinin varlığını veya işleyişini etkilemeksizin, müşterinin herhangi bir sıfatla üçüncü bir kişi adına hareket edebileceğini açıkça ortaya koymaktadır. Bu, müşteri tarafından temsil yoluyla hareket edilen durumları kapsayabileceği gibi müşterinin (ilgili hukuk sistemi dahilinde) dijital varlığı bir başkası için inançlı olarak elinde tuttuğu durumlar (örneğin, müşteri bir yatırım fonu veya dijital varlığı bir başka aile

üyesi için elinde tutan bir kişi olabilir) veya başka hukuk sistemlerindeki benzerlik gösteren kurgular dahilinde gündeme gelir.

Saklama ilişkisi örnekleri

10.10. Aşağıda, hizmet sağlayıcı ile müşteri arasındaki ilişkinin saklama ilişkisi olduğu durumlara ilişkin iki örnek durum yer almaktadır. Bunlar Açıklama 10.13 ve devamında değinilecek saklama ilişkisi haricinde kalan örnek durumlarla karşılaştırmalı olarak okunmalıdır. Saklamaya ilişkin ilk örnek durum, gözetimli saklama cüzdanının (bazen aracılı cüzdan olarak da adlandırılır) genel bir tarifini vermekte, ikinci örnek durum ise bu tür bir hizmetin daha geniş bir bağlamda nasıl sağlanabileceğine işaret etmektedir. İlgili örneklerde kullanılan “cüzdan” terimi, piyasada kullanıldığı anlamda, yani bir kişinin dijital bir varlıkla, örneğin açık ve/veya özel anahtarların oluşturulması ve yönetimi yoluyla etkileşime girmesini sağlayan yazılım (veya donanım) anlamında kullanılmaktadır. Bu etkileşimin hangi yollarla ve kim tarafından gerçekleştirileceği, kullanılan cüzdanın türüne bağlıdır. İlke 10(3) ve 10(4) ve Açıklama 10.7'de belirtildiği üzere, Açıklama 10.11 ve 10.12'de belirtilen bağlamda bir müşteri ile bir hizmet sağlayıcı arasında yapılan bir anlaşma, hizmet sağlayıcı tarafından kontrol edilen varlıkların bu kişinin iflasla ilgili bir sürece girmesi halinde onun alacaklılarına dağıtılabilecek varlıkların bir parçasını oluşturduğu açıkça belirtilmediği sürece, bir saklama anlaşması olarak kabul edilir, bu durumda ilgili anlaşma Açıklama 10.20'de tartışılan örnek durum kapsamında değerlendirmeye alınır.

Gözetimli veya aracılı cüzdan

10.11. Örnek Durum 1. Gözetimli veya aracılı cüzdan yapısı dahilinde, kullanıcılar dijital varlıkları bir hizmet sağlayıcının cüzdanlarına aktarır. Hizmet sağlayıcı (saklayan), dijital varlığın saklanacağı cüzdanın özel anahtarlarını elinde tutar. Aracılı cüzdanlar, genellikle bir aracının kullanıcılar arasında dijital varlıkların alım satımını kolaylaştırdığı ticaret platformları bağlamında söz konusu olur. Bir alım satım platformu hizmetinin parçası olarak aracılı cüzdan hizmetlerinin sağlanmasına ilişkin bir örnek Açıklama 10.12'de verilmiştir. Hizmet sağlayıcılar genellikle birden fazla türde cüzdan hizmeti sunarak kullanıcıların hem kendi kendine saklama hem de gözetimli cüzdan çözümlerinden

yararlanmasına olanak tanır (kendi kendine saklama için bkz. Açıklama 10.15-10.17) zira bu iki farklı cüzdan türü farklı amaçlara hizmet etmektedir.

Alım-satım hesabı

10.12. Örnek Durum 2. Bir hizmet sağlayıcı olan A, kullanıcılarına, kendi aracılığıyla itibari para ile dijital varlık satın alınabilmesine ve bunların elde tutulabilmesine imkân sağlayan “alım-satım hesabı” olarak adlandırdığı hizmeti sunar. A ile müşterisi arasındaki sözleşme dahilinde, alım-satım hesabındaki dijital varlıklar üzerindeki malvarlıksal mutlak hakların kullanıcıya ait olduğu ve A'ya devredilmediği açıkça belirtilmekte ve anılan hesaptaki dijital varlıkların A'ya ait olmadığı veya ona ödünç verilmediği vurgulanmaktadır. A'nın müşterileri arasındaki alım-satım hesabı üzerinden başlatılan bazı işlemler blokzincir dışında gerçekleşir ve yalnızca A'nın muhasebe defterine yaptığı girişler ile kayıt altına alınır. Öte yandan, kendi kendine saklama cüzdanı (A veya başka bir hizmet sağlayıcı tarafından sağlanan) ile A tarafından sağlanan bir alım-satım hesabı arasındaki bir işlem blokzincir üzerinde gerçekleşir.

Saklama ilişkisi haricinde kalan durumlara ilişkin örnekler

10.13. Bir kişinin bir dijital varlığı kontrol ettiği, ancak taraflar arasında saklama anlaşması niteliği taşımayan bir anlaşmanın bulunduğu ve yine bir hizmet sağlayıcıyla yapılan anlaşmanın İlke 10(3) ve 10(4)'te tanımlanan saklama anlaşması tanımına uymadığı bir dizi durum vardır. Aşağıdaki paragraflarda bu durumlara ilişkin örnekler gösterilmekte ve açıklanmaktadır.

10.14. Örnek Durum 3: Yatırımcı veya benzeri özellikte bir kişinin bir dijital varlığı kontrol ettiği durum. Bir kişi (örneğin bir yatırımcı) bazı donanım veya yazılımları kullanarak bir dijital varlığı kontrol edebilir. Örnek olarak, ilgili kişinin dijital varlığın kayıtlı olduğu blokzincirde tam düğüm (veya hafif düğüm) işlettiği veya blokzincire erişmek için cüzdan yazılımı veya hizmeti kullandığı durumlar gösterilebilir. Anılan tüm durumlarda, yatırımcı dijital varlığın kontrolünü elinde tutmaktadır zira bu kişi özel anahtarı kendi üzerinde tutar ve kullanır; anahtarı üçüncü bir kişiye emanet ya da teslim etmez. Yatırımcı tarafından kullanılan cüzdanın sağlayıcısı yalnızca yatırımcının özel anahtarlarını sakladığı ve kullandığı araçları (donanım veya yazılım) sağlar. Yatırımcı, cüzdanla ilgili olarak

gündeme gelebilecek arıza riskine katlanmak durumunda olur; ancak dijital varlıkları cüzdan sağlayıcı tarafından kontrol edilmez. Cüzdan sağlayıcının iflası, cüzdanı işletme veya muhafaza etme kabiliyetini etkileyebilir ancak yatırımcı tarafından kontrol edilen dijital varlıklar üzerinde herhangi bir hukuki etki meydana getirmez. Yatırımcı ile donanım veya yazılımı sağlayan kişi arasındaki ilişki tamamen sözleşmeye dayalı olup bu konuda belirleyici olan taraflar arasındaki anlaşma şartlarıdır.

10.15. Kendi kendine saklama, kullanıcının özel anahtarları doğrudan kendi bilgisayarına ya da cep telefonuna yüklediği ya da bulut tabanlı yazılımlara dayalı gözetimsiz cüzdanları kullanarak üzerinde tutmasıdır. Bu iki seçenek oldukça benzerdir: Temel fark özel anahtarların tutulduğu yerdedir. Her iki durumda da dijital varlık müşterinin kontrolündedir. Bu iki seçeneğe aşağıdaki iki paragrafta değinilmektedir.

Cüzdan yazılımı ile kendi kendine saklama

10.16. Örnek Durum 4. Bu paragrafta bahsi geçen “kendi kendine saklama” durumu, yine bu paragrafta bir örneği verilen cüzdan yazılımının kullanımına atıfta bulunmaktadır. “XX”, küresel bir geliştirici ve tasarımcı topluluğu tarafından geliştirilen açık kaynaklı bir yazılımdır. Çeşitli donanım cüzdanları ile uyumludur. XX kullanıcısı, özel anahtarlarla birlikte XX yazılımının yüklü olduğu cep telefonu veya bilgisayarda şifrelenmiş bir formatta saklanan bir cüzdan şifresi ve gizli kurtarma cümlesi oluşturur. XX yazılımını kullanan cüzdanlar aracılığıyla gerçekleştirilen işlemler blokzincir üzerine işlenir.

Bulut tabanlı yazılım ile kendi kendine saklama

10.17. Örnek Durum 5. Bir hizmet sağlayıcı olan Y, kullanıcılara gözetimsiz cüzdanlar temin etmektedir. Bir kullanıcı bir hesap oluşturur ve bir şifre belirler. Bu şifre, Y tarafından blokzincir üzerinde tutulan şifrelenmiş bir dosyaya erişim sağlar. Dosya ise, gizli bir özel anahtar kurtarma ifadesini, kullanıcının özel anahtarlarını ve dijital varlıklara ilişkin adresleri içerir. Şifre Y tarafından saklanmaz, kullanıcının kendisi tarafından güvenli ve gizli tutulmalıdır. Y'nin kullanıcının özel anahtarlarına, gizli özel anahtar kurtarma ifadesine veya şifresine erişimi yoktur. Bir şifre veya gizli özel anahtar kurtarma ifadesi doğru kullanıldığında, özel anahtarları içeren dosyaya kullanıcının bilgisayar veya cep telefonu üzerinden erişilir ve kullanıcı doğrudan blokzincir üzerinde gerçekleştirilecek

işlemleri yapabilir. Y şifrelenmiş dosyayı bulutta saklarken XX yazılımı kullanıldığında (bkz. Açıklama 10.16) şifrelenmiş dosya doğrudan kullanıcının bilgisayarında veya cep telefonunda yerel olarak saklanır. Bu nedenle, hizmet olarak yazılım modelinin (*software-as-a-service*) kullanıcıları, Y'nin cüzdan hizmetlerini sunmayı bırakmaya karar vermesi durumunda kendilerini zor bir durumda bulabilirler.

Özel anahtarların korunması

10.18. Örnek Durum 6: Bir işletmenin özel anahtarların korunmasına yönelik hizmet sunduğu durum. Bir başka anlaşma türü de bir hizmet sağlayıcının müşterisinin özel anahtarlarını koruduğu veya müşterinin özel anahtarlarını korumasını kolaylaştırmak için yazılım veya donanım sağladığı durumdur. Özelliklerine bağlı olarak, yazılım veya donanım sağlayıcısı müşterinin özel anahtarlarını kullanma ve böylece müşterinin dijital varlıklarının kontrolünü ele geçirme kabiliyetine sahip olabilir (veya olmayabilir). Ancak, bu tür bir anlaşmanın amacı tam olarak bu değildir ve genelde hizmet sağlayıcının müşterinin özel anahtarlarını müşteri tarafından kabul edilmeyen herhangi bir amaç için kullanması yasak tutulacaktır. Böyle bir durumda müşteri halen daha dijital varlığın kontrolünü ve varlığın bu kontrolü değiştirme yetkisini (İlke 6(1)(a)(iii)'deki terminoloji dahilinde ifade edildiğinde) haiz bulunmaktadır. Dolayısıyla bu tür bir iş modeli, piyasa katılımcıları tarafından bazen “saklama” olarak adlandırılrsa da, İlke 10'da tanımlanan türde bir saklama hizmeti değildir. Bir hizmet sağlayıcının saklama hizmeti sunduğu durumlarda, bu belirtilenden farklı olarak, müşteriler dijital varlıklarını bu hizmet sağlayıcı tarafından kontrol edilen adreslere ya da özel anahtarlara aktarır ya da hizmet sağlayıcı müşteri için kontrol ettiği dijital varlıkları devralır. Özel anahtarların korunmasına ilişkin bir örnek bir sonraki paragrafta yer almaktadır.

10.19. Z cüzdanı, özel anahtarları cihazın içinde üretir ve bu anahtarları yine aynı cihazın içinde depolar. Bu yaklaşım, anahtarların çevrimdışı tutulmasını sağlayarak, çevrimiçi bilgisayar korsanları ve diğer tehditlerden korunmalarını mümkün kılar; böylece, anahtarlar oluşturuldukları andan kullanılacakları ana kadar güvenli bir “soğuk cüzdan” ortamında kalır. Z donanımında çalışan yazılım, herhangi bir aracı kişi tarafından yönetilmez; üçüncü kişi araçların Z cüzdanında tutulan anahtarlara erişimi yoktur. Kullanıcı, Z cüzdanında bulunan anahtarlarla bir işlem gerçekleştirmek istediğinde, mobil uygulama mağazalarına

benzer bir yazılım aracılığıyla, dijital varlıkları gönderme, satın alma veya satma hizmeti sunan diğer sağlayıcıların uygulamalarına erişir.

Dijital varlıkların teslimine ilişkin anlaşma

10.20. Örnek Durum 7: Dijital varlıkların teslimi için bir anlaşma yapılması. Bir fintech firması ya da bir finansal kurum, örnek olarak bir aracı kurum, borsa veya bir ticaret platformu, bir müşteriden belirli miktarda dijital varlık alması ya da müşteri adına birincil veya ikincil piyasadan bu varlığı temin etmesi nedeniyle, söz konusu dijital varlığı müşteriye teslim etme yükümlülüğü altına girebilir. Bu tür bir firma veya kurum, müşteriye ait varlıkların (emanet veya saklama hesabından farklı bir banka hesabına benzer şekilde işleyen olarak değil, işleyen bir hesap tutar; bu hesapta belirli bir dijital varlığa ilişkin alacaklar ve borçlar kaydedilir. Böylece, hesabın bakiyesi her zaman kurumun müşteriye teslim etmekle yükümlü olduğu (veya tersi durumda müşteriden talep edebileceği) dijital varlık miktarını gösterir. Her bir dijital varlık bakımından bu hesap, itibari para cinsinden cari hesap gibi işler. Yatırımcı, dijital varlıklar üzerinde doğrudan bir tasarruf hakkına sahip değildir; yalnızca hesap sağlayıcısına karşı teminatsız kişisel bir alacak hakkına sahiptir. Eğer hesap sağlayıcısı iflas ederse, dijital varlıkların teslimine ilişkin alacak büyük olasılıkla itibari para cinsinden bir alacağa dönüştürülür ve diğer tüm teminatsız alacaklıların talepleriyle birlikte *pari passu* (eşit öncelikli) olarak değerlendirilir. Bununla beraber, bazı hukuk düzenlerinde dijital varlıkların bizzat kendisinin dağıtımına izin verilebilir. Eğer dijital varlık misli nitelikte değilse, ilgili alacak belirli bir varlığın teslimine yönelik olup; belirli bir türdeki dijital varlıkların genel olarak bir miktarına yönelik bulunmaz. Ancak bu durum, söz konusu yükümlülük için yapılan kişisel bir hak veya borçlunun iflasında teminatsız bir alacak hakkı hukuki nitelemesini değiştirmez.

10.21. Bir devlet, Açıklama 10.20'de belirtilen türde anlaşmalar yapan bazı veya tüm müşteri türleri bakımından riskin azaltılması için düzenleyici mahiyette hukuk kuralların (regülasyon) uygulama alanı bulup bulmayacağını değerlendirebilir. Buna bir örnek olarak, bu tür hesap hizmeti sağlayıcılarının belirli bir miktarda sermaye bulundurma zorunluluğu gösterilebilir. Bir başka örnek ise, hizmet sağlayıcının müşterilerine borçlu olduğu dijital varlıkların değeriyle orantılı kolayca paraya çevrilebilir (likit) değerleri bulundurma zorunluluğu olabilir; bu zorunluluğa, hesap hizmeti sağlayıcısının iflası durumunda müşteriler için bu tür varlıklar özelinde bir tercihte bulunma imkânı da eşlik edebilir. Diğer

örnekler, sözleşmede ilgili risklerin özel olarak açıklanması gerekliliği, bu tür hesap hizmeti sağlayıcılarının standartlara uygun biçimde oluşturulmuş kuruluşlar olması gerekliliği veya müşteri olabilecek kişilerin türüne ilişkin bir sınırlamalar (birçok kitle fonlaması düzenlemesinde olduğu gibi) olabilir.

Merkezi olmayan otonom kuruluşlar

10.22. Merkezi olmayan otonom kuruluşlar (DAO'lar) belirli dijital varlıkları kontrol etmek için bir blokzincir üzerinde depolanan ve yürütülen kodları (bunlar akıllı sözleşmeler veya uygulamalar olarak da adlandırılır) kullanır. Bir yatırımcı dijital bir varlığı belirli bir akıllı sözleşmeye aktarabilir, böylece bu akıllı sözleşme dijital varlığın nihai olarak ne zaman ve kime aktarılacağını belirler. İlgili durum, akıllı sözleşmeye konu olan dijital varlıkları kontrol eden kimliği belirlenebilir gerçek ya da tüzel bir kişinin bulunmaması halinde, kendi kendine saklama, saklama ve Açıklama 10.20'de belirtilen kişisel alacak talebi olasılıklarından farklıdır. Bazı hukuk sistemlerinde DAO bir tüzel kişi ya da bir trust olabilir yahut da akıllı sözleşmeler gerçek ya da tüzel kişiler tarafından kontrol edilir ve bu durumda ortada kimliği belirlenebilir bir kişi bulunur. Ancak, diğer durumlarda DAO, salt olarak gerçek ya da tüzel bir kişinin katılımı olmaksızın varlık bulan bir akıllı sözleşmeler ağıdır. Akıllı sözleşmenin işleyişi, blokzincir ağı üzerindeki katılımcılar arasında bir tür oylama veya mutabakata bağlı olabilir, ancak bu türden bir oylama veya mutabakat mekanizması, ilgili ağı katılma hakkına sahip tüm kişiler tarafından varlıkların ortak olarak kontrol edildiği anlamına gelmez. Bu paragrafta belirtilen nedenlerden ötürü, DAO içeren bir yapıda saklama anlaşmasının da yer alması pek olası değildir; fakat her durumda bu, öngörülen somut düzenlemenin içeriğine bağlı olarak değişkenlik gösterebilir.

İlke 11

Saklayanın müşteri karşısındaki yükümlülükleri

(1) Saklayan, müşterisi için muhafaza ettiği bir dijital varlıkla ilgili olarak ona karşı aşağıdaki yükümlülükleri üstlenir:

(a) saklayan, müşteri tarafından ve diğer hukuk tarafından izin verilmediği sürece, dijital varlığı devretme veya kendi yararına kullanma yetkisine sahip değildir;

(b) saklayan, aşağıdaki durumlar haricinde, müşteri tarafından dijital varlığın devri için verilen bir talimata uymakla yükümlüdür:

(i) saklayanın talimata uymasının, diğer hukuk tarafından veya müşterinin de tarafı olduğu veya onay verdiği saklayan ile üçüncü bir kişi arasındaki herhangi bir anlaşmayla yasaklanmış olması;

(ii) Saklayan, diğer hukuk veya müşteriyle yapılan bir anlaşma gereği, belirli koşullar altında, bu talimata uymak zorunda olmayabilir.

(c) saklayan dijital varlığı korumakla yükümlüdür.

(2) Saklama sözleşmesi veya diğer hukuk tarafından yasaklanmadığı sürece, bir saklayan, iki veya daha fazla müşterisi için, aynı özellikteki dijital varlıkları, bölünmemiş bir havuz yapısı dahilinde muhafaza edebilir.

(3) Bir saklayanın müşterisine karşı olan yükümlülükleri şunları da içerebilir:

(a) her bir müşteri için muhafaza edilen dijital varlıkların kaydının tutulması,

(b) dijital varlıkların müşteriler için tutulan kayıtlara uygun biçimde, her zaman güvenli ve etkin bir şekilde muhafaza edilmesi,

(c) (b) bendi kapsamındaki yükümlülüğün yerine getirilmesi için gerekli olması halinde dijital varlıkların derhal edinilmesi,

(d) müşteriler için muhafaza edilen dijital varlıkların saklayanın kendi hesabına muhafaza ettiği dijital varlıklardan ayrı tutulması,

(e) saklayana veya başka bir kişiye tanınan herhangi hakların saklı kalması kaydıyla, dijital varlıklardan doğan yararların, bu varlıkların lehine muhafaza edildiği müşteriye aktarılması.

(4) Bir müşteri veya diğer hukuk tarafından izin verildiği takdirde, bir saklayan bu İlke kapsamında müşterisine karşı olan yükümlülüklerini, alt saklayanın da bu İlkede belirtilen yükümlülüklerle bağlı olması koşuluyla, bir alt saklayan ile saklama sözleşmesi yaparak yerine getirebilir.

(5) Bir müşteri için saklayan tarafından muhafaza edilen bir dijital varlık, bir teminat hakkına konu oluşturabilir, bu:

- (a) müşteri tarafından o saklayan lehine tesis edilen bir teminat hakkı,*
- (b) saklayan lehine diğer hukuktan kaynaklanan bir teminat hakkı, veya*
- (c) müşteri tarafından üçüncü bir kişi lehine tesis edilen bir teminat hakkı olabilir.*

Açıklama

İlke 11(1)

11.1. İlke 11(1), bir müşteriyle yapılan bir anlaşma kapsamında saklama hizmeti sunan bir kişinin sahip olduğu yükümlülükleri belirler. Bu yükümlülükler temel bir nitelik arz ederler ve bir devlet bunların saklama sözleşmesi üzerinden bertaraf edilmesine izin vermemelidir. Eğer saklayan bir alt saklayan konumunda ise, alt saklayanın müşterisinin kendisi de yine bir saklayan konumunda olacaktır.

11.2. İlke 11 (1)(a)'daki yükümlülük, saklayanın dijital varlığı müşterinin ve diğer hukukun (İlke 2(4)'te tanımlandığı haliyle) izin verdiği durumlar haricinde kendi menfaati için kullanamaması hususunu düzenleme altına alır. Müşteri bu kullanıma sözleşmeyle veya saklayana talimat vererek rıza gösterebilir ve yine diğer hukukun izin verdiğinden daha sınırlı bir kullanıma onay verebilir. Bir devletin diğer hukuku da bir saklayanın saklama hizmeti verdiği dijital varlıklarla ilgili olarak kullanım hakkına sahip olmasına izin verebilir: Bu izin belirli bir düzenleyici mahiyetteki hukuk kuralları dahilinde ve/veya özel hukukta yer alabilir. İkinci durumda, iznin kapsamı bir saklama ilişkisinin söz konusu özel hukuk tarafından nasıl nitelendirildiğine bağlı bulunabilir.

11.3. İlke 11 (1)(b)'deki yükümlülük, bir saklayanın dijital varlıkla ilgili işlemler bakımından müşterinin talimatlarına göre hareket etmesi gereken bir kişi olduğu temel ilkesini ortaya koymaktadır. Ancak, bu yükümlülük, ceza hukuku veya düzenleyici mahiyetteki hukuk

kuralları da dahil olmak üzere diğer hukukta öngörülen herhangi bir yasakla ya da müşterinin doğrudan taraf olduğu veya saklayan ve üçüncü bir kişi arasında yapılmasına rıza gösterdiği herhangi bir sözleşmeyle sınırlanabilir. Müşteri, dijital varlık üzerinde saklamacıya bir teminat hakkı tanımışsa veya böyle bir teminat hakkı kanundan doğmuşsa, bu durum da saklayanın yükümlülüğünü sınırlar (bkz. İlke 11(5)). Ayrıca, diğer hukuk veya müşteriyle yapılan sözleşme, saklayanın belirli koşullar altında müşterinin talimatlarına uymak zorunda olmadığı durumları da düzenleyebilir. Bu tür hükümler, saklayanın temel yükümlülüğünü daha da sınırlandırır.

11.4. İlke 11(1)(c), saklayanın dijital varlıkların korunması bakımından müşteriye karşı belirli yükümlülükler üstlenmesi gerektiğini açıkça ortaya koymaktadır. Koruma kavramı, İlke 13(2)'de belirtilen sonucun sağlanmasını da içerir (Saklayanın iflas veya benzeri bir sürece girmesi hâlinde, saklamaya konu oluşturan varlıkların alacaklılara dağıtılacak varlıklar arasında yer almaması gerekmektedir). Belirtilen koruma yükümlülüklerinin ayrıntıları genellikle saklama sözleşmesinde düzenlenir. Bir devlet, saklayanlar bakımından özel hukuk kaynaklı hangi koruma yükümlülüklerinin öngörülebileceğini belirleme yetkisine sahiptir; bu nedenle ilgili yükümlülüklerin sözleşmeyle bertaraf edilmesine izin verilmez. devletler için öneri mahiyetindeki bazı düzenlemeler, İlke 11(3)'te yer almaktadır.

11.5. İlke 11 (1)'in dilinin işlevsel ve farklı hukuk kültürleri bakımından düşünüldüğünde tarafsız olması amaçlanmıştır. Bazı hukuk sistemlerinde saklayan ile müşteri arasındaki ilişki hukuki anlamda bir trust olarak nitelendirilirken, diğer bazı hukuk sistemlerinde aynı ilişki sözleşmeye dayalı veya başka türde bir hukuki ilişki olarak nitelendirilebilir.

İlke 11(2)

11.6. İlke 11(2), yaygın olarak karşılaşılan, bir saklayanın birden fazla müşteri için aynı türden dijital varlıkları muhafaza ettiği durumu ele almaktadır. Bu İlkeler dahilinde “aynı türden olma” ifadesi, piyasa katılımcıları tarafından misli nitelikte oldukları kabul edilen dijital varlıklar için kullanılmaktadır (ayrıca bkz. İlke 13(5)-13(7)). Misli olma, dijital varlığın teknik bir özelliği değildir, daha farklı olarak piyasa uygulamasına ilişkin bir konuyu oluşturur. Bir dijital varlığın herhangi bir birimi (veya miktarı) tanımı gereği kontrol edilebilir olduğu için dijital defterde kaydı bireyselleştirilmiş olarak tutulur (bkz. İlke 2(2)). Bununla birlikte, piyasa uygulaması gereği, birçok dijital varlık (kripto para birimleri gibi)

misli özellikte değerlendirilir, dolayısıyla bu tür varlıkların herhangi bir birimi veya birimleri, ilgili dijital varlığın teslimine ilişkin yükümlülüğün ifasını sağlayabilecektir.

11.7. Diğer hukuka veya saklama sözleşmesine tabi olmak üzere, İlke 11(2), bir saklayanın dijital varlıkları birden fazla müşteri için bölünmemiş bir havuz olarak tutmasına izin verir. Bunun iki sonucu vardır. Birincisi, saklayan bir ya da daha fazla özel anahtar kullanarak müşteri varlıklarından oluşan bölünmemiş bir havuzu kontrol edebilir, böylece söz konusu dijital varlığın belirli bir birimi ya da miktarı özellikle belirli bir müşteriye tahsis edilmez. Saklayanın bir alt saklayan nezdinde birden fazla müşteri için dijital varlık bulundurması halinde, bunların bölünmemiş bir havuz olarak muhafaza edilmesi, saklayanın her bir müşteri için alt saklayan nezdinde ayrı bir alt hesaba sahip olmasının gerekli bulunmadığı anlamına gelecektir. Sonuç olarak, herhangi bir dijital varlık için, bölünmemiş bir havuz, bir veya daha fazla özel anahtar kullanarak müşterileri için saklayan tarafından kontrol edilen bu tanımdaki tüm dijital varlıkların yanı sıra bir veya daha fazla alt saklayan nezdinde tutulan bu tanım dahilindeki tüm dijital varlıkları içerir. İkinci olarak, saklayan, müşterileri için bölünmemiş bir havuz olarak tutulan bir dijital varlıkla ilgili olarak bir müşteriden bir talimat aldığı anda, doğrudan kontrol ettiği veya bir alt saklayan nezdinde tuttuğu söz konusu dijital varlığın herhangi bir birimini veya miktarını kullanarak bu talimatı yerine getirebilir. Bunun nedeni, dijital varlığın bu türden çeşitli birimlerinin veya miktarlarının hepsinin aynı tanım altında değerlendirilebileceklerinin, yani yukarıda Açıklama 11.6'da ifade edildiği üzere, misli nitelik taşıdıklarının kabul edilmeleridir. Saklayanın dijital varlıkları bölünmemiş bir havuz yapısı dahilinde tutmasına izin verilmediği durumlarda, genellikle tam ayrıştırma olarak adlandırılan uygulamayı gerçekleştirmesi gerekir. İlke 11 (2)'de “bir saklayana” yapılan gönderme, müşterileri saklayan konumunda bulunan alt saklayanlar için de geçerlidir.

İlke 11(3)

11.8. İlke 11(3), bir devletin bir saklayanın müşteri karşısında altına girmesini isteyebileceği özel hukuk yükümlülüklerini belirler. Ancak bir devletin bu yönde bir tercihte bulunup bulunmamakta serbest olduğu ifade edilmelidir. Böyle bir tercihin takip edilmesi halinde, seçilen yükümlülüklerin zorunlu kılınması ve sözleşmeyle bertaraf edilemez hale getirilmelidir. Bundan ayrı olarak, bir devlet bu yükümlülükleri düzenleyici mahiyetteki kurallar çerçevesinde de saklayanlara yüklemeyi tercih edebilir. Anılan durumda

yükümlülük ihlali, özel hukuk yaptırımları yerine devlet tarafından uygulanacak kamusal mahiyetli yaptırımlara konu olur. Yine, saklayanın bir alt saklayan olması halinde müşterinin de bir saklayan olacağı hatırlanmalıdır. İlke 13(2)'de öngörülen sonuca bazı iç hukuklarda ulaşılabilmesi için, İlke 11(3)(d) kapsamındaki yükümlülüğün saklama sözleşmesinin şartları tarafından hariç tutulmasına izin verilmemesi gerekir. Bir devlet, benzer bir yükümlülüğü düzenleyici hukuk kuralları kapsamında getirmeyi de tercih edebilir.

11.9. İlke 11(3)(a) kapsamındaki yükümlülük, bir saklayanın her bir müşteri için muhafaza ettiği dijital varlıklara ilişkin kayıt tutma zorunluluğudur. Bu kayıt, ilgili dijital varlıkları gösteren dağıtık defterlerden ayrı olarak tutulabileceği gibi, teknoloji elverdiği takdirde dağıtık defterde saklanan bilgilerin bir parçası da olabilir.

11.10. İlke 11(3)(b) kapsamındaki yükümlülük, saklayanın bu kayıtlara karşılık gelen varlıkları muhafaza etme borcudur. Dolayısıyla, kayıtlar bir saklayanın A için 1 bitcoin muhafaza ettiğini gösteriyorsa, saklayanın en azından 1 bitcoini muhafaza etmesi gerekir.

11.11. İlke 11(3)(c) kapsamındaki yükümlülük, eksik olan varlıkların ikame edilmesi, başka bir ifadeyle saklayanın fiilen muhafaza ettiği varlıklar ile müşteri kayıtlarının uyumlu hâle getirilmesidir. İktisap edilecek varlıkların, kayıtlarda yer alan varlıklarla aynı nitelikte ve aynı miktarda olması gerekir.

11.12. İlke 11(3)(d) kapsamındaki yükümlülük, saklayanın müşteri varlıklarını öz varlıklarından (yani saklayanın kendi varlıklarından) ayırma yükümlülüğüne ilişkindir. Bir saklayan, müşterilerinin dijital varlıklarını kendi varlıklarından, bunları farklı özel anahtarlar kullanarak kontrol etmek suretiyle veya bir alt saklayan nezdinde farklı hesaplarda tutarak ayırabilir. Bunun hukuki sonucu, uygulanacak hukuka bağlıdır.

11.13. İlke 11(3)(d), belirli bir müşteriye ait varlıkların ayrıştırılmasını ele almamaktadır. bir saklayan, müşteri varlıklarını aynı türdeki varlıklar bakımından bölünmemiş bir havuz dahilinde tutmak yerine, bir müşteriye, o müşteriye ait varlıkların aynı türdeki diğer müşterilerin varlıklarından ayrı olarak muhafaza edilmesi imkânını sunabilir (tam ayrıştırma). Bu durumda saklayanın, müşterinin varlıklarını ayrı bir özel anahtar kullanarak kontrol etmesi veya bir alt saklayan nezdinde, söz konusu varlıkların münhasıran müşteriye

tahsis edilmesini sağlayacak ayrı bir hesapta tutması gerekir. Böyle bir düzenlemenin hukuki sonucu, uygulanacak diğer hukuka bağlıdır ve tabi olunan hukuk sistemine göre değişiklik gösterebilir.

11.14. İlke 11(3)(e) kapsamındaki, dijital varlıktan doğan tüm menfaatlerin müşteriye aktarılması yükümlülüğü, saklayana veya başka bir kişiye tanınmış olan hakka göre belirlenir. Bir dijital varlıktan doğan menfaatler; oy haklarını, temettüleri, ayni (para dışı) mahiyetteki dağıtımları (örneğin “*airdrop*”) ve çatallanma (“*fork*”) gibi ağ genelinde gerçekleşen bir olay sonucunda ortaya çıkabilecek ilave dijital varlıkları içerebilir.

İlke 11(4)

11.15. İlke 11(4), bir alt saklama yapısının kullanılabileceğini açıkça ortaya koymaktadır. Bu yapı kapsamında saklayan, ilgili dijital varlık bakımından bir alt saklayan ile bir saklama sözleşmesi akdetmek suretiyle dijital varlığı muhafaza eder (bkz. İlke 10(2) ve Açıklama 10.4). Böyle bir yapı, alt saklayanın İlke 11’de öngörülen yükümlülüklerle bağlı olması hâlinde kullanılabilir. Bununla birlikte, alt saklayanın, alt saklama sözleşmesi kapsamında, uygulanacak hukukun öngöreceği bir saklayan için öngörülen zorunlu ve sözleşme ile bertaraf edilemeyecek özel hukuk yükümlülüklerine tabi olmaması durumunda, saklayan müşterisine karşı kendi yükümlülüklerini ihlal etmiş sayılır. Bu yükümlülükler, İlke 11(1)’de yer alanlar ile ilgili devletin zorunlu kılmayı seçtiği İlke 11(3)’te sayılan yükümlülüklerdir. Alt saklayanın İlke 11 ve alt saklama sözleşmesi kapsamındaki yükümlülüklerini yerine getirmemesi hâlinde saklayanın müşterisine karşı ne ölçüde sorumlu olacağı, diğer hukuka göre belirlenir.

İlke 11(5)

11.16. İlke 11(5), bir saklayanın, bir müşteri için muhafaza ettiği dijital varlık üzerinde bir teminat hakkına sahip olabileceğini kabul etmektedir. Örnek olarak, müşteri saklayana, saklayanın teminat altına almak istediği ücretleri borçlu olabilir ya da saklayan dijital varlığın edinilmesi için müşteriye borç vermiş olabilir. İlke 11(5)(a) uyarınca bir teminat hakkı, İlke 15 kapsamında kontrol yoluyla üçüncü kişilere karşı hüküm ifade eder hâle getirilir; zira saklayan ya dijital varlığı bizzat kontrol etmektedir ya da söz konusu varlık bakımından bir alt saklayan ile bir saklama sözleşmesi akdetmiş bulunmaktadır. Bir

müşteri, saklayan tarafından muhafaza edilen bir dijital varlık üzerinde üçüncü bir kişi lehine de bir teminat hakkı tesis edebilir (bu husus, İlke 3(1) ve İlke 14(1)'de ortaya konulan dijital varlığın niteliğinden ileri gelmektedir). Ancak bu durumda, ya teminatlı alacaklının, dijital varlığı onun adına muhafaza eden saklayan aracılığıyla İlke 15 çerçevesinde dijital varlık üzerinde kontrolü sağlamak suretiyle teminat hakkını üçüncü kişilere karşı ileri sürülebilir hâle getirmesi ya da teminat hakkının, kontrol dışında, diğer hukuk tarafından öngörülen başka bir yöntem üzerinden üçüncü kişilere karşı hüküm ifade edebilir hâle getirilmesi gerekir.

İlke 12

Masum Müşteri

(1) Fıkra (2) düzenlemesi saklı kalmak kaydıyla, bir saklayanın bir dijital varlığı İlke 10(3) ve 10(4)'te tanımlandığı şekilde bir saklama sözleşmesi çerçevesinde muhafaza ettiği durumlarda, bu varlık özelinde malvarlıksal mutlak hak iddiasına dayalı hiçbir talep müşteriye karşı başarılı sonuç doğurabilecek biçimde yöneltilemez.

(2) Eğer saklayanın dijital varlığı onun için muhafaza ettiği zaman diliminde müşteri, başka bir kişinin dijital varlık üzerinde hak sahibi olduğunu ve gerçekleştirilen kazanımın bu kişinin hakkını ihlal ettiğini fiilen biliyorsa veya bilmesi gerekiyorsa, fıkra (1) uygulama alanı bulmaz.

(3) Eğer dijital varlıklar, bir saklayan tarafından iki veya daha fazla müşteri için bölünmemiş havuz yapısı dahilinde muhafaza ediliyorsa, fıkra (1) ve (2) dijital varlıkların muhafaza edildiği her bir müşteri bakımından geçerlidir.

Açıklama

12.1. İlke 12, bir saklayanın veya alt saklayanın bir dijital varlığın kontrolünü elde ettiği ve bu varlığı bir müşteri için veya varlığın bölünmemiş bir havuz yapısı dahilinde tutulması durumunda bir grup müşteri için muhafaza ettiği durumu düzenleme altına almaktadır (bu ikinci durum Açıklama 11.6 ve 11.7 ile İlke 11(2)'de ele alınmıştır). İlke 12 uyarınca, kontrolün saklayana geçmesiyle hakları ihlal edilen bir kişi tarafından söz konusu dijital varlık hakkında ileri sürülen bir talep, müşterinin bu hak ihlalini bildiği veya bilmesi gerektiği hâller dışında, müşteri bakımından başarılı sonuçlara ulaşamaz. Bu yönüyle İlke 12, masum iktisap kuralının, saklama ilişkisine özgü koşullara uyarlanmış bir görünümünü teşkil etmektedir. Bu bağlamda “masumiyet” standardı, İlke 8(5)(a)'da öngörülen paralel bir özellik gösterir. Bununla birlikte, İlke 8(1)(b) uyarınca bir devlet, bu standardı kendi hukuk sistemindeki iyiniyetle ve başkaca haklardan arı kazanım (*take free*) kurallarıyla uyumlu olacak şekilde belirlemek konusunda takdir yetkisine sahiptir. Son olarak, İlke 12, müşterinin bizzat dijital varlık üzerinde üçüncü bir kişi lehine bir hak tesis ettiği durumu kapsamamaktadır.

12.2. İlke 12, birden fazla saklama ilişkisi katmanının bulunduğu durumlarda, her bir saklama ilişkisi katmanı bakımından uygulanır. Bu çerçevede, alt saklayanın bir dijital

varlığı saklayan adına muhafaza etmesi (böyle bir durumda saklayan da söz konusu dijital varlığı bir müşteri adına muhafaza etmektedir, bkz. İlke 10(2)) İlke 12(1), alt saklayan karşısında müşteri konumunda bulunan saklayan bakımından uygulanır. Aynı zamanda, saklayanın söz konusu dijital varlığı müşteri adına muhafaza etmesi nedeniyle, İlke 12(1) saklayanın müşterisi bakımından da uygulanır.

12.3. Bir saklayanın müşteri adına bir dijital varlık üzerinde kontrol elde etmesinin çeşitli yolları bulunmaktadır. Somut olayın özelliklerine ve uygulanabilir hukukun bu durumu nasıl nitelendirdiğine bağlı olarak, müşterinin hukuki durumu ya İlke 8 ya da İlke 12 hükümlerine tâbi olacaktır. Olası bazı durumlara ilişkin örneklere aşağıdaki paragraflarda yer verilmektedir.

12.4. Örnek Durum 1. Bir saklayan, bir dijital varlığı kendi hesabına devralırken bu varlık üzerinde kontrol elde etmiş ve uygulama şartlarının da sağlanması itibarıyla İlke 8 uyarınca masum kazanımda bulunan sıfatını haiz olsun. Daha sonra, bunu izleyen bir satış işlemi kapsamında saklayan, dijital varlığı bir müşteriye devretmiş ve bu müşteri adına muhafaza etmeye başlamış olsun. Bu durumda İlke 12'nin uygulanmasına gerek bulunmamaktadır. Zira İlke 9(2) uyarınca, söz konusu dijital varlık hakkında saklayana karşı başarılı bir talep ileri sürülemez; dolayısıyla bu çerçevede saklayanın müşteri adına muhafaza ettiği dijital varlık bakımından müşteriye karşı da başarılı bir talebin ileri sürülebilmesi mümkün değildir. İlke 9(2), devralanın, devredenın sahip olduğu tüm malvarlıksal mutlak hakları kazanacağını öngörmektedir.

12.5. Örnek Durum 2. Bir müşterinin, bir dijital varlığın kendi adına edinilmesi için saklayana talimat verdiği ve saklayanın bu süreçte salt müşterinin vekili veya temsilcisi olarak hareket ettiği hâllerde, saklayanın kontrolünün müşteriye atfedilmesi ve müşterinin masum kazanımda bulunan sıfatını elde edebilmek için aranan diğer şartları da sağlaması kaydıyla, İlke 8 uyarınca müşteri masum kazanımda bulunan olarak kabul edilebilir.

12.6. Örnek Durum 3. Bir saklayanın Örnek 2'de belirtilenin dışında kalan durumlarda, bir dijital varlık üzerinde müşteri adına (veya bölünmemiş bir havuz yapısı dahilinde tutulacak dijital varlıklarda birden fazla müşteri adına; bkz. İlke 11(2)) muhafaza etmek üzere kontrol elde etmesi durumunda, İlke 12 uygulama alanı bulacaktır.

12.7. İlke 12, dijital varlığın birden fazla müşteri için bölünmemiş bir havuz yapısına dahilinde muhafaza ediliyor olup olmadığına bakılmaksızın uygulanır. Yine İlke 12(3)'te de ifade edildiği üzere, dijital varlıkların bölünmemiş bir havuz yapısı dahilinde muhafaza edilmesi durumunda da, İlke 12 her bir müşteri bakımından aynı şekilde uygulanır. Bu kapsamda, bir müşteri, ilgili havuzun parçasını oluşturan bir dijital varlık bakımından başka bir kişiye ait bir hakkın ihlal edildiğini bildiği veya bilmesi gerektiği durumlar dışında, söz konusu dijital varlık veya havuz yapısı dahilindeki diğer herhangi bir dijital varlık bakımından ona karşı herhangi bir talep ileri sürülemez. İlke 12, havuz yapısı dahilindeki müşterilerin birbirlerine karşı olan hukuki konumunu etkilemez. Bu konum, saklayanın iflası da dâhil olmak üzere (bkz. İlke 13(5) ve 13(7)), tüm müşterilerin havuzdan payları oranında ve orantılı biçimde yarar sağlamalarında somutlaşmaktadır.

İlke 13

Saklayanın İflası ve Alacaklıların Talepleri

(1) Bir saklayanın belirli bir saklama sözleşmesi kapsamında bir müşteri için muhafaza ettiği bir dijital varlık, saklayanın alacaklılarının taleplerinin karşılanması için kullanılamaz.

(2) Bir saklayanın iflasla ilgili bir sürece girmesi durumunda, onun belirli bir saklama sözleşmesi kapsamında bir müşteri için muhafaza ettiği bir dijital varlık, bu saklayanın alacaklılarına paylaştırılacak malvarlığı değerlerinin (varlıkların) bir parçasını oluşturmaz.

(3) Bir saklayan, bir müşteri için bir alt saklayan aracılığıyla dijital bir varlığı muhafaza ediyorsa ve saklayan iflasla ilgili bir sürece girerse, bu dijital varlıkla ilgili olarak saklayanın alt saklayana karşı sahip olduğu haklar, saklayanın alacaklılarına paylaştırılacak malvarlığı değerlerinin (varlıkların) bir parçasını oluşturmaz.

(4) Eğer bir saklayan iflasla ilgili bir sürece girerse, iflas idaresi aşağıdaki makul önlemleri almalıdır:

(a) saklayanın müşterisi için muhafaza ettiği bir dijital varlık üzerinde, ilgili müşteri veya onun tarafından tayin edilen bir saklayan lehine bir kontrol değişikliğinin gerçekleştirilmesi;

(b) saklayanın müşterisi için muhafaza ettiği bir dijital varlıkla ilgili olarak saklayanın herhangi bir alt saklayana karşı sahip olduğu hakların, söz konusu müşteri tarafından tayin edilecek başka bir saklayana devredilmesi de dahil olmak üzere, söz konusu müşteriye devredilmesi veya onun tarafından başka bir şekilde erişilebilir hale getirilmesi.

(5) Fıkra (6) ve (7) aşağıdaki tüm koşulların bir arada yerine getirilmesi halinde uygulanır:

(a) bir saklayanın iflasla ilgili bir sürece girmesi;

(b) aynı nitelikleri haiz dijital varlıkların saklayan tarafından iki veya daha fazla müşteri için bölünmemiş bir havuz yapısı dahilinde muhafaza edilmesi; ve

(c) iflas eden saklayan tarafından bu müşteriler için muhafaza edilen dijital varlıkların miktarı, onun bu müşteriler için muhafaza etmekle

yükümlü olduğu, aynı nitelikleri haiz dijital varlıkların toplam miktarından daha azdır (“eksiklik”).

[(6) Bu eksiklik, öncelikle saklayanın kendisi için muhafaza ettiği aynı nitelikleri haiz dijital varlıklardan karşılanır]¹.

(7) Herhangi bir [kalan] eksiklik, saklayanın dijital varlıkları lehlerine bölünmemiş bir havuz yapısı dahilinde muhafaza ettiği müşteriler tarafından, onun bu müşteriler için muhafaza etmekle yükümlü olduğu aynı nitelikleri haiz dijital varlıkların miktarı dikkate alınmak suretiyle orantılı olarak karşılanacaktır.

(8) Bir saklayan bir müşteri için bir dijital varlığı bir alt saklayan aracılığıyla muhafaza ediyorsa ve bu alt saklayan iflasla ilgili bir sürece girerse, saklayan anılan dijital varlığın kontrolünü iflas idaresinden almaya veya dijital varlığı başka bir alt saklayan aracılığıyla muhafaza etmeye çalışmalıdır.

Açıklama

İlke 13(1)

13.1. İlke 13(1), saklayanın iflasla ilgili bir sürece girmediği durumlarda uygulama alanı bulur. Bu hüküm, bir saklayanın bir müşteri adına muhafaza ettiği dijital varlıkların, saklayanın alacaklılarının taleplerinin karşılanması amacıyla kullanılamayacağını açıkça ortaya koymaktadır. Bu sonuç, saklayanın iflasla ilgili bir sürece girmesi hâlinde, müşteriler adına muhafaza edilen dijital varlıkların saklayanın alacaklılarına dağıtılabilecek malvarlığına dâhil olmadığını öngören ikinci paragrafın (fıkranın) özülüyle paralellik göstermektedir. Söz konusu hükümler, bu tür dijital varlıkların saklayana değil, müşterilere ait olduğu yönündeki temel ilkeyi yansıtmaktadır.

İflasla İlgili Süreç

13.2. İlke 13(2) – 13(8), bir saklayanın iflasla ilgili bir sürece girmesi hâlinde uygulanır. “İflasla ilgili süreç” kavramı İlke 2(6)’da tanımlanmıştır. Bununla birlikte, bir devletin belirli türdeki finansal kuruluşlar için, dijital varlık saklayanların bir kısmını da

¹ İlke 13 (6), bir devletin tercihi dahilinde benimseyebileceği bir hükümdür. Eğer bu yönde bir tercih kullanılırsa, ilke 13 (7)’de “kalan” ifadesinin muhafaza edilmesi gerekir.

kapsayabilecek özel bir iflas rejimi öngörebileceği göz önünde bulundurulmalıdır. Bu durumda, söz konusu özel rejim İlke 2(6)'daki tanım kapsamına girmiyorsa, devletin, bu saklayanlar bakımından “iflasla ilgili süreç” tanımını buna uygun şekilde değiştirmesi gerekecektir. Benzer şekilde, İlke 13'te öngörülen sonuçların bu özel rejim altında gerçekleşmesi mümkün değilse, İlke 13'ün de buna uygun olarak uyarlanması gerekecektir.

İlke 13(2)

13.3. İlke 13(2), saklayanın iflasının sonuçlarını, eşya veya mülkiyet gibi klasik hukuk kavramlarına başvurmaksızın, işlevsel bir yaklaşımla ortaya koymaktadır. Saklayanın iflası hâlinde, onun saklayan sıfatıyla müşteriler adına muhafaza ettiği dijital varlıklar, saklayanın alacaklılarına dağıtılabilecek malvarlığı değerlerine dâhil değildir. Buna karşılık, bir hizmet sağlayıcının müşteriyile yaptığı sözleşme, bir saklama sözleşmesi değil de dijital varlıkların teslimine ilişkin bir sözleşme niteliğinde ise (bkz. Açıklama 10.20'deki Örnek Durum 7), bu hizmet sağlayıcının kontrol ettiği varlıklar kural olarak alacaklılarına dağıtılacak malvarlığının bir parçasını oluşturur. Bir hizmet sağlayıcı, bazı müşteriler bakımından saklayan sıfatıyla hareket edebilir (İlke 10(1) anlamında “bu sıfatla hareket edilmesi”), ancak diğer müşteriler bakımından (sözleşmenin bir önceki cümlede belirtilen türde olması nedeniyle) saklayan sayılmayabilir. İlke 10(3) ve 10(4)'ün etkisi şöyle ortaya koyulabilir: İlke 10(3)'te sayılan saklama sözleşmesinin üç unsurunu da taşıyan her sözleşme, aksinin açıkça kararlaştırılmış olmaması hâlinde, İlke 13(2)'de öngörülen sonuçlara tâbi olur. Son olarak, İlke 13(2) bağlamında “saklayan” gerçekte bir alt saklayan, “müşteri” ise bir saklayan olabilir.

İlke 13(3)

13.4. İlke 13(3), bir dijital varlığın bir alt saklayan aracılığıyla muhafaza edilmesi hâlinde ortaya çıkan sonuçları düzenlemektedir (bkz. İlke 11(4)). Açıklama 10.4'te belirtildiği üzere, bir saklayanın bir dijital varlığı bir alt saklayan aracılığıyla muhafaza etmesi durumunda, saklayan (saklama sözleşmesi kapsamında alt saklayanın müşterisi sıfatıyla) alt saklayana karşı sözleşmeden doğan çeşitli haklara sahiptir. Saklayanın iflası hâlinde, onun alt saklayana karşı sahip olduğu bu haklar, saklayanın alacaklılarına dağıtılabilecek malvarlığı değerlerinin bir parçasını oluşturmaz.

İlke 13(4) – 13(7)

13.5. İlke 13(4) – 13(7), bir saklayanın iflasla ilgili bir sürece girmesi hâlinde, dijital varlıklar (veya alt saklayanın kullanıldığı durumlarda alt saklayana karşı haklar) bakımından uygulanması gereken -ya da İlke 13(6) bakımından uygulanabilecek- kurallara ilişkin yol gösterici nitelikte düzenlemeler içermektedir. Bu kurallar kapsamlı değildir; ilgili durumlarda ortaya çıkabilecek diğer tüm sorunlar, uygulanacak iflas hukuku tarafından belirlenir. Anılan bağlamda, bir saklayanın veya alt saklayanın, müşterileri adına muhafaza ettiği dijital varlıklar üzerinde bir teminat hakkına veya başka türden bir hakka sahip olabileceği de göz önünde bulundurulmalıdır (bkz. İlke 11(5)). Bu tür hakların, iflas idaresi temsilcisinin alacağı tedbirler üzerindeki etkisi, diğer hukuka göre belirlenecektir.

13.6. İlke 13(4), iflas idaresi temsilcisine, müşterinin saklayan tarafından kendisi adına muhafaza edilen dijital varlıklara erişimini sağlayabilmesi için makul adımları atma yükümlülüğünü yüklemektedir. Dijital varlıkların, saklayanın bir alt saklayan ile akdettiği saklama sözleşmesi aracılığıyla muhafaza edilmesi hâlinde (İlke 10(2)(b)), iflas idaresi temsilcisinin yükümlülüğü, saklayanın alt saklayana karşı sahip olduğu haklara ilişkindir. Müşteri, dijital varlıklar üzerinde kontrolü doğrudan kendisi elde etmek (veya alt saklayana karşı olan hakları devralmak) isteyebileceği gibi, bu varlıkların kendi adına başka bir saklayan tarafından muhafaza edilmesini de tercih edebilir. Bu sonucun sağlanabilmesi için iflas idaresi temsilcisinin, söz konusu dijital varlıklara ilişkin özel anahtarların temini gibi belirli işlemleri de gerçekleştirmesi gerekebilir.

13.7. İlke 13(5) – 13(7), aynı türdeki dijital varlıkların bir saklayan tarafından müşterileri adına bölünmemiş bir havuz yapısı dahilinde muhafaza edilmesi durumunda uygulanır (bkz. İlke 11(2) ve Açıklama 11.6). Aynı tür dijital varlıklardan oluşan bölünmemiş havuz yapılarına, Açıklama 11.6 ve 11.7’de değinilmektedir. Bir saklayan, dijital varlıkları bölünmemiş bir havuz yapısı dahilinde, ya varlıkları bizzat kontrol etmek suretiyle ya da belirli bir miktar dijital varlık bakımından bir alt saklayan ile bir saklama sözleşmesi akdetmek suretiyle muhafaza edebilir. Bu ikinci durumda, saklayanın alt saklayana karşı sahip olduğu haklar da bölünmemiş nitelikte olacaktır. İlkeler 13(5) – 13(7), belirli bir tür dijital varlık (veya alt saklayana karşı olan haklar) bakımından bir eksiklik bulunması hâlini düzenlemektedir. İlke 13(5), eksiklik durumunun ne anlama geldiğini açıklamaktadır. Bir

saklayanın iflasla ilgili sürecinde, mevcut bölünmemiş havuzların sayısı kadar farklı eksiklik durumunun ortaya çıkması da mümkündür.

13.8. Bir eksikliğin bulunması hâlinde, bir devlet, zararın öncelikle saklayanın kendi hesabına muhafaza ettiği aynı türden dijital varlıklardan karşılanmasını öngörmeyi tercih edebilir. Bu varlıklar, saklayanın bunları bizzat kontrol etmesi suretiyle ya da bir alt saklayan aracılığıyla muhafaza ediliyor olabilir. Bu yaklaşım, Cenevre Menkul Kıymetler Antlaşması'nın (*Geneva Securities Convention*) 25. maddesinde benimsenen yöntemi takip etmektedir. Bununla birlikte, anılan Antlaşma uyarınca bir devlet, bu kuralın kendi ülkesinde uygulanmayacağına ilişkin bir rezerv kaydı koyabilir. Benzer şekilde, İlke 13(6)'da öngörülen kuralın kabul edilip edilmeyeceği de bir devlet açısından bir hukuk politikası tercihidir. Bu nedenle, İlke 13(6) köşeli parantez içinde düzenlenmiştir.

13.9. İlke 13(7) uyarınca, eksiklik nedeniyle ortaya çıkan dijital varlık kaybı (veya alt saklayana karşı olan haklarda söz konusu olabilecek kayıp), saklayanın söz konusu varlıkları muhafaza etmekle yükümlü olduğu tüm müşteriler tarafından eşit sırada ve oranları nispetinde (*pari passu*) karşılanmalıdır. Başka bir ifadeyle, A dijital varlığına/veya A dijital varlığına ilişkin alt saklayana karşı olan haklara ilişkin bir eksiklik bulunmasına rağmen, B dijital varlığı bakımından herhangi bir eksiklik söz konusu değilse, A dijital varlığı bakımından ortaya çıkan eksiklik, saklayanın A dijital varlığını bölünmemiş bir havuz yapısı dahilinde muhafaza ettiği tüm müşteriler arasında payları oranında paylaşılır. Bu yaklaşım, Cenevre Menkul Kıymetler Antlaşması'nın (*Geneva Securities Convention*) 26(2). maddesinde benimsenen yöntemi esas almaktadır. Bir devletin İlke 13(6)'daki kuralı kabul etmesi hâlinde, İlke 13(7)'de köşeli parantez içinde yer alan “kalan” ibaresi devreye girer; aksi hâlde bu ibarenin kullanılmasına gerek bulunmaz.

İlke 13(8)

13.10. İlke 13(8), bir dijital varlığın bir alt saklayan aracılığıyla muhafaza edildiği hâllerde, alt saklayanın iflasının doğurduğu sonuçları düzenlemektedir (bkz. İlke 11(4)). Bu durumda saklayan, dijital varlık üzerindeki kontrolün iflas etmiş alt saklayandan alınarak ya kendisine ya da başka bir alt saklayana devredilmesini sağlamak için gerekli girişimlerde bulunmak zorundadır. Saklayanın da iflas etmiş olması hâlinde ise, onun saklama

sözleşmesi kapsamında alt saklayana karşı sahip olduğu haklar, saklayanın alacaklılarına dağıtılabilecek malvarlığına dâhil edilmez.

BÖLÜM V: TEMİNAT İŞLEMLERİ

İlke 14

Teminat işlemleri: Genel Bakış

- (1) Dijital varlıklar, teminat haklarının konusunu oluşturabilir.*
- (2) Bir dijital varlık başka bir malvarlığı değeri (varlıkla) bağlantılıysa, o dijital varlık üzerinde bir teminat hakkı kurulmasının söz konusu diğer malvarlığı değeri (varlık) üzerindeki hukuki etkisini tespit etmede diğer hukuk uygulama alanı bulur.*
- (3) Bir dijital varlık başka bir malvarlığı değeriyle (varlıkla) bağlantılıysa, bu dijital varlık üzerinde kurulan teminat hakkının üçüncü kişilere karşı ileri sürülebilir hale getirilmesinin diğer malvarlığı değeri (varlık) üzerindeki hukuki etkisini tespit etmede diğer hukuk uygulama alanı bulur.*

Açıklama

İlke 14(1)

14.1. İlke 14(1), dijital varlıkların (İlke 2(2)’de tanımlandığı üzere) malvarlıksal mutlak haklara konu olabileceğini düzenleyen İlke 3(1) üzerine inşa edilmiştir. Teminat hakları, malvarlıksal mutlak hak niteliğindedir, bu nedenle dijital varlıklar teminat haklarına konu edilebilir. İlke 14, teminatlı işlemler rejimlerinin, her tür taşınır varlığın teminat olarak kullanılmasına imkân tanınması gerektiğine ilişkin genel ilkeyi yansıtmaktadır. Bu yaklaşım, potansiyel teminatlı alacaklıların, hangi dijital varlıkların teminat değeri taşıdığına kendilerinin karar verebilmesine olanak sağlar.

14.2. Beşinci Bölüm, bir dijital varlık üzerinde bir teminat hakkının, teminat verenin veya üçüncü bir kişinin mevcut, gelecekte doğacak ya da şarta bağlı borçlarının ifasını güvence altına almak amacıyla teminatlı alacaklı lehine tesis edildiği işlemlere uygulanır. Beşinci Bölüm kapsamına giren bu işlemler, söz konusu Bölümün Açıklamalarında “teminatlı işlemler” olarak adlandırılmaktadır. Beşinci Bölümde yer alan İlkeler, dijital varlıklar üzerindeki teminatlarla ilgili olarak getirilmesi zaruri olan değişiklikler dışında, yerel hukuklarda teminat hakkına ve teminat hukukuna ilişkin mevcut kavramlara müdahale

etmeyi amaçlamamaktadır. Teminat haklarının malvarlıksal mutlak hak olma özelliklerine ilişkin birçok husus, diğer hukuk kurallarına tâbidir (bkz. İlkeler 3(3)(c), 3(3)(e) ve 3(3)(g)). İlkeler, teminat hakkının üçüncü kişilere karşı hüküm ifade eder hâle getirilmesinde kontrol dışındaki yöntemlerin mevcut olması (İlke 16’nın varsaydığı üzere) veya bir teminat hakkının paraya çevrilmesi sırasında teminat verenin ve üçüncü kişilerin önceden bilgilendirilmesi zorunluluğu gibi bazı kuralların varlığını varsaymakta ve bu kuralların dijital varlıklar üzerindeki teminat haklarının icrası bağlamında nasıl işleyeceğini açıklamaktadır.

14.3. Bu İlkeler, yalnızca UNCITRAL Teminatlı İşlemler Model Kanunu’nu (*UNCITRAL Model Law on Secured Transactions*) veya bu modele benzer yaklaşımları benimsemiş devletler için öngörülmemiştir. Dolayısıyla, “teminatlı işlemler” kapsamına giren işlem türleri ile “teminat hakkı” kavramına dâhil olan hak türleri, uygulanacak yerel hukuka göre belirlenecektir. Örneğin, “teminatlı işlemler” kavramı genellikle rehin, ipotek benzeri yükler veya teminat amaçlı temlik gibi çeşitli teminat haklarını tesis eden işlemleri kapsar. Bunun yanı sıra, kesin (tam) devir işlemlerini de içerebilir; bu tür devirlerin “teminatlı işlemler” kapsamında değerlendirilip değerlendirilmeyeceği, yerel hukuktaki teminatlı işlemlere yönelik düzenlemelere bağlıdır. Nitekim UNCITRAL Teminatlı İşlemler Model Kanunu ile bazı ulusal teminatlı işlemler mevzuatları, alacakların kesin devrini de kapsama almaktadır. Cenevre Menkul Kıymetler Sözleşmesi (*Geneva Securities Convention*) ise, aracı nezdinde tutulan menkul kıymetler üzerinde teminat hakkı tesis edilmesi veya mülkiyet devrine dayalı teminat sözleşmeleri yoluyla kurulan teminat işlemlerini kapsamaktadır. Bazı yerel hukuk sistemleri, bir borcun teminat altına alınması amacıyla varlığın “mülkiyetinin” alacaklıya devredildiği güvene dayalı mülkiyet devri türü düzenlemeler öngörmektedir. Dijital varlıkların kesin devri, farklı bağlamlarda kullanılabilir. Bu nedenle, teminatlı işlemler hukukunun, bir devletin dijital varlıkların kesin devrine ilişkin genel kurallarıyla uyumlu şekilde koordine edilmesi önem taşımaktadır. Yerel hukuklar arasındaki bir diğer farklılık alanı, bir teminat hakkının üçüncü kişilere karşı hüküm ifade eder hâle getirilmesinin, teminat hakkının kurulmasından ayrı bir aşama olarak görülüp görülmediğine ilişkindir. Bazı hukuk düzenlerinde, kimi teminat hakları kurulduğu andan itibaren üçüncü kişilere karşı ileri sürülebilir hâle gelmektedir. Bu tür hukuk sistemlerinde, bu İlkelerde teminat hakkının üçüncü kişilere karşı hüküm ifade eder hâle getirilmesine yapılan atıflar, teminat hakkının kurulmasına yapılmış atıflar olarak anlaşılmalıdır (Ayrıca bkz. Açıklama 14.8).

14.4. Bu İlkelerin kabulü sürecinde, bir devletin mevcut teminatlı işlemler mevzuatında, Beşinci Bölümde öngörülen dijital varlıklara özgü özel kuralları içerecek şekilde değişiklik yapmasını gerektirebilir. Bu çerçevede, söz konusu özel kuralların uygulanacağı dijital varlığın, İlke 2(2)'de yer alan tanım esas alınarak belirlenmesi gerekir. Örneğin, UNCITRAL Teminatlı İşlemler Model Kanunu (veya buna benzer bir ulusal teminatlı işlemler mevzuatı) kapsamında, bu durum, dijital varlıkların, hâlihazırda genel kuralların uygulandığı daha geniş “gayrimaddi varlıklar” kategorisinden ayrılması sonucunu doğuracaktır (örneğin, üçüncü kişilere karşı hüküm ifade etmenin yalnızca tescil yoluyla sağlanması). Bu yaklaşım, belirli varlık türleri (örneğin mevduat hesapları) bakımından öngörülmüş olabilecek varlığa özgü kuralları (örneğin üçüncü kişilere karşı hüküm ifade etmenin kontrol yoluyla sağlanması) tamamlayıcı nitelikte olacaktır. Bir dijital varlığın başka bir varlıkla (“diğer varlık”) bağlantılı olması hâlinde, söz konusu diğer varlık, bir devletin iç hukukunda “menkul kıymetler” gibi belirli bir kategori kapsamında yer alabilir (bağlantının varlığı ve hukuki etkisinin diğer hukuka tâbi olduğu göz önünde bulundurulmalıdır; bkz. İlke 4). Bağlantının niteliği, diğer hukuk çerçevesinde, bağlantılı dijital varlığın da emre yazılı veya hamiline yazılı senetler ya da kıymetli evrak gibi belirli bir varlık kategorisine dâhil edilmesine yol açabilir (bkz. Açıklama 4.22). Bu tür durumlarda, ilgili varlık kategorisine özgü teminatlı işlemler kuralları, uygun düştüğü ölçüde ya diğer varlığa ya da dijital varlığın kendisine uygulanacaktır.

14.5. Devletler, dijital varlıklara özgü kurallar öngörmeyi değerlendirmelidir. Bu kurallar, dijital varlıkları bir teminat türü olarak genel nitelikte kapsayabileceği gibi, bağlantılı dijital varlıkların çeşitli alt kategorileri bakımından ayırt edici ek düzenlemeler de içerebilir. Bununla birlikte, devletlerin, çok sayıda bağlantılı dijital varlık kategorisi için ayrı ayrı teminatlı işlemler kuralları öngörerek karmaşık bir sistem oluşturma yoluna da gitmemesi gerekir. İlke 6'da düzenlenen kontrol kavramı, bağlantılı olsun ya da olmasın, tüm dijital varlık türleri bakımından teminat haklarının üçüncü kişilere karşı hüküm ifade etmesinde eşit şekilde uygulanmalıdır (bkz. İlke 15).

14.6. Beşinci Bölümde yer alan İlkeler, dijital varlıklar üzerindeki teminat haklarına ilişkin olarak üçüncü kişilere karşı hüküm ifade etme, öncelik ve icra gibi belirli hususları düzenlemektedir. Bununla birlikte, teminatlı işlemlere ilişkin pek çok mesele, İlke 2(4)'te

tanımlanan diğer hukuka tâbidir. Teminatlı işlemlerin aynî yönlerine uygulanacak hukuku belirleyen kurallar ise, İlke 5(1)'de (İlke 5(5) saklı kalmak kaydıyla) düzenlenmiştir.

14.7. Örnek Durum 1. X devleti'nin teminatlı işlemler hukuku, dijital varlıkları daha geniş bir “gayrimaddi varlıklar” kategorisinden ayrı tutmamaktadır. Kontrol, bir teminat hakkının üçüncü kişilere karşı hüküm ifade eder hâle getirilmesinde tanınan bir yöntem olmakla birlikte, yalnızca banka hesapları ve aracı nezdinde tutulan menkul kıymetler bakımından mümkündür. Bu nedenle, bir dijital varlık üzerinde kontrol sahibi olan bir teminatlı alacaklının, teminat hakkını üçüncü kişilere karşı ileri sürebilmek için tescil yoluna başvurması gerekebilir. Bu İlkelerin uygulanması sonrasında ise, bu tescil kaydı, üçüncü kişilere aleniyet sağlanması bakımından gereksiz bir adım hâline gelecektir. Zira aktarılan durumda, teminatlı alacaklı İlke 6 anlamında dijital varlık üzerinde kontrol sahibidir ve bu kontrol, İlke 15 uyarınca teminat hakkının üçüncü kişilere karşı hüküm ifade etmesi için yeterlidir.

İlke 14(2) ve 14(3)

14.8. İlke 14(2) ve 14(3), dijital bir varlık ile başka bir varlık (ister fiziki dünyaya ait bir varlık ister başka bir dijital varlık olsun) arasındaki herhangi bir bağlantının varlığı, şartları ve hukuki sonuçlarının diğer hukukun konusu olduğunu öngören İlke 4'ü yansıtmaktadır. Örneğin, dijital bir varlık ile fiziki dünyaya ait bir varlık arasındaki bağlantı, diğer hukuk kuralları uyarınca kıymetli evrak niteliğinde bir belge olarak tanınıyorsa, dijital varlık üzerinde bir teminat hakkının kurulması ve üçüncü kişilere karşı hüküm ifade etmesi, fiziki dünyaya ait varlığa da etki edecektir. Buna karşılık, böyle bir tanıma söz konusu değilse, teminat hakkı yalnızca dijital varlığın kendisiyle sınırlı kalacaktır. Bu yaklaşım, UNCITRAL Teminatlı İşlemler Model Kanunu'nun, kıymetli evrak üzerinde kurulan teminat hakkının evrakın temsil ettiği eşyalara da genişletilebileceğini öngören 16. maddesiyle uyumludur. Ancak anılan Model Kanun, “kıymetli evrak” kavramını tanımlamamaktadır; zira bu husus teminatlı işlemler hukukunun değil, diğer hukuk dallarının konusudur. Ayrıca İlkeler 14(2) ve 14(3), UNCITRAL Teminatlı İşlemler Model Kanunu'nun 17. maddesinde benimsenen yaklaşımı izlemektedir. Buna göre, bir varlık üzerindeki teminat hakkı, “bağlantılı bir varlığa” kendiliğinden etki etmez; örneğin fikri hak üzerindeki bir teminat, bu hakkın ilgilendirdiği maddi varlık üzerinde etki doğurmaz. Dolayısıyla, diğer hukuk iki varlık arasında hukuken geçerli bir bağlantı kurmadıkça,

bunlardan biri üzerinde teminat hakkı tesis edilmesi, diğerini etkilemez. Gerçek (fiziki) dünyaya ait bir varlık üzerinde tesis edilen ve dijital bir varlıkla bağlantılı olduğu ileri sürülen teminat hakları ise, bu İlkelerin kapsamı dışındadır, zira bu İlkeler yalnızca dijital varlıkları konu almaktadır. Açıklama 14.2’de belirtildiği üzere, bu İlkeler yerel hukuklardaki teminat hakkı yapılarına müdahale etmemektedir. Bazı hukuk sistemlerinde teminat hakkının kurulması ile üçüncü kişilere karşı hüküm ifade etmesi birbirinden ayrılmaz niteliktedir (bkz. Açıklama 14.3). Bu tür hukuk düzenlerinde, İlke 14(3)’ün ayrıca uygulanmasına gerek bulunmayabilir.

14.9. Örnek Durum 2. X devleti’nde bir fatura, altta yatan ödeme alacağını temsil eden (kapsayan) bir belge olarak kabul edilmemektedir. Faktör A, nitelikli inceleme amacıyla dijital faturalar üzerinde düzenli olarak kontrol sağlamaktadır. Bu durum, ne alacak üzerinde bir teminat hakkı doğurur ne de böyle bir hakkı üçüncü kişilere karşı hüküm ifade eder hâle getirir. Buna karşılık Faktör B, dijital varlık biçiminde düzenlenen faturalar kapsamındaki alacaklar üzerinde düzenli olarak teminat hakkı tesis etmektedir ve bu teminat hakları üçüncü kişilere karşı hüküm ifade etmektedir. Ancak bu durum, dijital varlık niteliğindeki faturalar üzerinde bir teminat hakkı doğurmaz ve böyle bir hakkı üçüncü kişilere karşı ileri sürülebilir hâle getirmez. Dolayısıyla uygulamada, alacak ile fatura arasında hukuken geçerli bir bağlantı bulunmadığı için, dijital fatura üzerindeki bir teminat hakkı, tıpkı ödeme alacağını temsile elverişli bulunmayan kâğıt bir fatura üzerindeki teminat hakkı gibi, herhangi bir teminat değeri taşımayacaktır.

İlke 15

Üçüncü Kişilere Karşı İleri Sürülebilirliği Sağlama Yöntemi Olarak Kontrol

Bir dijital varlık üzerindeki teminat hakkı, aşağıdaki koşullardan birinin sağlanması halinde, kontrol yoluyla üçüncü kişilere karşı ileri sürülebilir hale getirilebilir:

- (a) teminatlı alacaklı, İlke 6'da tanımlandığı şekilde dijital varlık üzerinde kontrole sahipse; veya*
- (b) bir saklayan, İlke 10(2)'de belirtildiği şekilde dijital varlığı teminatlı alacaklı için muhafaza ediyorsa.*

Açıklama

Üçüncü Kişilere Karşı Hüküm İfade Etme (İleri Sürülebilirliği Sağlama) Yöntemi Olarak Kontrolün Tercih Edilme Gerekçeleri

15.1. İlke 15, dijital bir varlık üzerindeki teminat hakkının, diğer hukuka göre uygulanabilir olan üçüncü kişilere karşı hüküm ifade etme yöntemlerine ek olarak, kontrol yoluyla da üçüncü kişilere karşı ileri sürülebilir hâle getirilebileceğinin bir devlet tarafından kabul edilmesi gerektiğini öngörmektedir. Bu durum, teminatlı alacaklının dijital varlık üzerinde bizzat kontrol sahibi olduğu hâllerde olduğu gibi, bir saklayanın -alt saklayan dâhil olmak üzere- dijital varlığı teminatlı alacaklı adına muhafaza ettiği durumlarda da geçerlidir. Genel olarak üçüncü kişilere karşı hüküm ifade edebilirlik, teminatlı alacaklının teminat hakkını alenileştirmeye yönelik bir adım atmasını gerektirir. Bu adımlar arasında, örneğin zilyetliğin devri, borçlunun bildirilmesi, tescil ve kontrol yer alabilir. Ancak bu yöntemlerden bazıları dijital varlıklar bakımından uygulanabilir değildir (örneğin maddi bir eşyanın zilyetliğinin teslim yoluyla devri).

15.2. Birçok devlette, tescil, çoğu (hatta tüm) varlık türleri bakımından teminat hakkını üçüncü kişilere karşı hüküm ifade eder hâle getiren bir yöntem olmakla birlikte (örnek olarak UNCITRAL Teminatlı İşlemler Model Kanunu kapsamındaki tüm taşınırılar bakımından), kripto ödöncü piyasasında tescil uygulamasına yaygın olarak başvurulmamaktadır. Bu durum, gerçekleştirilen işlem bakımından belirli bir kredi riskini doğurmaktadır. Ayrıca, teminat haklarına ilişkin bir tescil sisteminin bulunmadığı

devletlerde, piyasa katılımcıları üçüncü kişilere karşı hüküm ifade edebilirliğe ilişkin mevcut şartların farkında olmayabilir ya da bu şartlar, piyasa uygulamaları açısından bir engel teşkil edebilir.

15.3. Piyasa katılımcıları, teminat altına alınmış dijital varlığa borçlunun erişimini engellemek amacıyla genellikle bazı fiili önlemler almaktadır. Bu önlemler çoğunlukla, dijital varlığın borçlunun cüzdanından teminatlı alacaklının cüzdanına aktarılması veya çoklu imza gibi düzenlemeler yoluyla teminatlı alacaklının kontrolü altına alınması şeklinde ortaya çıkmaktadır. Bazı hukuk sistemlerinde bu tür adımlar, dijital varlık üzerindeki teminat hakkının üçüncü kişilere karşı hüküm ifade etmesini sağlayan bir yöntem olarak hâlihazırda tanınmaktadır. Bu durumda, teminatlı alacaklının veya onun temsilcisinin kontrolündeki bir cüzdana yapılan aktarım, borçlunun iflası hâli de dâhil olmak üzere, teminat hakkını üçüncü kişilerin taleplerine karşı korumak için yeterli olacaktır. Bu İlkeler, yerel hukuklardaki teminat hakkı yapılarına müdahale etmediğinden, iflas hâlindeki koruma; teminat hakkının üçüncü kişilere karşı hüküm ifade etmesi ve önceliğinin tanınması yoluyla veya dijital varlığın teminatlı alacaklıya kesin olarak devredilmiş olması nedeniyle borçlunun malvarlığından hariç tutulması suretiyle sağlanabilir. Buna karşılık, bu tür fiili adımları tanımayan hukuk düzenlerinde, tescilin yapılmamış olması teminatlı alacaklı açısından son derece ağır sonuçlar doğurabilir. Her hâlükârda, üçüncü kişilere karşı hüküm ifade edebilirliğe ilişkin mevcut şartlar, dijital varlıkları teminat olarak kabul eden sistemler bakımından hukuki belirsizlik yaratabilmektedir.

15.4. Teminatlı işlemler hukuku ve bağlantılı düzenlemeler, bazı varlık türleri bakımından, bir varlık üzerindeki kontrol değişikliğinin, ister kesin devir ister teminat amacıyla olsun, varlığın devri için yeterli olmasını zaten öngörebilmektedir. Hukukun, belirli taşınır varlık türleri bakımından kontrolün bir görünümünü tanıdığı durumlarda, bu kapsama giren dijital varlıklar üzerindeki teminat hakları da aynı kontrol yöntemiyle üçüncü kişilere karşı hüküm ifade eder hâle getirilebilir. Örneğin, aracı nezdinde tutulan menkul kıymetlerle bağlantılı dijital varlıklar bakımından, bağlantının diğer hukuk alanları çerçevesindeki etkisine bağlı olarak böyle bir sonuca ulaşılabilir. Bununla birlikte, teminatlı işlemler hukukunda kontrol mekanizmaları öngörülmemiş olan çok sayıda dijital varlık türü bulunması muhtemeldir.

15.5. Geçmişte, belirli varlık türleri üzerindeki teminat haklarını düzenleyen rejimler, ortaya çıkan sektör uygulamalarını yansıtacak şekilde değiştirilmiştir (örneğin finansal teminatın tutulduğu menkul kıymet hesaplarındaki kayıt esaslı sistemler). Açıklama 15.3'te de belirtildiği üzere, kripto ödöncü piyasasında hâkim olan uygulamalar, tescil ve üçöncü kişilere karşı hüküm ifade edebilirliğin sağlanmasına yönelik geleneksel yöntemlere dayanmamaktadır.

Üçöncü Kişilere Karşı İleri Sürülebilirliği Temin Etme Yöntemi Olarak Kontrol

15.6. Bir devlet, dijital varlıklara ilişkin mevzuatının başka bölümlerinde İlke 6'da yer alan kontrol tanımına atıfta bulunmalı; böyle bir atıf bulunmuyorsa, dijital bir varlık üzerindeki teminat hakkının üçöncü kişilere karşı hüküm ifade etmesini sağlayan bir araç olarak İlke 6'daki kontrol tanımını teminatlı işlemler hukukuna dâhil etmelidir. Bu tanım kapsamında kontrol, teminatlı alacaklının dijital varlık bakımından belirli bir yetkiler bütününe elde etmesi hâlinde mevcuttur. İlke 15, İlke 6(3) ve İlke 10(2) ile birlikte değerlendirildiğinde, teminatlı alacaklının gerekli yetkileri doğrudan, üçöncü kişi bir saklayan aracılığıyla ya da çoklu imza düzenlemelerinde olduğu gibi diğer taraflarla iş birliği içinde kullanabileceğini öngörmektedir (bkz. Açıklama 6.13). Kontrolün, bir teminat hakkının üçöncü kişilere karşı hüküm ifade etmesinin bir yöntemi olarak bir devletin hukukuna dâhil edilmesi, öncelik kurallarının yapısını etkileyecek olup bu husus İlke 16'da ele alınmakta; ayrıca teminatın paraya çevrilmesini kolaylaştırarak İlke 17'de incelenen icra süreçlerini desteklemektedir.

15.7. Teminatlı işlemler hukukunda, kontrolün İlke 15 ile uyumlu biçimde tanınması, uygulanacak hukukta üçöncü kişilere karşı hüküm ifade etmenin birden fazla yönteminin bulunması sonucunu doğurabilir. Bir dijital varlık, teminatlı işlemler hukukunun üçöncü kişilere karşı hüküm ifade etme için bir veya daha fazla yöntem öngördüğü bir varlık türü kapsamına giriyorsa, teminat hakkı bu yöntemlerden herhangi biriyle üçöncü kişilere karşı ileri sürülebilir hâle getirilebilir. İlke 15, bir devletin, kendi teminatlı işlemler hukukunun genel ilkeleri ile uyumlu olmak kaydıyla, dijital varlıklar üzerindeki teminat hakları bakımından kontrolü tek ve yegane yöntem olarak belirlemesini de engellememektedir (örneğin, bir devletin mevduat hesapları üzerindeki teminat hakları bakımından üçöncü kişilere karşı hüküm ifade etmenin tek yolunun kontrol olduğunu öngörmesi gibi).

15.8. Bu İlkeler kapsamında kontrol, teminat hakkının üçüncü kişilere karşı hüküm ifade etmesini sağlamak amacıyla üç farklı durumda kullanılabilir. Birinci olarak, teminatlı alacaklı, İlke 6’da öngörülen gerekli yetkileri doğrudan edinebilir. İkinci olarak, teminatlı alacaklı bu yetkileri üçüncü kişilerle paylaşabilir; bu durum da İlke 6 anlamında kontrol teşkil eder (bkz. ayrıca Açıklama 6.11). Üçüncü olarak ise, hâlihazırda kontrol sahibi olan bir taraf (örneğin bir saklayan), ilgili yetkileri teminatlı alacaklı adına kullanmayı kabul edebilir. Bu üçüncü duruma örnek olarak, bir saklayanın, bir dijital varlığı, bir alt saklayan ile akdettiği saklama sözleşmesi çerçevesinde müşteri adına muhafaza etmesi hâli gösterilebilir (bkz. İlke 10(2)).

Teminatlı Alacaklı ile Borçlu Arasında Paylaşılan Kontrol

15.9. Açıklama 15.9 – 15.13, teminatlı alacaklı ile borçlunun, İlke 6(1)(a)’da belirtilen yetkileri paylaştıkları durumu ele almaktadır (bu durum, Açıklama 15.8’de belirtilen ikinci ihtimal kapsamındadır). İlke 6(3), bu yetkilerin birden fazla taraf arasında paylaşılmasının, kontrolün varlığını ortadan kaldırmayacağını öngörmektedir. Bununla birlikte, bir kişi fiilen bu yetkilere sahip olsa dahi, bir sözleşme sonucunda bu yetkilerden birini veya birkaçını kullanma hakkı hukuken sınırlandırılmış olabilir.

15.10. Bazı (dijital olmayan) varlıklar bakımından, diğer hukuk, teminatlı alacaklı ile teminat veren arasında varlığın tasarrufuna ilişkin yetkinin belirli ölçüde paylaşılmasını, teminat hakkının kontrol yoluyla üçüncü kişilere karşı hüküm ifade etmesini zedelemeyen kabul edebilmektedir. Bu durum, devletten devlete farklılık gösterebilir. Örneğin, bir banka hesabı üzerindeki teminat hakkı üçüncü kişilere karşı hüküm ifade edebilir; buna rağmen kontrole ilişkin anlaşma, teminatlı alacaklı saklayana teminat verenin talimatlarının yerine getirilmemesi yönünde bildirimde bulunana kadar, teminat verene varlık üzerinde tasarruf yetkisi tanıyabilir.

15.11. İlke 15, devletlere, üçüncü kişilere karşı hüküm ifade etme kurallarını, İlke 6 ile uyumlu olacak şekilde fiili yetkilerin paylaşımı esasına göre tasarlamalarını önermektedir. Teminatlı alacaklının fiili yetkileri kullanma hakkına getirilen sınırlamalar, onun kontrolünün üçüncü kişilere karşı hüküm ifade etme bakımından yeterli olmasını engeller. Bu tür sınırlamalara örnek olarak, teminatlı alacaklının dijital varlık üzerinde fiilen tasarruf

edememesi veya teminatlı alacaklının, sözleşme gereği, borçlunun rızası olmaksızın dijital varlık üzerinde tasarrufta bulunmasının yasaklanmış olması halleri gösterilebilir.

15.12. Bir devlet, diğer varlıklar bakımından teminat haklarının üçüncü kişilere karşı hüküm ifade etmesine ilişkin olarak benimsenmiş yaklaşımı (bkz. Açıklama 15.10) dijital varlıklara da uygulamayı tercih edebilir. Bu durumda, bazı devletlerde, teminatlı alacaklının borçlunun temerrüdü hâlinde kontrolü kullanabilecek bir konumda bulunması yeterli görülebilir; bu sürece kadar borçlu, fiili yetkileri kullanma hakkını muhafaza edebilir. Buna karşılık, bazı devletler, üçüncü kişilere karşı ileri sürülebilirliğin sağlanması için borçlunun fiili yetkileri kullanma hakkına hiç sahip olmamasını şart koşabilir. Bu husus, ilgili devletin takdirine bağlı bir hukuk politikası tercihidir.

Kontrolle İlişkin Örnekler

15.13. Örnek Durum 1. İlkeleri iç hukukuna aktarmamış olan A devleti'nde, bir teminatlı alacaklı, bir dijital varlık portföyü üzerinde teslim bağli bir rehin tesis etmektedir. Uygulanacak hukuk, dijital varlıklar bakımından teminat hakkının üçüncü kişilere karşı hüküm ifade etmesini sağlayan özel bir mekanizma öngörmemekte; buna karşılık, teminat olarak verilen tüm gayrimaddi varlıklar bakımından üçüncü kişilere karşı hüküm ifade etmenin tek yolu olarak tescili kabul etmektedir. Teminatlı alacaklı, borçlusundan, ilgili dijital varlığı çoklu imza düzenlemesi yoluyla kontrolü teminatlı alacaklıda bulunan üçüncü bir cüzdana aktarmasını talep etmiş; ancak herhangi bir tescil gerçekleştirmemiştir. Daha sonra borçlu, iflasa ilişkin bir sürece girmiştir. Bu durumda teminatlı alacaklı, A devleti hukukuna uygun şekilde hakkın üçüncü kişilere karşı ileri sürülebilirliğini sağlayamadığından, teminat hakkını kaybetme riskiyle karşı karşıya kalabilir. Buna karşılık, bu İlkeleri hukukuna aktarmış olan B devleti'nde, teminatlı alacaklı, borçlunun iflası hâlinde etki doğurabilecek biçimde, kontrol yoluyla teminat hakkını üçüncü kişilere karşı hüküm ifade eder hâle getirebilirdi.

15.14. Örnek Durum 2. Dijital varlıkların bir saklayan tarafından bir müşteri adına muhafaza edildiği bir durumda, saklayan, kontrol yetkilerini teminatlı alacaklı adına kullanmayı taahhüt etmektedir. Eğer ilgili devlet, “kontrol”ü teminatlı işlemler rejiminde üçüncü kişilere karşı ileri sürülebilirliğin sağlanmasında bir yöntem olarak kabul etmişse, bu hâlde teminat hakkı üçüncü kişilere karşı geçerli olacaktır.

İlke 16

Teminat Haklarının Önceliği

Bir dijital varlık üzerinde, İlke 15 uyarınca kontrol yoluyla üçüncü kişilere karşı ileri sürülebilir hale getirilen bir teminat hakkı, kontrol dışındaki herhangi bir yöntemle üçüncü kişilere karşı geçerli hale getirilen bir teminat hakkına göre önceliğe sahiptir.

Açıklama

Kontrolü Elinde Bulunduran Teminatlı Alacaklının Önceliği

16.1. İlke 16, bir teminatlı alacaklının dijital bir varlık üzerindeki teminat hakkını tescil veya uygulanacak hukuk uyarınca tanınan başka bir yöntemle üçüncü kişilere karşı hüküm ifade eder hâle getirdiği, ancak dijital varlık üzerinde kontrolü elde etmediği; buna karşılık başka bir teminatlı alacaklının da aynı dijital varlık üzerindeki teminat hakkını kontrol yoluyla (İlke 15 uyarınca) üçüncü kişilere karşı hüküm ifade eder hâle getirdiği durumu düzenlemektedir. Bu durumda İlke 16, kontrol yoluyla teminat hakkını üçüncü kişilere karşı ileri sürülebilir kılan teminatlı alacaklının, kontrolü elde etme adımını diğer teminatlı alacaklının tescil yaptırmamasından veya teminat hakkını başka bir yöntemle üçüncü kişilere karşı ileri sürülebilir hale getirmesinden sonra atmış olsa dahi önceliğe sahip olacağını öngörmektedir. Bu düzenleme, UNCITRAL Teminatlı İşlemler Model Kanunu'nda (*UNCITRAL Model Law on Secured Transactions*) ve birçok Devlet hukukunda benimsenen genel kuraldan ayrılmaktadır. Anılan genel kurala göre, aynı varlık üzerindeki birden fazla teminat hakkı arasındaki öncelik, teminat hakkının üçüncü kişilere karşı hüküm ifade eder hâle getirildiği zaman sırasına (çoğunlukla tescil sırasına) göre belirlenir. Bununla birlikte, bazı hukuk sistemlerinde, belirli varlık türleri üzerinde belirli bir yöntem kullanılarak tesis edilen teminat haklarına, üçüncü kişilere karşı hüküm ifade etme noktasında öncelik tanınabilmektedir. Örneğin, kıymetli evrak üzerindeki bir teminat hakkı, üçüncü kişilere karşı zilyetlik yoluyla hüküm ifade eder hâle getirilmişse, genellikle başka yöntemlerle üçüncü kişilere karşı etkin kılınmış diğer teminat haklarına göre üstün tutulur. Benzer şekilde, bir Devletin hukuku; banka hesapları, aracı nezdinde tutulan veya tutulmayan menkul kıymetler, para, kıymetli evrak ve diğer bazı varlık türleri bakımından ilgili varlığa özgü bazı öncelik kuralları öngörebilir.

16.2. İlke 16 ile dijital varlıklara tatbik edilen bu yaklaşım, birden fazla gerekçe üzerinden temellendirilebilir. İlk olarak, zamana bağlı olmayan öncelik tanınması, ilave bazı adımları atan teminatlı alacaklının, teminat altına alınmış varlığa daha yüksek ölçüde güvenerek ve bunu esas alarak hareket ettiğini kabul eder. Bu durum, bazı yerel hukuk rejimlerinde, kıymetli evrakın zilyetliğini elde eden teminatlı alacaklının hakkının, tescil yoluyla üçüncü kişilere karşı hüküm ifade eder hâle getirilmiş diğer teminat haklarına üstün tutulmasıyla benzerlik göstermektedir. İkinci olarak, teminat hakkını kontrol yoluyla üçüncü kişilere karşı hüküm ifade eder hâle getiren teminatlı alacaklının, herhangi bir sicil araştırması yapmasına gerek bulunmaz. Bu da, kıymetli evrak gibi diğer varlıklar bakımından geçerli olan yaklaşımla paraleldir; zira zilyetliği devralan tarafın bir de sicil araştırması yapması beklenmez. İlgili durum, işlem maliyetlerini azaltmakta ve varlığın devredilebilirliğini artırmaktadır. Ayrıca, dijital varlıklar bakımından sicil araştırması yapmak çoğu zaman pratik değildir. Teminat alacaklısı, teminat verenin kimliğini, yerini ya da hangi sicilin araştırılması gerektiğini dahi bilemeyebilir. Üçüncü olarak, bu öncelik yaklaşımı, alacaklıların müşterilerine bir dijital varlığın edinilmesini sağlamak amacıyla kredi açtıkları ve bu varlık üzerinde önceki tarihli bir tescile rağmen öncelik bekledikleri kredi uygulamalarıyla (teminat karşılığı kredi verme) da uyumludur. Dördüncü olarak, bu yaklaşım, temerrüt hâlindeki duruma da paraleldir; zira kontrol sahibi olan teminatlı alacaklı, teminat hakkını icra etme bakımından en elverişli konumdadır. Anılan durum, teminatlı alacaklıları bu avantajlı konuma geçmeye teşvik eder. Teminatlı alacaklıya öncelik elde etme imkânı tanınması, piyasa öngörülebilirliğini ve hukuki güvenliği artırır. Ayrıca, İlke 16’da benimsenen yaklaşım, teminatlı işlemler alanındaki uluslararası düzenlemelerle – UNCITRAL Teminatlı İşlemler Model Kanunu ve Cenevre Menkul Kıymetler Sözleşmesi’nin ilgili hükümleri dâhil olmak üzere- uyumludur; zira bu düzenlemeler de teminat üzerinde belirli bir kontrolü elde eden teminatlı alacaklılara öncelik tanımaktadır.

16.3. Birçok Devlette, diğer hukuk kuralları, bazı varlıklar bakımından tanınan devredilebilirlik (özellikle tedavül kabiliyeti), bunları devralanlara, tescil veya başka yöntemlerle üçüncü kişilere karşı hüküm ifade eder hâle getirilmiş teminat haklarını bertaraf etme imkânı tanımaktadır. Örneğin, paranın zilyetliğini, teminatlı bir alacaklının haklarını ihlal ettiğini bilmeden devralan bir başka kişi, parayı üzerindeki teminat hakkından ari olarak iktisap eder. Bu İlkelerde “devralan” kavramı, teminatlı alacaklıyı da

kapsayacak şekilde tanımlanmıştır (bkz. İlke 2(5)). İlkeler, dijital varlıklara yüksek düzeyde devredilebilirlik özelliğini tanıdığından, bunları devralanlar -teminatlı alacaklılar dâhil olmak üzere- İlke 8’de öngörülen yaklaşımdan yararlanabilecektir. Çoğu teminatlı alacaklının, masum kazanıma ilişkin, masum hareket etme, varlık üzerindeki hak çatışmasına ilişkin herhangi bir bilgiye sahip olmama ve Devletin İlke 8(1)(b) uyarınca öngörebileceği varlığı belirli bir değer karşılığı elde etme şartlarını karşılaması beklenir. Bu husus özellikle önemlidir; zira yukarıda açıklandığı üzere, teminat hakkını kontrol yoluyla üçüncü kişilere karşı hüküm ifade eder hâle getiren teminatlı alacaklının herhangi bir teminat sicilini ayrıca araştırması beklenmez. Her ne kadar İlke 8 uyarınca bir teminatlı alacaklının masum kazanımda bulunan olarak sayılabilmesi için çatışma gösterebilecek hakka ilişkin hiçbir bilgisinin bulunmaması gerekse de, İlke 16’nın etkisi, kontrol elde eden teminatlı alacaklının böyle bir bilginin bulunmamasından bağımsız şekilde, tescil yoluna giden teminatlı alacaklıya üstün tutulmasıdır. Aynı sonuca, UNCITRAL Teminatlı İşlemler Model Kanunu dâhil olmak üzere birçok teminatlı işlemler mevzuatında da ulaşılmaktadır. Nitekim anılan Model Kanun’un 45. maddesi, rakip bir teminat hakkının bilinmesinin önceliği etkilemeyeceğini öngörmektedir.

Birden Fazla Teminatlı Alacaklının Kontrol Sahibi Olması

16.4. Birden fazla teminatlı alacaklı, dijital varlıklar üzerinde kontrol elde edebilir ya da ilgili yetkileri paylaşabilir; bu durum, teminat hakkının üçüncü kişilere karşı hüküm ifade etmesini de kapsar. Böyle bir durum, dijital varlığın, bir saklayan tarafından birden fazla teminatlı alacaklı adına muhafaza edilmesinin kabul edildiği hâllerde ortaya çıkabilir. Kural olarak, bu durumda teminatlı alacaklıların kendi aralarındaki öncelik ilişkisini, aralarında belirli bir sırayı tayin etmek veya alacaklılar arası sözleşme yapmak suretiyle düzenlemeleri beklenir. Böyle bir sözleşmenin bulunmaması hâlinde, öncelik uyuşmazlığı, uygulanacak hukukun teminatlı işlemlere ilişkin düzenlemeleri dahilinde yer alan genel öncelik kuralına göre çözümlenir; bu kural genellikle zamanda önce olanın hak bakımından da önce geleceği ilkesini yansıtır. Buna göre, saklayanın bu konudaki teyidini ilk alan teminatlı alacaklı önceliğe sahip olur.

Uygulanacak Hukuk

16.5. İlke 5(1), kontrol yoluyla üçüncü kişilere karşı hüküm ifade eder hâle getirilmiş bir teminat hakkı ile, tescil gibi kontrol dışı yöntemlerle üçüncü kişilere karşı hüküm ifade eder hâle getirilmiş çatışan bir teminat hakkı arasındaki uyumsuzlıklara uygulanacak hukuku belirler. İlke 5(5)(b) uyarınca ise, kontrol dışındaki yöntemlerle üçüncü kişilere karşı hüküm ifade eder hâle getirilmiş teminat hakları arasındaki uyumsuzlıklara uygulanacak hukuk, diğer hukuk tarafından belirlenir. Örneğin, UNCITRAL Teminatlı İşlemler Model Kanunu'na göre, bir gayrimaddi varlık üzerindeki teminat hakkının önceliğine uygulanacak hukuk, teminat verenin bulunduğu yer hukukudur. Bu tür bir öncelik çatışması, bu İlke kapsamında düzenlenmemiş olup, genel teminatlı işlemler hukukunun konusunu oluşturur.

16.6. Örnek Durum. Borçlunun tüm varlıkları üzerindeki bir teminat hakkı, tescil yoluyla üçüncü kişilere karşı hüküm ifade eder hâle getirilmiştir. Borçlu, teminat altına alınmış stoklarını elden çıkararak karşılığında dijital varlıklar edinmiş; bu dijital varlıklar borçlu tarafından toplanarak, bunlar üzerinde kontrol sahibi kılınan bir saklayana aktarılmıştır. Saklayan da, kontrolü altındaki dijital varlıklar karşılığında borçluya kredi sağlamaktadır. Uygulanacak hukukun teminatlı işlemlere ilişkin düzenlemeleri, kontrolü üçüncü kişilere karşı hüküm ifade etmenin bir yöntemi olarak tanıyor (bkz. İlke 15) ve kontrol yoluyla üçüncü kişilere karşı hüküm ifade eder hâle getirilmiş teminat haklarına da öncelik veriyorsa (bkz. İlke 16); saklayanın teminat hakkı, dijital varlıklar üzerinde stokların bedeli olarak elde edilen teminat hakkına öncelikli olacaktır.

İlke 17

Teminat Haklarının Cebri İcrası

(1) Bir dijital varlık üzerinde kurulan teminat hakkının cebri icrası, iyi niyetle veya ticari açıdan makul bir şekilde hareket edilmesine ilişkin gereklilikler de dahil olmak üzere diğer hukuka tabidir.

(2) Bir saklayan tarafından muhafaza edilen dijital varlık üzerindeki teminat hakkı, kontrol dışında bir yöntemle üçüncü kişilere karşı ileri sürülebilir hale getirilmişse, saklayanın aksi yönde bir iradesi bulunmadıkça, teminatlı alacaklı, bu teminat hakkını yalnızca bir mahkeme veya diğer bir kamu otoritesi aracılığıyla cebri icra etme hakkına sahiptir.

Açıklama

Genel

17.1. İlke 17, teminat haklarının icrasını kolaylaştırabilecek teknolojilerden (örneğin teminatın yerinin tespiti veya uzaktan devre dışı bırakılması) ziyade, teminat haklarının icrasını düzenleyen hukuki kurallara ilişkindir. Etkin icraya ilişkin bu ve benzeri hususlar, UNIDROIT'nın "Etkili İcra İçin En İyi Uygulamalar" (*Best Practices for Effective Enforcement*) başlıklı ayrı bir projesinde ele alınmaktadır.

17.2. İlke 17, dijital varlıklar üzerindeki teminat hakları bakımından belirli icra yöntemleri öngörmemektedir. Genel olarak, diğer hukukta yer alan ve herkes için geçerli olan icra yöntemleri -yargısal icra da dahil olmak üzere- dijital varlıklar özelinde de aynen uygulanır. Bu Açıklamalar, UNCITRAL Teminatlı İşlemler Model Kanunu'nun (*UNCITRAL Model Law on Secured Transactions*) VII. Bölümünde yer alanlar gibi mevcut icra kurallarının, dijital varlıklar üzerindeki teminat hakları bakımından nasıl uygulanması gerektiği konusunda devletlere yol göstermektedir. Bir devletin hukuku, teminatlı alacaklıların, diğer hukuklardan kaynaklanan veya teminat sözleşmesinde öngörülen başvuru yollarını kullanmasını engellememelidir. Dijital varlıklar menkul kıymet işlemleri, türev işlemler ve benzeri finansal yapılarda yaygınlaştıkça, devletler tarafından bu tür işlemlerin tarafları için tasfiye netleştirmesi (*close-out netting*) imkânının sağlandığından emin olunmalıdır. İlke 14'e ilişkin Açıklamalarda da belirtildiği üzere, bu İlkeler, teminatlı

işlemlerin uygulanacak hukuk bakımından nitelendirilmesine ilişkin bir değişiklik önermemektedir. Bu nedenle, icraya ilişkin bazı durumlarda, dijital varlığı kesin olarak kazanan teminatlı alacaklılar bakımından, uygulanacak diğer hukuk hiçbir şart öngörmeyebilir ya da daha düşük düzeyde şartları benimsemiş olabilir.

17.3. Teminat hakkının icrası kapsamında; teminatın paraya çevrilmesi, tahsilat (dijital varlığın fiilen bağlı olduğu varlığın bir para alacağı olması hâlinde) ve teminatlı borcun tamamının veya bir kısmının ifası karşılığında teminatın kabulü gibi tüm icra yolları, dijital varlıklar üzerindeki teminat hakları bakımından da kullanılabilir olmalıdır. Teminatlı alacaklılar, haklarını kullanırken; ticari bakımdan makul davranma, bildirimde bulunma, elde edilen bedelleri öncelik kurallarına göre dağıtma gibi, genel teminatlı işlemler hukukunda yer alan icra kurallarına uymak zorundadır. Bazı durumlarda, dijital varlığın doğası veya teknik yapısı, belirli icra yetkilerinin kullanılmasına fiilen engel olabilir. Bununla birlikte, teminatlı işlemlere ilişkin uluslararası standartlarda yer alan genel icra kuralları, dijital varlık ödünç verenlerin ve ilgili diğer tarafların beklentilerini karşılayacak ölçüde esnek görünmektedir. Yine de devletlerin, Açıklama 17.4 – 17.7’de belirtilen birtakım hususları dikkate almaları gerekir.

17.4. Teminat hakkının üçüncü kişilere karşı ileri sürülebilir hâle getirilmesinde kullanılan yöntem, hakkın icra kabiliyetini doğrudan etkileyebilir. Kontrol, temerrüt hâlinde icrayı kolaylaştıran bir unsurdur; bu nedenle teminat hakkı kontrol yoluyla üçüncü kişilere karşı ileri sürülebilir kılınmışsa, teminatlı alacaklı tarafından gerçekleştirilecek icra süreci genellikle daha sorunsuz biçimde gerçekleştirilecektir. Buna karşılık, dijital varlık üzerindeki teminat hakkı kontrol yerine tescil yoluyla üçüncü kişilere karşı ileri sürülebilir kılınmışsa, teminat veren varlık üzerindeki kontrolü elinde tuttuğundan, uygulamada alacaklının bu varlık üzerinde icra yoluna gitmesi zorlaşabilir. Bu durumda, teminatlı alacaklı, temerrütten sonra, teminat veren kontrolü kendisine devretmeyi reddederse, kontrolü elde etmek için bir mahkeme kararına ihtiyaç duyabilir. Bu durum, maddi bir malvarlığı değerinin zilyetliğini devretmeyi reddeden teminat verenin durumuyla benzerlik gösterir. Ayrıca, duruma göre kontrol başka bir teminatlı alacaklıya geçmiş ve bu alacaklı öncelikli konumda bulunuyor olabilir (bkz. İlke 16). Böyle bir durumda, genel teminatlı işlemler hukuku, üst sıradaki teminatlı alacaklının icra sürecini devralabilip alamayacağını ve eğer alabiliyorsa da bunun nasıl yapılacağını belirler.

17.5. Teminatlı işlemler hukuku, genellikle, teminat hakkının icrasında bildirimde bulunma gibi yükümlülükler öngörerek ilgili tarafların menfaatleri arasında bir denge kurar. Bununla birlikte, bazı durumlarda bu yükümlülüklerin uygulanmayacağı istisnalar da tanınabilir. Örneğin, UNCITRAL Teminatlı İşlemler Model Kanunu’nun 78(8). Maddesi, varlığın hızla değer kaybedebileceği veya tanınmış bir piyasada satıldığı hâllerde bildirim yükümlülüğüne çeşitli istisnalar tanımaktadır. Bu tür istisnalar, her olasılığı kapsamasa da birçok dijital varlık bakımından uygulanabilir niteliktedir (örnek olarak bitcoin hızlı şekilde değer kaybedebilirken, sabit (stabil) kripto varlıklar için bu her zaman geçerli olmayabilir; bazı NFT’ler tanınmış piyasalarda işlem görürken, bazıları görmeyebilir). Bu istisnalar gelecekte söz konusu olabilecek gelişmeleri kapsayacak genişlikte kaleme alınmışsa, teminatlı işlemler hukukundaki icra hükümlerinin dijital varlıklar için ayrıca değiştirilmesine gerek olmayabilir. Bazı devletler, belirli varlık türleri için, bildirim yükümlülüğü içermeyen özel icra usulleri de öngörmektedir. Örneğin, Cenevre Menkul Kıymetler Sözleşmesi’nin (*Geneva Securities Convention*) 33. maddesi, aracı nezdinde tutulan menkul kıymetler bakımından bildirim yapılmaksızın satış veya hakkın doğrudan doğruya eldesi yoluyla icraya izin vermektedir. Benzer icra usullerinin, özellikle bu tür varlıklara benzeyen dijital varlıklar üzerindeki teminat hakları bakımından da kabul edilmesi, İlke 17 ile uyumlu olacaktır.

17.6. Genel olarak uygulanabilir icra hükümlerine getirilen istisnaların tanınması, otomatik icra mekanizmalarının işlerliğini kolaylaştırmaktadır. Otomatik icraya örnek olarak, teminat-kredi oranının belirli bir eşik değer altına düşmesi hâlinde dijital varlığın kendiliğinden tasfiye edilmesi gösterilebilir. Bu oranın düşüşünün teminat sözleşmesi uyarınca bir temerrüt hâli teşkil etmesi durumunda, söz konusu işlem bir teminat hakkının icrası niteliği taşır. Birçok sistem tasarımcısı, teminatlı işlemler hukukundaki icra kurallarının bu tür durumlara nasıl uygulanacağını yeterince bilmemektedir. Sistemler, genel icra hükümlerine tanınan istisnalar kapsamında tasarlanmış olsalar dahi, teminatlı alacaklının ticari bakımdan makul davranma yükümlülüğüne veya dürüstlük kuralı gibi başka bir uygulanabilir standarda uygun hareket edilmesi yine gerekli bulunur.

17.7. Dijital varlıklar söz konusu olduğunda, mahkemelerin icra yükümlülüklerine tanınan istisnaların yorumlanması bakımından rehberliğe ihtiyaç duyması olasıdır. Örneğin, Açıklama 17.5’te belirtilen istisnalardan biri olan “tanınmış piyasa”, satılan varlıkların misli nitelikte olduğu ve fiyatların bireysel pazarlığa tâbi olmadığı; borsa veya emtia

piyasaları gibi piyasalardır. Tanınmış piyasa istisnasının amacı, bu özel işlemin sağladığı etkinlik ve maliyet avantajlarını kolaylaştırırken, ilgili tarafların menfaatlerini zedelememektir. Tanınmış bir piyasanın mutlaka düzenleme veya gözetim altında olması şart değildir; ancak düzenleyici mahiyette gerekliliklerin veya rehberlerin varlığı, bu istisnanın uygulanmasında yararlı ölçütler sunabilir. Bir piyasanın bu istisna kapsamında değerlendirilip değerlendirilemeyeceği işlevsel bir testle belirlenir; yoksa piyasanın “türü”ne dayanmaz. Dijital varlık borsalarının tanınmış piyasa sayılıp sayılmayacağı, bu çerçevede belirlenen ölçütlere göre değerlendirilecektir.

İlke 17(2)

17.8. Dijital varlığın teminat veren adına bir saklayan tarafından muhafaza edilmesi hâlinde, yargı dışı icra, saklayanın teminatlı alacaklının talimatları doğrultusunda harekete geçmesini gerektirir. Ancak teminatlı alacaklı bilinmiyorsa, aracı konumundaki saklayan bu talimatları yerine getirmek noktasında istekli olmayacaktır; nitekim birçok teminatlı işlemler mevzuatı, bu durumda aracıları koruyan hükümler içermektedir. Örneğin, UNCITRAL Teminatlı İşlemler Model Kanunu’nun 82(4). maddesi, bir banka hesabı üzerindeki teminat hakkı bakımından, yargı dışı icranın ancak bankanın teminatlı alacaklının talimatları doğrultusunda hareket etmeyi kabul etmesi hâlinde mümkün olduğunu öngörmektedir. İlke 17(2), dijital varlık saklayanların teminat hakkının icrası sürecinde korunmalarını düzenlemektedir. Teminat hakkı, İlke 15 uyarınca kontrol yoluyla üçüncü kişilere karşı ileri sürülebilir hâle getirilmişse, saklayan dijital varlığı teminatlı alacaklı adına muhafaza eder ve kural olarak teminatlı alacaklıya karşı bazı yükümlülükler altına girer; bunlar arasında, teminatlı alacaklının talimatı üzerine dijital varlık üzerindeki kontrolün değiştirilmesi de yer alır (bkz. İlke 11(1)(b)). Buna karşılık, teminat hakkı tescil gibi kontrol dışındaki bir yöntemle üçüncü kişilere karşı ileri sürülebilir hâle getirilmişse, saklayanın teminatlı alacaklıya karşı herhangi bir yükümlülüğü bulunmaz. Bu hâllerde, saklayan teminatlı alacaklının talimatlarına uymayı kabul etmezse, teminatlı alacaklının bir mahkemeden veya diğer bir yetkili kamu otoritesinden karar alması gerekecektir.

17.9. Örnek Durum. Bir teminat hakkı, teminatlı alacaklı üç taraflı bir çoklu imza yapısının taraflarından biri olmak üzere, kontrol yoluyla üçüncü kişilere karşı hüküm ileri sürülebilir hâle getirilmiştir. Teminat veren de bu yapının tarafı olmakla birlikte, üçüncü kişi teminatlı alacaklı adına hareket etmektedir. Kontrol değişikliğinin gerçekleşmesi için ise, iki tarafın

birlikte hareket etmesi gerekmektedir. Temerrüt hâlinde, çoklu imza düzenlemesi devreye girer ve teminat altına alınmış dijital varlık, teminatlı alacaklının münhasır kontrolüne geçer. Bu durum, teminatın teminatlı borcun ifası karşılığında kabul edilmesine veya cebri satış yoluyla paraya çevrilmesine imkân tanır. Bununla birlikte, teminatın borcun ifası karşılığında kabul edilmesine ilişkin olarak uygulanabilir diğer hukukta öngörülen tüm şartlar geçerliliğini korur.

BÖLÜM VI: USUL HUKUKU VE CEBRİ İCRA

İlke 18

Usul Hukuku ve Cebri İcra

Bu İlkelerde aksi öngörülmedikçe, dijital varlıklar özelindeki usul hukukuna ilişkin hususlar, cebri icra süreci de dâhil olmak üzere, diğer hukuka tabidir.

Açıklama

Genel

18.1. İlke 18, bir devletin genel mahiyetli usul hukukunun; (i) dijital varlıkları konu alan ve icraya ilişkin olmayan her türlü yargısal süreci, (ii) dijital varlıkları içeren mahkeme kararlarının icrasına yönelik usullere ve (iii) dijital varlıklar bakımından yetkiye dayalı icra süreçlerine uygulanacağını açıkça ortaya koymaktadır. Birinci kategori, icra mahiyeti göstermeyen yargısal süreçleri kapsar; bunlara hakkın önceliğine ilişkin uyuşmazlıklar ile bir kişinin bir dijital varlık üzerinde kontrole sahip olduğunu ispatlamasının gerektiği yargısal süreçler de dâhildir (bkz. İlke 7). Kategori (ii)'nin içeriği, özel bir açıklamaya lüzum olmaksızın kendiliğinden anlaşılabilir. Kategori (iii) ise, bu paragrafın devamında açıklanmaktadır. Cebri icra, alacaklının borçluya karşı olan alacağını borçluya ait bir varlığa el koyulması ve bu varlığın değeri üzerinden alacağın karşılanması ya da bir kamu otoritesi aracılığıyla söz konusu varlık üzerinde hak veya kontrolün elde edilmesi suretiyle ona tatmin sağlayan süreçtir. Hukuk sistemine ve somut duruma bağlı olarak bu süreç; bir mahkeme kararı veya emri, icra kabiliyeti olan bir tahkim kararı, sözleşme hukuku dışında bir hukuk kuralı uyarınca hüküm doğuran mahkeme dışı bir sulh anlaşması veya noter ya da başka bir kamu otoritesi tarafından düzenlenen resmî bir belge gibi hukuken icra edilebilir bir araçla başlatılabilir. Bu süreç, bir kamu otoritesi tarafından veya bir kamu otoritesinin gözetimi altında hareket eden özel bir kişi tarafından yürütülür.

18.2. Bununla birlikte, belirli bir devletin usul hukuku kurallarına bağlı olarak, dijital varlıkların kendine özgü özellikleri dikkate alınarak, bu kurallarda veya kuralların uygulama biçiminde bazı uyarlamaların yapılması yerinde olabilir. Açıklama 18.3 – 18.7

altında, bu tür uyarlamaları gerekli kılacak özelliklere veya özellik kombinasyonlarına ilişkin bazı örnekler sunulmaktadır.

18.3. Dijital varlıklara ilişkin bir mahkeme kararının icrası veya bir kamu otoritesi aracılığıyla icra süreci söz konusu olduğunda, çoğu zaman bir kamu otoritesinin ya da onun yetkilendirdiği bir kişinin bir veya birden fazla dijital varlık üzerinde kontrol elde etmesi gerekecektir. Ancak bu durum, diğer varlık türleri üzerindeki kontrolün (ya da zilyetliğin) ele geçirilmesine kıyasla her zaman kolay değildir. Örneğin, dijital varlık üzerinde kontrol sahibi olan kişi tespit edilmiş olsa bile, bu kişi cüzdana erişim sağlayan parolayı ve/veya özel anahtarı açıklamayı reddedebilir. Bu nedenle, mahkemenin (veya yetkili başka bir otoritenin), ilgili kişiye kontrol değişikliğini gerçekleştirmesini veya dijital varlığa erişimi başka bir şekilde mümkün kılmasını emretmesi gerekli bulunabilir. Usul hukukunun ve uygulamasının bu tür durumları kolaylaştıracak şekilde düzenlenmesi yerinde olacaktır.

18.4. Dijital varlık üzerinde kontrol sahibi olduğu belirlenen kişi bir saklayan ise, kamu otoritesi veya onun yetkilendirdiği kişi, saklayana kontrolün değiştirilmesi ya da varlığa erişimin sağlanması yönünde talimat vermek isteyecektir. Saklayanın bu talimata rıza göstermemesi hâlinde, yine bir mahkeme veya yetkili otorite tarafından saklayana dijital varlık üzerindeki kontrol değişikliğini gerçekleştirmesi ya da dijital varlığa gerekli erişimin sağlanması yönünde emir verilmesi gerekecektir. Bu tür durumlarda da usul hukukunun ve uygulamasının süreci kolaylaştırması uygun olacaktır.

18.5. Dijital varlıkların ayırt edici özelliklerinden kaynaklanabilecek bir diğer güçlük, dijital varlık üzerinde kontrol sahibi olan kişinin her zaman kolayca tespit edilememesidir. Bu durumda, kamu otoritesi veya onun yetkilendirdiği kişi, saklayan gibi üçüncü kişilerden bilgi temin etmek isteyebilir. Örnek olarak, bu bilgiler İlke 6(1)(b)'de belirtilen nitelikte bilgiler olabilir. Bazı hâllerde ise, yargılamaya veya icraya ilişkin süreçlerin başlatılabilmesi ya da etkili biçimde yürütülebilmesi için üçüncü kişilerden elde edilebilecek daha genel nitelikte bilgilere ihtiyaç duyulabilir. Tüm bu durumlarda, gerekli bilgilerin elde edilmesini kolaylaştıracak bir usul hukuku yaklaşımı benimsenmesi yerinde olacaktır; ancak bu kolaylaştırma ile gizlilik ve mahremiyet gerekleri arasında uygun bir denge kurulması lazım gelir.

18.6. Dijital varlıkların bir özelliği de kolay ve hızlı biçimde devredilebilmeleridir. Bazı durumlarda, bu varlıkların yerine geçen değerlere yönelik talepler mümkün olmaya devam etse bile (uygulanacak diğer hukuka bağlı olarak), ilgili varlık ile temsil edilen asıl ekonomik değer fiilen kaybolabilir. Bu nedenle, mahkeme veya diğer yargılamalarda ya da icra sürecinde varlıkların korunması büyük önem taşıyabilir. Usul hukukunun, ihtiyati tedbir, varlıkların bloke edilmesi kararı veya dijital varlıklar üzerindeki kontrolün mahkemeye ya da başka bir kamu otoritesine devredilmesi gibi geçici koruma tedbirlerini öngörerek bu hususta bir kolaylaştırma sağlaması uygun olacaktır.

18.7. Dijital varlıkların ve bunların kaydedildiği sistemlerin bir başka özelliği, fiziksel bir konumlarının bulunmamasıdır. Yine ilgili varlıklar üzerinde kontrol sahibi olan kişilerin zaman içinde farklı hukuk sistemlerine tabi yerlerde bulunabileceklerdir. Bu nedenle, yargılamalar veya icra süreçleri çoğu kez sınır aşan nitelik taşıyacak ve birden fazla devletteki mahkemeleri veya kamu otoritelerini ilgilendirecektir. Usul hukukunun bu durumu dikkate alacak şekilde düzenlenmesi yerinde olacaktır.

18.8. Dijital varlıklar bakımından yetkiye dayalı icra süreçleri konusundaki ayrıntılı çalışmalar, UNIDROIT'nın "Etkili İcra İçin En İyi Uygulamalar" (*Best Practices for Effective Enforcement*) başlıklı projesi kapsamında yürütülmektedir. Bu alanda özel bir yönlendirme için, söz konusu projenin gelecekteki çalışmalarına atıf yapılmaktadır.

BÖLÜM VII: İFLAS

İlke 19

İflasın Dijital Varlıklar Üzerindeki Malvarlıksal Mutlak Haklara Etkisi

(1) Bir dijital varlık üzerindeki İlkeler hukuku veya diğer hukuk uyarınca üçüncü kişilere karşı etkili hâle getirilmiş olan bir malvarlıksal mutlak hak, iflasla ilgili bir süreçte iflas idaresine, alacaklılara ve diğer üçüncü kişilere karşı da etkilidir.

(2) Fıkra (1), iflasla ilgili bir süreç nedeniyle uygulanabilir mahiyetteki herhangi bir maddi hukuk veya usul hukuku kuralının uygulanmasını etkilemez; bunlara örnek olarak aşağıdakileri gösterilebilir:

(a) alacak kategorilerinin sıralamasıyla ilgili kurallar;

(b) bir işlemin imtiyazlı özellik göstermesi veya bir devrin alacaklıları aldatma amacı taşıması nedeniyle iptaline ilişkin kurallar; veya

(c) iflas idaresinin kontrolü veya denetimi altındaki bir malvarlığı değeri (varlık) üzerindeki hakların cebri icrasına ilişkin kurallar.

Açıklama

Genel Bakış

19.1. İlke 19, iflasın dijital bir varlık üzerindeki malvarlıksal mutlak hakka etkisini düzenlemektedir. İlke 3(1), “dijital varlıkların malvarlıksal mutlak haklara konu olabileceğini” öngörmektedir. Bu da, dijital bir varlık üzerinde malvarlıksal mutlak bir hakkın sahibi olan kişinin, söz konusu hak üçüncü kişilere karşı da hüküm ifade edecek hâle getirilmişse, bu hakkı üçüncü kişilere karşı ileri sürebileceği anlamına gelir. İlke 19, dijital bir varlık üzerindeki ve üçüncü kişilere karşı hüküm ifade eden bir malvarlıksal mutlak hakkın, iflasla ilgili bir süreçte de ilgili taraflara karşı geçerliliğini koruduğunu teyit etmektedir. Aşağıda açıklandığı üzere, iflasla ilgili sürece tabi bulunan kişi (“borçlu”), malvarlıksal mutlak bir hakkın sahibi olan kişi olabileceği gibi, başka bir kişi de olabilir.

19.2. İlke 8’de düzenlenen masum kazanım kuralı ile İlke 15’te öngörülen ve bir teminat hakkının kontrol yoluyla üçüncü kişilere karşı ileri sürülebilir hâle getirilebilmesi

durumları dışında, İlke 3(3) uyarınca bir kişinin dijital bir varlık üzerinde malvarlıksal mutlak bir hakka sahip olup olmadığı ve bu malvarlıksal mutlak hakkın üçüncü kişilere karşı ileri sürülebilir hâle getirilip getirilmediği hususları, “diğer hukuk” tarafından belirlenir (yani İlke 2(4) anlamında, İlkeler hukukunun dışında kalan devlet hukukuna). İlke 19(1), iflas öncesinde mevcut olan bu üçüncü kişilere karşı hüküm ifade edebilirliğin, iflasla ilgili bir süreç dahilinde de devam edeceğini öngörmektedir. Bu etkinin somut sonucu, olayın özelliklerine ve uygulanacak diğer hukuka bağlı olacaktır. Bununla birlikte genel olarak, UNCITRAL İflas Hukuku Yasama Rehberi’nin (*UNCITRAL Legislative Guide on Insolvency Law*) (2004) ikinci bölümünde önerildiği üzere (bkz. Tavsiye 35), borçlunun iflas süreci kapsamındaki malvarlığı değerleri, ilgili hakların kapsamı ve verdikleri yetkiler çerçevesinde, borçlunun malvarlıksal mutlak hak sahibi olduğu varlıklardan oluşur.

Tipik Durumlar

19.3. İlke 19’un uygulanmasının sonuçları, üç tipik durum dikkate alınmak suretiyle örneklendirilebilir: (1) Bir dijital varlık üzerinde “hak sahibi” olan veya teminatlı alacaklı sıfatıyla dijital bir varlık üzerinde teminat hakkı edinmiş bir kişinin iflası; (2) Borçlu sıfatıyla bir dijital varlık üzerinde alacaklı lehine teminat hakkı tesis etmiş olan bir kişinin iflası; (3) Bir müşterisi adına dijital varlık üzerinde kontrol sahibi olan bir saklayanın iflası. Üçüncü durumda, müşteri dijital varlığını geri almak isteyecektir. İlke 19 esas itibarıyla (1) ve (2) numaralı durumlara ilişkindir; bunlar, alacaklılara dağıtım yapılan bir iflas süreci bağlamında İlke 19’un işleyişini örneklendirmek üzere Açıklama 19.4 – 19.8’de ele alınmaktadır. (3) numaralı durum (saklayanın iflası) özel olarak İlke 13 ve bu İlkeye ilişkin Açıklamalarda ele alınmaktadır. Alt saklayanın iflası ise, İlke 13(8) kapsamında değerlendirilmektedir.

Durum (1)

19.4. Durum (1), çeşitli şekillerde ortaya çıkabilir. Bu durumun ilk alt görünümü, bir kişi bir dijital varlık üzerindeki mutlak hak sahibini olup ilgili varlık üzerinde kontrol sahibidir; örneğin varlık cüzdan yazılımı kullanarak kendi kendine saklama yoluyla elde tutulduğunda durum böyledir (bkz. Açıklama 10.15 – 10.17). Bu kişi iflas ettiğinde, dijital varlık onun iflas süreci kapsamındaki malvarlığı değerlerine dâhil olur; zira kişinin

malvarlıksal mutlak hakkı iflas hâlinde de geçerliliğini korur (İlke 19(1)). Tipik iflas hukukunda, iflas idaresi, borçlunun malvarlıksal mutlak haklarını alacaklıların yararı için kullanabilir; bu bağlamda, borçlunun dijital varlıkları üzerinde kontrol sağlayabilir, bunları satabilir ve elde edilen bedeli alacaklılara dağıtabilir. Burada “kontrol” kavramı, İlke 6’daki teknik anlamıyla değil, geniş anlamıyla kullanılmaktadır. Ancak dijital varlık üzerinde kontrol sağlanması, diğer varlık türlerine kıyasla daha güç olabilir. Cüzdana erişim ve/veya özel anahtar genellikle belirli bir parola ile korunur ve borçlu bu parolayı açıklamayı reddedebilir. İflas idaresinin, borçlunun parolayı açıklamasını emreden bir mahkeme kararı alıp alamayacağı ve bunun nasıl sağlanacağı, uygulanabilir iflas hukukuna bağlıdır.

19.5. Durum (1)’in ikinci alt görünümünde, iflas eden kişi dijital varlık üzerinde malvarlıksal mutlak hak sahibidir; ancak varlık onun adına bir saklayan tarafından muhafaza edilmektedir. Bu durumda da malvarlıksal mutlak hak, iflas sürecine rağmen geçerliliğini korur ve yukarıda da açıklandığı üzere iflas idaresi dijital varlığı geri alarak satmak isteyecektir. Bu durumda süreç daha kolaydır; zira uygulanacak iflas hukuku izin veriyorsa, iflas idaresi saklayana talimat vererek varlığın kendi kontrolüne veya satış konusunda anlaşma sağlanan üçüncü bir kişiye devrini sağlayabilir.

19.6. Durum (1)’in üçüncü alt görünümü, iflas eden kişinin bir teminatlı alacaklı olarak dijital varlık üzerinde teminat hakkı edinmiş olmasıdır. Teminat hakkının üçüncü kişilere karşı ileri sürülebilirliğini sağlamak için bu kişi dijital varlık üzerinde kontrolü elde etmiş veya uygulanacak hukukta öngörülen diğer yöntemlere başvurmuş olabilir (bkz. ayrıca İlke 16 ve ilgili Açıklamalar). Bu durum, ilk görünümle benzerdir; her iki hâlde de iflas eden kişi, dijital varlık üzerinde malvarlıksal bir mutlak hakka sahiptir (birinde tam malvarlıksal mutlak hak sahibi, diğerinde teminatlı alacaklı sıfatıyla). Teminatlı alacaklının iflası hâlinde, dijital varlık üzerindeki teminat hakkı borçlunun iflas süreci kapsamındaki malvarlığı değerlerine dâhil olur; zira malvarlıksal mutlak hak iflas hâlinde de geçerliliğini sürdürür. Bkz. Açıklama 19.4.

19.7. Durum (1)’in dördüncü alt görünümünde ise, iflas eden kişi teminatlı alacaklı olarak dijital varlık üzerinde bir teminat hakkı edinmiştir; ancak varlık onun adına bir saklayan tarafından muhafaza edilmektedir. Bu durum, ikinci görünüme benzer niteliktedir. İflas

eden alacaklının teminat hakkı, iflas sürecine rağmen geçerliliğini korur. Ayrıca bkz. Açıklama 19.5.

Durum (2)

19.8. Durum (2) de çeşitli alt görünümde içermektedir. İlk alt görünümde, bir kişi dijital varlık üzerinde malvarlıksal mutlak hak sahibi olup bu varlık üzerinde kendi kendine saklama yoluyla kontrol sahibidir (bkz. Açıklama 10.15–10.17) ve bu dijital varlık üzerinde alacaklı lehine bir teminat hakkı tesis etmiştir. Bu kişinin iflası hâlinde, alacaklı iflas süreci sırasında dijital varlık üzerindeki teminat hakkını icra etmek isteyebilir. İlke 19(1) uyarınca, alacaklının teminat hakkı iflastan etkilenmez. Bu durum, uygulanacak iflas hukukuna ve somut olaya bağlı olarak, teminat hakkının alacaklı tarafından doğrudan icra edilmesini veya iflas idaresinin varlığı paraya çevirerek alacaklının bu bedel üzerinden tatmin sağlamasını mümkün kılar. Her hâlükârda, teminat hakkı, diğer varlıklar üzerindeki teminat haklarıyla aynı etkiye sahiptir (bu etkinin kapsamı uygulanacak iflas hukukuna bağlıdır; bkz. örnek olarak Açıklama 19.12). Ancak yukarıda belirtilen kontrolün elde edilmesine ilişkin güçlükler bu durumda da ortaya çıkabilir. Dijital varlığın iflas eden kişi adına bir saklayan tarafından muhafaza edilmesi hâlinde de aynı değerlendirme geçerlidir; ancak saklayan teminatlı alacaklının talimatları doğrultusunda hareket etmeyi kabul etmedikçe, bir mahkeme veya yetkili makamdan karar alınması gerekecektir (bkz. İlke 17(2)). Buna karşılık, teminatlı alacaklı dijital varlık üzerinde kontrol elde etmişse, teminat hakkının yargı dışı yollarla icrası önemli ölçüde kolaylaşır (bkz. Açıklama 17.4); ancak bunun mümkün olup olmayacağı yine uygulanacak iflas hukukuna bağlıdır.

İlke 19(2)

19.9. İlke 19, dijital bir varlık üzerindeki malvarlıksal mutlak hakların iflas hâlinde etkilenmemesini amaçlamakla birlikte, bu koruma mutlak değildir (bkz. ayrıca İlkeler 5(6) ve 5(7)). Örneğin, bir devletin diğer hukukunun uygulanması, ilgili dijital varlık üzerinde başka bir kişinin haklarına öncelik tanınması sonucunu doğurabilir. İlke 19(1), iflasla ilgili sürecin bir sonucu olarak uygulanması gereken -ister maddi ister usulî nitelikte olsun- bu tür kuralların işleyişini etkilemez. Söz konusu kurallar, bir devletin hukukunun İlkeler hukukunun dışında kalan (İlke 2(4) anlamında “diğer hukuk” olarak) herhangi bir bölümünde yer alabilir; buna vergi hukuku, iflas hukuku, genel özel hukuk ve usul hukuku

da dâhildir. İlke 19(2), İlke 19(1) tarafından etkilenmeyen ve bir Devletin diğer hukukundaki ilgili kuralların alacaklıların haklarını etkileyebileceği üç duruma örnek vermektedir.

19.10. İlke 19(2)(a)'da yer alan ilk örnek, alacak türlerinin sıralanmasına (öncelik düzenine) ilişkindir. İflas süreci kapsamındaki alacakların veya yine bu sürece dâhil olan belirli varlıklar üzerindeki taleplerin hangi sıraya göre karşılanacağını düzenleyen uygulanacak devlet hukuku, kural olarak bazı alacaklı gruplarına diğer alacaklılara (teminatlı alacaklılar dâhil) göre öncelik tanır. Örneğin, bir devlet hukuku, iflas eden kişinin belirli varlıkları bakımından kamu alacaklarına teminatlı ve teminatsız alacaklılara nazaran öncelik tanıyabilir ya da iflas sürecinin masraflarının, diğer teminatlı ve teminatsız alacaklıların taleplerine göre öncelikli olduğunu öngörebilir.

19.11. İlke 19(2)(b)'de yer alan ikinci örnek, hileli tasarruflar ile ilgilidir. Uygulanabilir Devletin iflas veya özel hukuku uyarınca, dijital varlıklar üzerindeki malvarlıksal mutlak hakların devri, belirli bir süre içinde yapılmışsa ve borçlu bu devri (diğer) alacaklılarını zarara uğratmak amacıyla gerçekleştirmişse, borçlunun iflas idaresi tarafından iptal edilebilir. Bu nedenle, bir Devletin iflas veya özel hukuku, dijital varlığı iktisap etmiş bir kişinin bu varlık üzerindeki malvarlıksal mutlak hakkına müdahale edebilir. Benzer şekilde, uygulanacak iflas hukuku veya özel hukuk, belirli şartların gerçekleşmesi hâlinde, alacaklılardan birine ayrıcalık tanıyan nitelikteki dijital varlık devirlerinin de iflas idaresi tarafından geri alınmasına imkân verebilir.

19.12. İlke 19(2)(c)'de gösterilen üçüncü örnek, iflas idaresinin, Açıklama 19.4'te açıklandığı üzere dijital varlık üzerinde kontrol elde etmiş olması hâlinde, İlke 19(1)'in, söz konusu varlık üzerindeki hakların icrasına ilişkin uygulanacak hukuk kurallarının işleyişini -ister iflas idaresi ister başka bir kişi tarafından icra edilsin- etkilemeyeceğini açıklığa kavuşturmaktadır. Örneğin, teminatlı alacaklının icra yoluna başvurmasını askıya alan bir kural, İlke 19(1) tarafından bertaraf edilmez. İlke 19(2)(c), İlke 19(1) ile birlikte okunduğunda, dijital varlıkların tutulduğu (veya kayıt altına alındığı) sistemi işletenler de dâhil olmak üzere üçüncü kişilerin, iflas idaresinin iflas eden kişinin bu dijital varlıklar üzerindeki haklarını kullanmasını tanıması ve buna imkân sağlaması gerektiği sonucunu da doğurmaktadır. Saklama ilişkileri bakımından bkz. İlke 13.