Sayfa 1

Akıllı Sözleşme Değer Aktarım Protokolleri
Dağıtık Mobil Uygulama Platformu

Patrick Dai 1 , Neil Mahi 1 , Jordan Earls 1 , Alex Norta 2
1 Qtum Vakfı, Singapur
vakıf@qtum.org
2 Büyük Ölçekli Sistem Grubu, Tallinn Teknoloji Üniversitesi,
Akadeemia tee 15A, 12816 Tallinn, Estonya
alex.norta.phd@ieee.org

Öz. Kanıtı kullanan blockchain özellikli akıllı sözleşmeler
işlemler için pay doğrulama, önemli performans vaat ediyor
iş kanıtı çözümlerine kıyasla avantajlar. Geniş endüstri benimsemesi için
Diğer önemli gereksinimler ayrıca karşılanmalıdır. Sınav için-
geriye dönük uyumlu akıllı sözleşme sistemleri otomatikleştirmelidir
lite mobile ile kuruluşlar arası bilgi-lojistik düzenleme
basit ödeme doğrulama (SPV) tekniklerini destekleyen cüzdanlar.
şu anda lider akıllı sözleşme çözümü Ethereum, hesaplama kullanıyor
müttefik pahalı iş kanıtı doğrulamasının, birden çok
zaman alır ve tüm blok zincirinin indirilmesini gerektirir. Con-
sırayla, Ethereum akıllı sözleşmelerinin sınırlı faydası vardır ve resmi olmayan
bir güvenlik sorunu olan anlambilim. Bu tanıtım belgesi, web sitesindeki boşluğu dolduruyor.
Qtum akıllı sözleşme çerçevesini sunarak son teknoloji
sosyoteknik uygulama uygunluğunu, resmi
anlambilim dili ifade gücü ve akıllı sözleşmenin sağlanması
hızlı en iyi uygulama endüstri dağıtımı için şablon kitaplıkları. Biz dis-
Ethereum alternatifine kıyasla Qtum'un faydalarına küfür
ve sektör için Qtum akıllı sözleşmeli gelecek geliştirme planlarını sunun-
vakalar uygulamaları.

Anahtar kelimeler: akıllı sözleşme, iş ağı modeli, DAPP, mobil,
bilgi lojistiği, kuruluşlar arası, eşler arası, dağıtılmış sistem
tem, e-yönetişim, Qtum çerçevesi

1. Giriş

Kolaylaştıran, doğrulayan ve yasallaştıran orkestrasyon ve koreografi protokolleri
hesaplama, rıza gösteren taraflar arasında müzakere edilmiş bir anlaşma anlamına gelir,
akıllı sözleşmeler. İkincisi, başlangıçta aşağıdaki gibi çeşitli alanlarda uygulama bulur:
örneğin, finansal teknoloji [6], Nesnelerin İnterneti (IoT) uygulamaları [33], dijital-
imzalama çözümleri [11]. Akıllı sözleşmelerin önemli bir yönü merkezi olmayan
Başlangıçta sözde iş kanıtı (PoW) aracılığıyla işlemlerin doğrulanması
[42]. Akıllı sözleşmelere olanak tanıyan temel teknoloji, kamuya açık olarak dağıtılan bir
defter, işlem olaylarını gerekmeden kaydeden blok zinciri olarak adlandırdı.

Sayfa 2

güvenilir bir merkezi otoriteye sahip olmak. Blockchain teknolojisi,
eşler arası (P2P) bir kripto para birimi olan Bitcoin'in [23] başlangıcı ve ödeme
protokol katmanında sınırlı bir işlem kümesi içeren sistem. Bit-
madeni paralar, hesaplama açısından pahalı olan işlem doğrulaması için PoW kullanır ve
yoğun elektrik.

Bitcoin'lerin aksine, birçok akıllı sözleşme sistemi şu özelliklere sahiptir:
JavaScript sözdizimine ve hedeflerine benzeyen Turing-complete dil Solidity 1
yasalaştırma için, örneğin, Ethereum Virtual [44] makinesi. Ethereum, de-
facto, çeşitli eksikliklerden rahatsız olmasına rağmen, akıllı sözleşme sisteminin lideri.
İlk olarak, iş kanıtı işlem doğrulaması, ölçeklenebilirliği noktaya kadar azaltır

Ethereum'un çoğu endüstri uygulaması için uygun olmadığı düşünüldüğünde.
İkincisi, yakın tarihli bir kitle fonlaması olay incelemesinde, Ethereum'a bağlı Solidity
akıllı sözleşme 2 eksikliğinden kaynaklanan güvenlik açıkları nedeniyle saldırıya uğradı .
resmi doğrulamalar için araçlarla ilgili son teknoloji [3]. Güvenlik
kusur, ca. 50 milyon dolar. Sonuç olarak, Ethereum bir
hardfork, iki ayrı Ethereum sürümü veren bir şizmle sonuçlanıyor 3 . Hala
başka bir Ethereum hardfork 4'e hizmet reddi saldırısı neden oldu ve daha fazlası
proof-of-stake [2] işlem doğrulamasını gerçekleştirmek için hardforks 5 beklenmelidir
ve blockchain parçalama [20].
Daha fazla neden, Ethereum endüstrisinin yaygın şekilde benimsenmesini sınırlar [8]. Sınav için-
kuruluşlar arası bilgi lojistiğini otomatikleştirememe, eksik
harici ve ilgili dahili öncelikler arasındaki farklılıkları koruyan gizlilik
vate sözleşmeleri, daha iyi blok zincirleri için güvenli ve istikrarlı sanal makineler
Proof of stake [2] işlem doğrulama, resmi olarak doğrulanabilir akıllı
sözleşme dilleri, tümünün indirilmesini gerektirmeyen lite cüzdanlar
basit ödeme ile akıllı sözleşmeler için blok zinciri ve mobil cihaz çözümleri
ment doğrulama (SPV) [14]. İkincisi, istemcilerin yalnızca
keyfi bir tam düğüme bağlandıklarında başlıkları bloke eder [23].
Qtum, mevcut bir eksiklik için Ethereum Sanal Makinesi'ni (EVM) kullanırken
[19] 'a göre daha uygun alternatifler arasında, EVM'nin bu tür eksiklikleri vardır.
daha önceki saldırılarda olduğu gibi yanlış yönetilen istisnalara ve dezavantajlara karşı
işlem sıralaması, zaman damgaları vb. gibi beklemeler. Aynı zamanda
em- ile sektörde ölçeklenebilirliğe ulaşmak için akıllı sözleşme sistemi için arzu edilir
yan zincirler [10] ve harcanmamış işlem çıktıları (UTXO) [10],
Bitcoins [23] veya Renkli madeni paralar gibi diğer blok zinciri sistemleriyle uyumluluk
[36]. Ayrıca, Bitcoin Lightning Network'ün özelliklerinin benimsenmesi
[35], çift yönlü mikro ödeme kanalları aracılığıyla ölçeklenebilirlik sağlar.
1 http://solidity.readthedocs.io/en/develop/
2 https://www.wired.com/2016/06/50-million-hack-just-showed-dao-human/
3 https://bitcoinsmagazine.com/articles/ethereum-classic-hard-forks-diffuses-
zorluk-bomba-1484350622 /
4 https://cointelegraph.com/news/ethereum-hard-fork-no-4-has-arrived-as-dos-
saldırılar yoğunlaştırmak
5 https://forum.daohub.org/t/whats-up-with-casper-proof-of-stake-and-
sharding / 6309

---

3. Sayfa

Ethereum gibi akıllı sözleşme sistemleri dikkat çekerken,
Yukarıda tartışılan nedenlerden dolayı endüstri tarafından benimsenme mevcut değildir. Bu whitepa-
akıllı sözleşme için Qtum 6 çerçevesini belirleyerek boşluğu giderir
akıllı sözleşme çözümünün nasıl geliştirileceği sorusuna cevap veren sistemler
kuruluşlar arası olanak sağlamak için kritik müşteri gereksinimlerini karşılama
maliyetleri ve zamanı azaltmak için bilgi lojistiği? Bir ihtilaf ayrılığı oluşturmak için
cerns, aşağıdaki alt soruları soruyoruz. Farklılaşan teknolojik
Qtum akıllı sözleşme çözümlerinin sağladığı performans avantajları? Nedir
Qtum çerçevesinin karşıladığı kritik akıllı sözleşme gereksinimleri? Nedir
organizasyonel bilgi lojistiği otomasyonunun benzersiz özellikleri
Qtum framework desteklemeyi hedefliyor?
Bu whitepaper'ın geri kalanı aşağıdaki gibi yapılandırılmıştır. İlk Bölüm 2
Qtum çerçevesinin teknolojiye ulaşmak için somut avantajlarına odaklanır.
ilgili çözümlere kıyasla mantıksal olarak performans artar. 3. Bölüm
ilgili paydaşlarla birlikte işlevsel ve kaliteli hedefler verir.
sosyoteknik olarak organize edilmiş akıllı sözleşme sistemleri. Bölüm 4, koşunun nasıl

ning vakası, Qtum-çerçeve değer aktarım protokolü tarafından desteklenmektedir. En sonunda,
Bölüm 5, bu teknik incelemeyi sınırlamaların tartışılmasıyla birlikte sonlandırır,
sorunlar ve gelecekteki geliştirme çalışmaları.
2 Qtum Performans Avantajı
Qtum'un birincil hedeflerinden biri, ilk UTXO tabanlı akıllı
Proof of Stake (PoS) [37] konsensüs modeli ile sözleşme sistemi. İkincisi
bir sonraki bloğun yaratıcısının kriptoda tutulan servete göre seçildiği anlamına gelir.
para birimi. Bu nedenle, bloklar genellikle madencilik yapılmak yerine dövülür veya orada darp edilir.
işlem ücretlerine ek olarak blok ödüllerdir ve sahtekarlar bir yüzde alır
koydukları fon miktarı için "faiz".
Qtum, Bitcoin ve Ethereum ekosistemleriyle uyumludur ve şunları hedefler:
Ethereum Virtual Machine (EVM) com ile bir Bitcoin varyasyonu üretmek
açıklık. Ethereum'dan farklı olarak, Qtum EVM'nin sürekli olarak geri döndüğünü unutmayın.
koğuşlar uyumludur. Pragmatik bir tasarım yaklaşımını benimseyen Qtum,
Mobil cihazlardan oluşan bir stratejiye sahip kullanım örneklerini deneyin. İkincisi Qtum'a izin verir
Blockchain teknolojisini geniş bir İnternet kullanıcıları yelpazesine tanıtmak ve böylece,
Merkezi olmayan PoS işlem doğrulaması.
Kalan kısım aşağıdaki şekilde yapılandırılmıştır. Bölüm 2.1 avantajları karşılaştırıyor
Ethereum hesap modeline karşı Bitcoin UTXO. Sonra, Bölüm 2.2 dis-
Qtum blok zinciri için fikir birliği platformuna küfrediyor. Bölüm 2.3,
Qtum sözleşmelerinin EVM'ye entegrasyonu. Son olarak, Bölüm 2.4,
Qtum operasyonları için ödeme modeli.
6 https://qtum.org/

---

4. sayfa

2.1 UTXO'ya Karşı Hesap Modeli
UTXO modelinde, işlemler girdi olarak harcanmamış Bitcoinleri kullanır.
stroyed ve işlem çıktıları olarak yeni UTXO'lar oluşturulur. Harcanmamış işlem
işlem çıktıları değişiklik olarak yaratılır ve harcayıcıya [1] döndürülür. Böylece,
farklı özel anahtar sahipleri arasında belirli miktarda Bitcoin aktarılır,
ve işlem zincirinde yeni UTXO'lar harcanır ve oluşturulur. Bir UTXO
Bitcoin işleminin kilidi, değiştirilmiş bir
bir işlemin sürümü. Bitcoin ağında madenciler,
işlem, herhangi bir girdi içermeyen, coinbase işlemi olarak adlandırılır. Bitcoin
Sınırlı sayıda işlem içeren işlemler için bir komut dosyası dili kullanır 7 . İçinde
Bitcoin ağı, komut dosyası sistemi verileri yığınlar halinde işler (Ana Yığın
ve Alt Stack), LIFO ilkesini izleyen soyut bir veri türü olan
Son Giren, İlk Çıkar.
Bitcoin istemcisinde, geliştiriciler isStandard () fonksiyonunu [1] kullanarak
betik türlerini marize edin. Bitcoin istemcileri şunları destekler: P2PKH (Genel Anahtara Öde
Hash), P2PK (Genel Anahtara Ödeme), MultiSignature (15'ten az özel anahtar işareti
tabiatlar), P2SH (Komut Dosyasına Öde Karma) ve OP_RETURN. Bu beş standartla
betik türleri, Bitcoin istemcileri karmaşık ödeme mantıklarını işleyebilir. Bunun yanında,
Madenciler kapsüllemeyi kabul ederse standart olmayan bir komut dosyası oluşturulabilir ve
çalıştırılabilir
standart dışı bir işlem.
Örneğin, komut dosyası oluşturma ve yürütme süreci için P2PKH kullanmak,
hayali Bitcoin ile bir fırında ekmek için 0.01BTC ödediğimizi varsayıyoruz.
adres ”Ekmek Adresi”. Bu işlemin çıktısı:
OP_DUP OP_HASH160 <Bread Public Key Hash> OP_EQUAL OP_CHECKSIG
OP_DUP işlemi yığındaki en üst öğeyi kopyalar. OP_HASH160 döndürür
en üst öğe olarak bir Bitcoin adresi. Bir bitcoin, bir Bitcoin reklamının sahipliğini kurmak için-
bir dijital anahtar ve bir dijital imza ile ek olarak elbise gereklidir. OP_EQUAL

İlk iki öğe tam olarak eşitse, aksi takdirde YANLIŞ (0) ise DOĞRU (1) sonucunu verir.
Son olarak, OP_CHECKSIG, bir değer ile birlikte bir genel anahtar ve imza üretir.
bir işlemin hash edilmiş verisine ait imza için kimlik belirleme, dönen
Bir eşleşme olursa DOĞRU.
Kilit komut dosyasına göre kilit açma komut dosyası:
<Ekmek İmzası> <Ekmek Genel Anahtarı>
Yukarıdaki ikisiyle birleştirilmiş komut dosyası:
<Ekmek İmzası> <Ekmek Genel Anahtarı> OP_DUP OP_HASH160
<Bread Public Key Hash> OP_EQUAL OP_CHECKSIG
Yalnızca kilit açma komut dosyası ve kilit komut dosyası önceden tanımlanmış eşleşen bir
koşul, komut dosyası kombinasyonunun yürütülmesidir. Ekmek demek
İmza, geçerli bir Ekmek Adresinin özel anahtarı ile eşleştirilerek imzalanmalıdır
imza ve sonra sonuç doğrudur.
Maalesef, Bitcoin'in kodlama dili Turing-complete değil, örneğin,
döngü işlevi yoktur. Bitcoin betik dili yaygın olarak kullanılmamaktadır
Programlama dili. Sınırlamalar, güvenlik risklerini engelleyerek azaltır.
7 https://en.bitcoin.it/wiki/Script

5.Sayfa

karmaşık ödeme koşullarının ortaya çıkması, örneğin, sonsuz döngüler oluşturma veya
diğer karmaşık mantık boşlukları.
UTXO modelinde, geçmişini şeffaf bir şekilde geriye doğru izlemek mümkündür.
halka açık defter aracılığıyla yapılan her işlem. UTXO modelinin paralel pro-
birden fazla adres arasındaki işlemleri başlatmak için yeteneği bırakarak,
uzayabilirlik. Ek olarak, UTXO modeli, bu kullanıcıların gizliliğini destekler.
Adresi Değiştir'i bir UTXO çıktısı olarak kullanabilir. Qtum'un hedefi
UTXO modelinin yenilikçi tasarımına dayalı akıllı sözleşmeler uygulayın.
UTXO modeline kıyasla Ethereum, hesap tabanlı bir sistemdir 8 . Daha ön
cisimle, her hesap devletle doğrudan değer ve bilgi aktarımı yaşar.
geçişler. 20 baytlık bir Ethereum hesap adresi,
bir işlem için tek seferlik işlemeyi sağlamak için sayaç,
Ether adı verilen işlem ücretlerini ödemek için ana dahili kripto yakıtı, isteğe bağlı
sözleşme kodu ve varsayılan-boş hesap deposu.
İki tür Ether hesabı bir yandan özel anahtar kontrollüdür
harici ve diğer yandan sözleşme kodu kontrollü. Eski kod geçersizliği
hesap türü, mesaj aktarımı için işlemleri oluşturur ve imzalar. İkincisi
dahili depolamayı okumak ve yazmak için bir mesaj aldıktan sonra kodu etkinleştirir,
sözleşmeler oluşturmak veya başka mesajlar göndermek.
Ethereum'da, bakiye yönetimi gerçek anlamda bir banka hesabına benzer.
dünya. Yeni oluşturulan her blok, potansiyel olarak
diğer hesaplar. Her hesabın kendi bakiyesi, deposu ve kod alanı tabanı vardır
diğer hesapları veya adresleri aramak için ve ilgili yürütme sonuçlarını saklar.
Mevcut Ethereum hesap sisteminde, kullanıcılar P2P işlemlerini şu yolla gerçekleştirir:
istemci uzaktan prosedür çağrıları. Daha fazla hesaba mesaj gönderilmesine rağmen
akıllı sözleşmeler mümkündür, bu dahili işlemler yalnızca
her hesabın bakiyesi ve bunları Ethereum'un halka açık defterinde izleme
meydan okuma.
Yukarıdaki tartışmaya dayanarak, Ethereum hesap modelini düşünüyoruz
ölçeklenebilirlik darboğazı olmak ve Bitcoin ağının net avantajlarını görmek
UTXO modeli. İkincisi, istediğimiz ağ etkisini artırdığından
teklif, beklemedeki Qtum sürümü için önemli bir tasarım kararı,
UTXO modelinin benimsenmesi.
2.2 Konsensüs Yönetimi

Mutabakat ve hangi platformun uygun olduğu konusunda devam eden tartışmalar var.
ilgili proje gereksinimlerinin ihtiyaçları. Mutabakat konuları en yaygın olarak
küfredilenler: PoW [41], PoS [2], Dinamik PoS 9 ve Bizans Hata Toleransı [7]
HyperLedger tarafından tartışıldığı gibi. Uzlaşmanın doğası, verilere ulaşmakla ilgilidir
dağıtılmış algoritmalarla tutarlılık. Mevcut seçenekler, örneğin Fischer
Lynch ve Paterson teoremi [5] olmadan fikir birliğine varılamayacağını belirtir.
Düğümler arasında% 100 anlaşma.
8 https://github.com/ethereum/wiki/wiki/White-Paper
9 http://tinyurl.com/zxgayfr

Sayfa 6

Bitcoin ağında madenciler, hash ile doğrulama sürecine katılırlar.
PoW üzerinden çarpışma. Bir madencinin hash değeri hesaplanabildiğinde ve
belirli bir koşulu karşılarsa, madenci ağa yeni bir blok olduğunu iddia edebilir
mayınlı:
Hash (BlockHeader) ≤
M
D
Madencilerin miktarı M ve madencilik zorluğu D için Hash () şunu temsil eder:
[0, M] ve D değer aralığına sahip SHA256 gücü. Kullanılan SHA256 algoritması
by Bitcoin, her düğümün her bloğu hızlı bir şekilde doğrulamasını sağlar.
madenciler, madencilik zorluğuna göre yüksektir.
80 baytlık BlockHeader, her bir farklı Nonce ile değişir. Genel fark
Zorlu madencilik seviyesi, toplam hash gücüne göre dinamik olarak ayarlanır
blockchain ağının. İki veya daha fazla madenci aynı anda bir bloğu çözdüğünde
zaman, ağda küçük bir çatallanma olur. Bu, blockchain'in
hangi bloğu kabul etmesi veya reddetmesi gerektiğine karar vermesi gerekir. İçinde
Bitcoin ağı, zincir en çok kanıtlanmış çalışmanın ekli olduğu meşrudur.
PoS blok zincirlerinin çoğu, miraslarını PeerCoin 10'a geri döndürebilir , yani
Bitcoin Core'un önceki bir sürümüne dayanmaktadır. Farklı PoW algoritmaları var
Scrypt 11 , X11 12 , Groestl 13 , Equihash [4] vb.
yeni bir algoritma, hesaplama gücünün tek bir
varlık ve Uygulamaya Özel Tümleşik Devrelerin (ASIC)
ekonomiye tanıtılması. Qtum Core, PoS'yi en son
Temel fikir birliği oluşumu için Bitcoin kaynak kodu.
Geleneksel bir PoS işleminde, yeni bir bloğun üretimi karşılamalıdır
aşağıdaki durum:
ProofHash <madeni para × yaş × hedef
ProofHash'ta, bahis değiştirici [40], harcanmamış çıktı ile birlikte hesaplar.
koyar ve şimdiki zaman. Bu yöntemle bir kötü niyetli saldırgan başlayabilir
büyük miktarlarda jeton yaşı biriktirerek çifte harcama saldırısı. Bir diğeri
Madeni para yaşının neden olduğu sorun, düğümlerin ödülden sonra aralıklı olarak çevrimiçi
olmasıdır.
Sürekli çevrimiçi olmak yerine ing. Bu nedenle, geliştirilmiş sürümünde
PoS anlaşması, madeni para yaşının kaldırılması, daha fazla düğümü çevrimiçi eşzamanlı olmaya
teşvik eder
neously.
Orijinal PoS uygulaması, aşağıdakilerden dolayı çeşitli güvenlik sorunlarından muzdariptir:
olası bozuk para yaşı saldırıları ve diğer saldırı türleri [16]. Qtum aynı fikirde
Blackcoin ekibinin güvenlik analizi [40] ve PoS 3.0 14'ü en son
Qtum Core. PoS 3.0 teorik olarak coinlerini daha uzun süre hisseden yatırımcıları ödüllendiriyor,
cüzdanlarını çevrimdışı bırakan madeni para sahiplerine hiçbir teşvik vermez.
10 https://peercoin.net/

11 https://litecoin.info/Scrypt
12 http://cryptorials.io/glossary/x11/
13 http://www.groestlcoin.org/about-groestlcoin/
14 http://blackcoin.co/

---

7. Sayfa

Akıllı Sözleşme Bilgileri ve Değer Lojistiği
7
2.3 Qtum Sözleşmesi ve EVM Entegrasyonu
EVM, 256 bitlik bir makine kelimesi ile yığın tabanlıdır. Çalışan akıllı sözleşmeler
Ethereum'da yürütmeleri için bu sanal makineyi kullanın. EVM tasarlanmıştır
Ethereum'un blok zinciri için ve bu nedenle, tüm değer aktarımının kullanıldığını varsayar.
hesap tabanlı bir yöntem. Qtum, Bitcoin'in blockchain tasarımına dayanıyor
ve UTXO tabanlı modeli kullanır. Böylece, Qtum bir hesap soyutlama katmanına sahiptir.
UTXO tabanlı modeli, hesap tabanlı bir arayüze çeviren
EVM. Hesaplamadaki bir soyutlama katmanının gizlemek için yararlı olduğunu unutmayın.
bir ayırma oluşturmak için belirli işlevselliğin uygulama ayrıntıları
birlikte çalışabilirliği ve platform bağımsızlığını kolaylaştırmaya yönelik endişeler.
EVM Entegrasyonu: Qtum'daki tüm işlemler Bitcoin Scripting Lan-
guage, tıpkı Bitcoin gibi. Ancak Qtum'da üç yeni işlem kodu var.
- OP_EXEC: Bu işlem kodu, bir işlemin özel olarak işlenmesini tetikler (açıklandı
aşağıda) ve belirli bir giriş EVM bayt kodunu yürütür.
- OP_EXEC_ASSIGN: Bu opcode ayrıca OP_EXEC gibi özel işlemleri tetikler.
Bu işlem kodu, sözleşme için bir sözleşme adresi ve veri girişi içerir. Sonraki
verilen veriyi geçerken sözleşme bayt kodunun yürütülmesini izler
(EVM'de CALLERDATA olarak verilir). Bu işlem kodu isteğe bağlı olarak parayı bir
akıllı sözleşme.
- OP_TXHASH: Bu işlem kodu, muhasebenin garip bir bölümünü uzlaştırmak için kullanılır
soyutlama katmanı ve şu anda yürütülen bir işlem kimliği karmasını iter
işlem.
Geleneksel olarak, komut dosyaları yalnızca bir çıktı harcamaya çalışırken çalıştırılır.
Örneğin, komut dosyası blok zincirindeyken, standart bir genel anahtarla
karma işlem, doğrulama veya yürütme gerçekleşmez. Yürütme ve doğrulama
İşlem girdisi çıktıya başvurana kadar işlem gerçekleşmez. Bu işte
nokta, işlem yalnızca girdi betiği (ScriptSig) sağlıyorsa geçerlidir.
ikincisinin sıfırdan farklı bir sonuç döndürmesine neden olan çıktı betiğine geçerli veriler.
Ancak Qtum, anında uygulanan akıllı sözleşmelere uyum sağlamalıdır.
blok zincirine birleştirildiğinde. Şekil 1'de gösterildiği gibi, Qtum bunu şu şekilde başarır:
içeren işlem çıktı betiklerinin (ScriptPubKey) özel olarak işlenmesi
OP_EXEC veya OP_EXEC_ASSIGN. Bu işlem kodlarından biri bir
komut dosyası, işlem yerleştirildikten sonra ağın tüm düğümleri tarafından yürütülür
bir bloğa. Bu modda, gerçek Bitcoin Komut Dosyası Dili, daha az
komut dosyası dili ve bunun yerine verileri EVM'ye taşır. İkincisi durumu değiştirir
kendi durum veritabanında, işlem kodlarından herhangi biri tarafından yürütülmesi üzerine, benzer
bir Ethereum sözleşmesine.
Qtum akıllı sözleşmelerinin kolay kullanımı için verileri doğrulamamız gerekiyor
akıllı bir sözleşmeye ve yaratıcısına belirli bir yayından gelen
keyhash adresi. Qtum blok zincirinin UTXO setini önlemek için
OP_EXEC ve OP_EXEC_ASSIGN işlem çıktıları çok büyük hale gelmekten
ayrıca harcanabilir. OP_EXEC_ASSIGN çıktıları, kodları sözleşmeler tarafından harcanır
başka bir sözleşmeye veya bir pubkeyhash adresine para gönderir. OP_EXEC çıktıları

---

8. Sayfa

8

Alex Norta
Şekil 1. Qtum işlem işlemi.
sözleşme intihar operasyonunu kendi kendini ortadan kaldırmak için kullandığında harcanır
blok zincirinden.
Qtum Hesap Soyutlama Katmanı EVM, bir
hesap tabanlı blok zinciri. Ancak Qtum, bitcoin tabanlı olduğundan UTXO-
tabanlı blok zinciri ve aşağıdakilere izin veren bir Hesap Soyutlama Katmanı (AAL) içerir
EVM, Qtum blok zincirinde önemli değişiklikler olmadan çalışacak
sanal makineye ve mevcut Ethereum sözleşmelerine.
EVM hesap modelinin akıllı sözleşme programcıları için kullanımı kolaydır.
Mevcut sözleşmenin dengesini ve diğer olumsuzlukları kontrol eden işlemler mevcuttur.
blok zincirindeki yollar ve para gönderme işlemleri var (ekli

---

Sayfa 9

verilere) diğer sözleşmelere. Bu eylemler oldukça basit ve küçük görünse de
malistik, UTXO tabanlı Qtum blok zincirinde uygulanması önemsiz değiller.
Bu nedenle, bu işlemlerin AAL uygulaması, daha karmaşık olabilir.
beklenen.
Bir Qtum-blockchain konuşlandırılmış akıllı sözleşme, onun tarafından atanır ve çağrılabilir
adres ve sıfır olarak ayarlanmış yeni konuşlandırılmış bir sözleşme bakiyesini içerir. Var
şu anda Qtum'da bir sözleşmenin bir
sıfır olmayan bakiye. Bir sözleşmeye para göndermek için işlem,
OP_EXEC_ASSIGN işlem kodu.
Aşağıdaki örnek çıktı komut dosyası bir sözleşmeye para gönderir:
1; sanal makinenin sürümü
10000; işlem için gaz limiti
100; Qtum satoshis'te gaz fiyatı
0xF012; sözleşmeyi göndermek için veriler
(genellikle Solidity ABI kullanır)
0x1452b22265803b201ac1f8bb25840cb70afe3303;
ripemd −160 kontrat txid hash değeri
OP EXEC ASSIGN
Yukarıdaki basit komut dosyası, işlem işlemeyi OP_EXEC_
ATAMA işlem kodu. Benzin çıkışının olmadığı veya başka istisnaların meydana gelmediği
varsayılırsa, değer
sözleşmeye verilen miktar OutputValue'dur. Gazın kesin detayları
mekanizmayı aşağıda tartışıyoruz. Bu çıktıyı blok zincirine ekleyerek, çıktı
sözleşmeye sahip UTXO kümesinin etki alanını girer. Bu çıktı değeri yansıtılır
Harcanabilir çıktıların toplamı olarak sözleşmenin dengesinde.
Şekil 2. Fonları atayın ve / veya bir mesaj sözleşmesi TX.
Şekil 2 standart bir halktan bir sözleşmeye para göndermeyi gösterse de
anahtar hash çıktısı, bir sözleşmeden diğerine para gönderme yöntemi
neredeyse aynı. Sözleşme başka bir sözleşmeye veya halka para gönderdiğinde
anahtar hash adresi, eski sahip olduğu çıktılardan birini harcıyor. Gönderen

---

Sayfa 10

sözleşme, fon gönderimi için Beklenen Sözleşme İşlemlerini içerir. Bunlar
işlemler, geçerli olabilmeleri için bir blokta bulunmaları gerektiğinden özeldir.
Qtum ağı. Beklenen Sözleşme İşlemleri madenciler tarafından yapılırken
tüketiciler tarafından üretilmek yerine işlemleri doğrulamak ve yürütmek.

Bu nedenle, P2P ağında yayınlanmıyorlar.
Şekil 3. Beklenen Sözleşme İşlem Listesini gösteren Qtum bloğu doğrulaması.
Beklenen Sözleşmeli İşlemleri gerçekleştirmek için birincil mekanizma,
Şekil 3'ün parçası olan yeni işlem kodu, OP_TXHASH, hem OP_EXEC hem de
OP_EXEC_ASSIGN iki farklı moda sahiptir. İnfazlarının bir parçası olarak
çıktı komut dosyası işleme, EVM yürütülür. İşlem kodları yürütüldüğünde
giriş komut dosyası işlemenin bir parçası olarak, ancak EVM,
çift yürütme. Bunun yerine, OP_EXEC ve OP_EXEC_ASSIGN işlem kodları davranır
işlemsizlere benzer ve 1 veya 0 döndürür, yani harcanabilir veya harcanamaz
sırasıyla, belirli bir işlem karma değerine göre. OP_TXHASH bu yüzden

---

bu kavramın işleyişi için önemlidir. Kısaca, OP_TXHASH yeni bir işlemdir
mevcut harcama işleminin SHA256 karmasını üzerine aktaran kod eklendi
Bitcoin Script yığını. OP_EXEC ve OP_EXEC_ASSIGN işlem kodları,
Harcama girişimi sırasında Beklenen Sözleşme İşlem Listesi.
İşlem (genellikle OP_TXHASH'den) işlem kodlarına geçtikten sonra
Beklenen Sözleşme İşlem Listesinde var, sonuç 1 veya harcama
yapabilmek. Aksi takdirde, getiri 0'dır veya harcanamaz. Bu şekilde OP_EXEC ve
Vouts kullanan OP_EXEC_ASSIGN yalnızca bir sözleşme olduğunda harcanabilir ve bu nedenle,
Hesap Soyutlama Katmanı, ödemenin harcanabilir olmasını gerektirir, yani
sözleşme para göndermeye çalışır. Bu, güvenli ve sağlam bir yolla sonuçlanır.
sözleşme fonlarının yalnızca uyumlu bir sözleşme tarafından harcanmasına izin vermek
normal bir UTXO işlemi ile.
Belirli bir senaryo, bir sözleşmenin birden fazla çıktıya sahip olması durumunda ortaya çıkar.
harcanmak. Her düğüm farklı çıktılar seçebilir ve bu nedenle tamamen farklı
OP_EXEC_ASSIGN işlemlerini harcamak için ferent işlemler. Bu çözüldü
Qtum'da fikir birliği açısından kritik madeni para toplama algoritması ile. İkincisi benzer
bir kullanıcı cüzdanında kullanılan standart para toplama algoritması. Ancak Qtum
hizmet reddi (DoS) riskini önlemek için algoritmayı önemli ölçüde basitleştirir
saldırı vektörleri ve basit fikir birliği kurallarını gerçekleştirmek. Bu fikir birliği ile kritik
madeni para toplama algoritması, artık diğer düğümlerin farklı seçim yapma olasılığı yoktur.
bir sözleşme ile harcanacak ent madeni paralar. Farklı çıktılar alan herhangi bir madenci / düğüm
ana Qtum ağından uzaklaşmalı ve blokları işleniyor
geçersiz.
Şekil 4'teki bir EVM sözleşmesi bir pubkeyhash'a para gönderdiğinde
adrese veya başka bir sözleşmeye göre, bu olay yeni bir işlem oluşturur.
mutabakat açısından kritik madeni para toplama algoritması, en iyi sahip olunan çıktıları seçer.
sözleşme havuzu. Bu çıktılar, girdi betiği ile girdi olarak harcanır.
(ScriptSig) tek bir OP_TXHASH işlem kodu içerir. Dolayısıyla çıktılar,
fonlar için varış yeri ve kalanları göndermek için bir değişiklik çıktısı (gerekirse) -
işlemin fonlarını sözleşmeye geri döndürmek. Bu işlem hash eklendi
Beklenen Sözleşme İşlem Listesine ve ardından işlemin kendisi
sözleşme yürütme işleminden hemen sonra bloğa eklenir. bir Zamanlar
Oluşturulan bu işlem doğrulanır ve yürütülür,
Beklenen Sözleşme İşlem Listesi aşağıdaki gibidir. Ardından, bu işlem karması
Beklenen Sözleşme İşlem Listesinden çıkarıldı. Bu modeli kullanarak,
sabit kodlu bir işlem sağlayarak bunları harcamak için sahte işlemleri yapmak imkansızdır.
OP_TXHASH kullanmak yerine girdi komut dosyası olarak hash.
Yukarıda açıklanan soyutlama katmanı, EVM sözleşmelerini ihmal eder.
madeni para toplama ve özel çıktılar. Bunun yerine, EVM sözleşmeleri yalnızca şunu bilir:
onların ve diğer sözleşmelerin bir bakiyesi vardır, böylece bunlara para gönderilebilir
sözleşmelerin yanı sıra sözleşme sisteminin dışından pubkeyhash adreslerine.

Sonuç olarak, Qtum ve Ethereum arasındaki sözleşme uyumluluğu güçlüdür
ve bir Ethereum sözleşmesini
Qtum blok zinciri.

Sayfa 12

12
Alex Norta
Şekil 4. OP_EXEC_ASSIGN işlem sözleşmesini harcayın.
Eklenen Standart İşlem Türleri: Aşağıdakiler standart işlemlerdir
Qtum'a eklediğimiz eylem türleri. Burada Bitcoin komut dosyası olarak belgelenmiştir.
şablonlar: Blok zincirine yeni bir sözleşme dağıtmak bir çıktı komut dosyası gerektirir
aşağıdaki gibi:
1; sanal makinenin sürümü
[Gaz limiti]
[Gaz fiyatı]
[Sözleşmeli EVM bayt kodu]
OP EXEC
Blockchain üzerinde halihazırda konuşlandırılmış bir sözleşmeye fon göndermek,
aşağıdaki komut dosyası:
1; sanal makinenin sürümü
[Gaz limiti]
[Gaz fiyatı]
[Sözleşmeye gönderilecek veriler]
[sözleşme işlem kimliğinin rip − emd160 karması]
OP EXEC ASSIGN
Gerektiği için harcama için standart bir işlem türü olmadığını unutmayın.
Beklenen Sözleşme İşlem Listesi. Bu nedenle, bu harcama işlemleri
P2P ağında ne yayın ne de geçerli.
2.4 Gaz Modeli
Qtum'un Bitcoin blok zincirine Turing-bütünlüğü eklemesiyle karşılaştığı bir sorun
caydırmak için makul olmayan bir işlemin yalnızca boyutuna güveniyor
madencilere ödenen ücret. Bunun nedeni, bir işlemin sonsuza kadar
işlem yapan madenciler için tüm blok zincirini döngüye alın ve durdurun. Şekil olarak
5 gösteri, Qtum projesi Ethereum'dan gelen gaz konseptini benimsiyor. İçinde
gaz konseptinde, yürütülen her EVM işlem kodunun bir fiyatı vardır ve her işlemin

---

Sayfa 13

Akıllı Sözleşme Bilgileri ve Değer Lojistiği
13
Harcanacak bir miktar gaz. İşlem sonrası kalan gaz,
gönderen.
Şekil 5. Gaz geri ödeme modeli.
Sözleşmenin yürütülmesi için gereken gaz, gaz miktarını aştığında
bir işlem için mevcutsa, bir işlemin eylemleri ve durum değişiklikleri
geri döndü. Böylece, değiştirilmiş herhangi bir kalıcı depolama, orijinal durumuna geri döndürülür.
herhangi bir sözleşme fonunun harcanmaması için herhangi bir harcama dahil. Rağmen
bir ters çevirme, bir işlemin tüm gazı tüketilir ve işleme verilir
hesaplama kaynakları zaten harcandığından beri madenci.
Qtum, Ethereum'un gaz modelini kullansa da, gaz planlamasını bekliyoruz.
ule, yani her EVM işlem kodunun gaz fiyatı Ethereum'dan önemli ölçüde farklıdır.
Kesin değerler, Ethereum'daki mevcut fiyatlar ile karşılaştırılarak belirlenir.
her işlem kodu için gereken işlem ve blok zinciri kaynaklarının miktarı
Qtum.
Bir sözleşme finansmanı veya dağıtım işlemi oluştururken, kullanıcı spesifikasyonu

gaz için iki özel öğe. GasLimit, tüketim miktarını belirler.
bir sözleşme yürütme ile mümkün gaz. İkinci öğe, ex-
Qtum Satoshis'teki her bir gaz biriminin fiil fiyatı. İkincisi şu anda daha küçük
Blockchain'in kaydettiği Bitcoin para biriminin birimi. Maksimum Qtum
bir sözleşme yürütme harcaması, GasLimit'in çarpımına eşittir.
GasPrice. Bu maksimum harcama, tarafından sağlanan işlem ücretini aşarsa

---

Sayfa 14

14
Alex Norta
bu durumda işlem geçersizdir ve madencilik yapılamaz veya işlenemez.
Bu maksimum harcama çıkarıldıktan sonra kalan işlem ücreti
İşlem Büyüklüğü Ücreti ve standart Bitcoin ücret modeline benzer.
Bir işlemin uygun önceliğini belirlemek için madenciler iki
değişkenler. İlk olarak, işlem boyutu ücreti, bir işlemin toplam boyutuyla eşleşmelidir.
yani, genellikle kilobayt formülü başına minimum para miktarı ile belirlenir.
İkinci değişken, bir sözleşme yürütmenin GasPrice değeridir. Kombinasyon halinde,
PoS madencileri işlemek için en önemli ve karlı işlemleri seçer
ve bir bloğa dahil edin. Sonuç olarak, bir serbest piyasa ücret modeli vardır.
madenciler ve kullanıcılar işlem hızlarına uyan en iyi ücreti optimize ediyor
ve ödemeye razı oldukları bedel.
Geri ödemeler: UTXO modelini kullanarak, madencilere işlem ücreti olarak gönderilen fonlar
pazarlığa açık değildir. Madencinin bir ücreti kısmen iade etmesi imkansızdır.
madencinin işlem yapması beklenenden daha kolaydır. Yine de, gaz için-
modelin yararlı olması için, parayı gönderene geri iadesi için bir yöntem mevcut olmalıdır.
Ayrıca, çalışan bir işlemin durumunu geri almak mümkün olmalıdır.
gazın bitmesi ve gaz ücretlerinin madencilere iade edilmesi.
Qtum'da gaz ücretlerinin iadesi,
bir madencinin madeni para bazlı işlemi. Yeni bir blok doğrulama konsensüsü ekliyoruz
Para iadesi çıktılarının coinbase işleminde mevcut olmasını sağlamak için kural.
Aksi takdirde, madenciler gazı iade etmemeyi seçebilirler. Geri ödeme,
çıktı betiğini kopyalayarak bir işlem fonunun göndereni. Güvenlik nedeniyle,
bu komut dosyası şu anda standart bir pubkeyhash veya scripthash için öde
senaryo. Daha fazla güvenlik çalışmasının ardından kısıtlamayı kaldırmayı planlıyoruz.
Referans için OP_EXEC_ASSIGN, con-
yol fonları:
Girişler: (itme sırasına göre)
- Harcama için işlem karması [isteğe bağlı]
- sürüm numarası (kullanılacak VM sürümü, şu anda yalnızca 1)
- gaz limiti (bu yürütme tarafından kullanılabilecek maksimum gaz miktarı)
- gaz fiyatı (Her bir gaz ünitesinin kaç qtum olduğu)
- veriler (bu akıllı sözleşmeye aktarılacak veriler)
- akıllı sözleşme adresi
Çıktılar: (pop sırasına göre)
- Harcanabilir (fonlar şu anda harcanabiliyorsa)
Sonuç olarak, aşağıda bir örnek EXEC_ASSIGN veriyoruz:
1
10000
100
0xABCD1234 ...
3d655b14393b55a4dec8ba043bb286afa96af485
EXEC_ASSIGN

Sayfa 15

Sanal makinenin yürütülmesi bir gaz dışı istisna ile sonuçlanırsa, bu ödeme,
OP_TXHASH betiğini kullanan bloktaki bir sonraki işlem.
Bu işlem için oluşturulan vout, şuradan alınan bir pubkeyhash betiğidir.
vin [0] .prevout komut dosyası. Qtum'un bu erken versiyonunda, yalnızca pubkeyhash
gönderenlere sanal makine finansman işlemleri için izin verilir. Diğer formlar olabilse de
VM yürütmesine neden olmak için bloklara kabul edildiğinde, EVM'deki msg.sender
"0" ve herhangi bir gaz bitmesi veya gerekli olan gaz iadesi, sözleşmenin sürdürülmesine neden olur
para kaynağı.
Kısmi Geri Ödeme Modeli: Gaz modeli ile ilgili olarak,
Harcanmamış kısmı çeşitli nedenlerle iade edin. Bir yandan kullanıcılar harcayabilir
sözleşmelerinin düzgün bir şekilde yürütülmesini sağlamak için büyük miktarda fon. Yine de
kullanılmayan gaz Qtum iadesi olarak iade edilir.
Gazın dönüş adresi blok zincirinde vin [0] olarak ifade edilir.
gönderen işlemin komut dosyası. Gaz, standart kullanılarak bir sözleşmeye gönderilir
bitcoin işlem ücreti mekanizması. Böylece yeni ücret modeli,
bu işlem ücretini yapmak için:
gaz ücreti = gaz limiti ∗ gaz fiyatı
txfee = vin - vout
tx geçiş ücreti = txfee - gaz ücreti
geri ödeme = gaz ücreti - kullanılmış gaz
Madencilerin hem tx_relay_fee hem de
işlemin belirlenmesi için tek bir "kredi fiyatı" değerinin altındaki gas_price
öncelik.
Sözleşmenin yürütülmesi sırasında, gaz jetonları toplam ücretten çıkarılır, yani,
gas_price ile çarpma. Sözleşmenin yürütülmesini tamamladıktan sonra, kalan-
Bu gas_fee'nin der'i, verilen gaz dönüş betiğine bir
madencilerin blok ödüllerini almak için kullandıkları coinbase işleminin çıktısı.
Coinbase eklenen vout vin [0] .prevout'tan bir pubkeyhash'tır. Amacıyla
bir gaz iadesi alırsanız, bu harcanan bir pubkeyhash ödemesi olmalıdır. Aksi takdirde, gaz
para iadesi madencide gaz dışı durumda kalır ve para gönderilir
sözleşmede kalacak.
Şu anda yalnızca bir EVM sözleşmesinin yürütülmesinin mümkün olduğunu unutmayın.
işlem başına. Böylece, iki sözleşmenin icra edilmesi durumunda asla ortaya çıkmaz.
işlem ücretini paylaşmaya çalışın. Bu senaryo çözüldükten sonra etkinleştirilebilir
İşlem başına birden fazla EVM uygulamasıyla ilgili mevcut sorunlar. Mevcut
tasarım, işlem başına birden çok sözleşme yürütmeyi destekler.
Önemli GAS Edge Durumları: Madenciler sözleşmeli gaz konusunda dikkatli olmalı,
ve fon-getiri senaryoları. İkinci komut dosyası çıktısı bir bloğun
maksimum boyut daha sonra sözleşme işlemi bu bloğa konulamaz.
Bunun yerine, gaz dönüşü komut dosyası yürütmesi, bir sonraki madencilikte tekrar gerçekleşmelidir.
blok. Madenciler, aday blokta yeterli kapasitenin bulunmasını sağlamalıdır.
sözleşmeyi yürütmeden önce gaz dönüşü betiği. Takip etmemek
bu kural, geri ödeme betiğinin

Sayfa 16

mevcut bloğa uymuyor. İade edilecek gaz fonu yoksa, ödeme yok
fonların iade edilmesi için şart vardır.
İşlem ücretinin gas_fee'yi içerdiği konusunda fikir birliği kritiktir. Bir trans-
bir bloğa eklerken eylem geçersizdir, negatif bir gaz iadesi ile sonuçlanır veya
gas_fee işlem ücretinden düşük olduğunda.

Birden fazla OP_EXEC içeren hiçbir işlem çıktı komut dosyası geçerli değildir veya
OP_EXEC_ASSIGN işlem kodu. Bu, komut dosyası oluşturma yeteneklerini sınırlasa da tercih edilir
potansiyel özyineleme ve çoklu yürütme sorunlarına. Sonuç olarak, statik
analizi, bir komut dosyasının geçersiz olup olmadığını belirlemek için yeterlidir.
Oldukça blok zinciri odaklı Qtum tekniklerinden sonra, şimdi kavramı açıklayacağız-
her zaman akıllı sözleşme yaşam döngülerinin yönetimi. Kavramsal ön
devam filmindeki cümle bilimsel literatür tarafından desteklenmektedir [12, 13, 24, 18, 26, 27, 32].
3 Akıllı Sözleşme Yönetimi
Yukarıda belirtildiği gibi, yaşam döngüsü yönetiminin güvenlik için gerekli olduğunu varsayıyoruz.
Akıllı sözleşmeler yapmak, potansiyel işbirliği yapan tarafların uygun şekilde incelenmesini sağlamak
yürürlüğe girmeden önce gerçekleşir. Başarısız bir deniz mahsulünden gerçek hayattaki bir vakayı
düşünüyoruz
bir ticari işlem çatışmasının yetersiz tanımlanmış bir durumdan ortaya çıktığı durumlarda teslimat 15
geleneksel sözleşme (CC). Bir AB şirketi (alıcı) 12920 kg mürekkep balığı siparişi verir.
Güney Asyalı bir şirketten (satıcı) balık. CC'de ürünün sorumluluğu
Taşıyıcı malları alana kadar kalite satıcıya aittir. Belirsiz
Fikasyon, CC'de belirtilmeyen malların kalitesiyle ilgilidir ve
Alıcı, nakliye şirketine devredilmeden önce malları kontrol etmez
(taşıyıcı).
Akıllı sözleşme alternatifi, yetersiz spesifikasyon ihtilafını çözer.
CC'de var. Bu nedenle, Bölüm 3.1'de sunulan Qtum-çerçeve hedef modeli
tamamen resmileştirilmiş bir akıllı sözleşme yaşam döngüsünün özelliklerini yansıtır.
[18, 26, 27, 32]. Daha sonra, Bölüm 3.2 deniz ürünleri için küçük bir yaşam döngüsü örneği
vermektedir.
sevkiyat çantası.
3.1 Yaşam Döngüsü Yönetimi Hedefleri
Hedefleri tartışmak için aşağıdaki yaklaşımı kullanıyoruz. Ajan Odaklı Model
ing (AOM) yöntemi [38] bir sosyo-teknik gereksinimler-mühendislik yaklaşımıdır
bu, kuruluşlara ait olabilecek insanların teknoloji kullandığını hesaba katar.
problemleri çözmek için işbirliği yapma bilimi. Bu bölümde, AOM kullanıyoruz
hedef-model türü için önemli sosyo-teknik davranış özellikleri
Koşu çantasını destekleyen Qtum akıllı sözleşme sistemi. Hedef modelleri
teknik ve teknik olmayan paydaşlar arasındaki iletişimi,
problem alanının anlaşılmasını artırmak. AOM hedef modellerinin
aynı zamanda yeni çevik yazılım geliştirme teknikleri için de yararlıdır [39].
15 http://cisgw3.law.pace.edu/cases/090324s4.html

Şekil 6. AOM hedef modelleri için modelleme öğeleri.
Bir hedef modeli, Şekil 6'da gösterilen üç ana unsurdan oluşur.
Hedefler olarak adlandırdığımız ve paralelkenarlar, roller olarak tasvir edildiğimiz tional gereksinimler
yapışkan adamlar ve işlevsel olmayan gereksinimler olarak tasvir ediyoruz. İkincisi iki
varyantlar, yani yazılımla ilgili işlev dışı gereksinimler için kalite hedefleri
bulutlar olarak tasvir edilmiş ve insanla ilgili duygusal hedefler elips olarak tasvir edilmiştir.
hedef modeli, atomik olmayan bir merkezi kök değer önermesiyle başlar. Con-
sırayla, değer önerisi bir ağaç hiyerarşisinde alt hedeflere ayrıştırılır
Her bir alt hedef, ana hedefine ulaşmak için bir yönü temsil ettiğinde [21] ve
en düşük alt hedef atomik olmalıdır. Hedeflere roller, kalite ve kalite atanmış olabilir.
alt düzey hedeflere miras kalan duygusal hedefler.
Qtum Çerçevesinin Değer Önerisi: Hedefin kökü
Şekil 7'de tasvir ettiğimiz Qtum-çerçevesi ve bu, çaprazın değer önermesidir.
organizasyonel bilgi ve değer aktarımı lojistik otomasyonu. Biz böldük
akıllı sözleşme yaşam döngüsü yönetimi için hedeflere karmaşık değer önerisi

[26, 27, 32], yani kurulum, kullanıma sunma, yürürlüğe koyma, geri alma, sonlandırma. Bunlar rafine Bölüm 3.2'de daha detaylı inceleyeceğimiz hedefler.
Şekil 7. Yaşam döngüsü yönetimi iyileştirmesi ile Qtum değeri önerisi [26, 27, 18].
Şekil 7'de sektörün benimsenmesi için temel bir duygusal hedef,
amaçlanan davranışı güvenilir bir şekilde gerçekleştirmek için sosyoteknik Qtum-sistemi [34]. İçinde bu durumda güven, teknolojiyi kullanan insanlar arasındaki bağımlılıklarla ilgilidir.
hedeflere ulaşmak için. Ekonomik olarak uygun ve ek olarak benimsemesinin kolay olduğunu düşünüyoruz
yaygın endüstri yayılımını etkileyen duygusal hedefler. İlk anlamı

Sayfa 18

Qtum sistemini kullanmanın ekonomik yatırım getirisi sağlarken,
ikincisi, Qtum ile çalışmak için kişisel giriş engelinin düşük olduğu anlamına gelir.
Değer önerisiyle bağlantılı olan ve herkesi etkileyen kalite hedefleri vardır.
Qtum sisteminin parçalarını iyileştirmek. Bir referanstan çıkardığımız bu kalite hedefleri
organizasyonel iş süreci farkında işbirliği için mimari [28].
Aşağıdaki kalite hedefleri [9, 17] 'ye göre yapılandırılmıştır. Aşağıdaki
Sistem yürütme sırasında kalite hedefleri fark edilemez.
Değiştirilebilir, Qtum sisteminin yaşam döngüsü boyunca değiştiği ve adapte olduğu anlamına gelir
iş bağlamına. Ek olarak, organizasyonel olarak het-
ticari yazılımların düzenli olarak güncellenmesini içeren erojen sistem ortamları
eşya. Entegre edilebilir sistemler, ayrı ayrı geliştirilmiş ve entegre edilmiş bilgisayarlardan oluşur.
bileşenler arasındaki arayüz protokollerinin eşleşmesi gereken ponentler.
Bu nedenle, Qtum'un bileşenleri arasındaki entegrasyon sağlanmalıdır.
Ardından, Qtum için koşu sırasında fark edilebilen kalite hedeflerini belirliyoruz.
zaman. Birlikte çalışabilirlik, Qtum'un çalışma zamanında sistemlerle birlikte çalışması gerektiği anlamına gelir
planlama, lojistik, üretim, harici gibi iş fonksiyonlarını desteklemek
ortak sistemler vb. Dinamik birlikte çalışabilirlik zorlukları ticari,
kavramsal ve teknik heterojenlik. Güvenli, yetkisiz kişilere direnmek anlamına gelir
Güvenilir kullanıcılara hizmet sağlarken kullanım ve hizmet reddi girişimleri
iyi bir üne sahip. Güvenlik, güven ve itibar sorunlarını ele almak için, sev-
Qtum için genel stratejiler mümkündür. Blockchain destekli bir kimlik doğrulama
hizmet işbirliği yapan tarafları denetler, ağ olaylarını izler, denetler ve günlüğe kaydeder.
Bir sistemin iletişimi şifrelenebilir, vb. Son derece otomatik
işbirliği, sistemlerin tüm akıllı sözleşme yaşam döngüsünü kapsamasını gerektirir.
Bu nedenle, Qtum yüksek derecede anlamlı renk olasılıkları sağlamalıdır.
izin verirken sıkıcı ve tekrarlayan işleri işleyen emek otomasyonu
İnsanların kalan yaratıcı eyleme odaklanması. Esnek işbirliği,
hetero-
gen verileri [25]. Bu nedenle, Qtum çeşitli kuruluşlar arası işbirliğine olanak sağlamalıdır.
heterojen kavramları ve teknolojileri uyumlaştıran konuşma senaryoları. Kullanılabilir
Kuruluşlar arası bilgi lojistiği için Qtum'un kullanımı kolay olması gerektiği anlamına gelir
otomasyon ve üç alana ayrışır. Hata önleme önceden tahmin edilmelidir
ve yaygın olarak ortaya çıkan işbirliği hatalarını önleyin. Hata işleme sistemdir
bir kullanıcının hatalardan kurtarması için destek. Öğrenilebilirlik, gerekli olanı ifade eder
kullanıcıların Qtum sistemine hakim olma zamanını öğrenme.
Son olarak, mimariye özgü kalite hedefleri vardır. Tamlık
akıllı sözleşme ömrü için gerekli bileşenleri içeren Qtum kalitesidir.
döngü yönetimi. Ölçeklenebilirlik, Qtum'un
iki ortak taraf tek bir konfigürasyonda. Uygulanabilir, Qtum'un
Organizasyonlar arası bilgi lojistiğini ve değerini otomatikleştirmek için araç
transferler. Taşınabilir, Qtum'un bilgi lojistiğini,

iş açısından endüstriyel alan ve işbirliği heterojenliği-,
kavramsal ve teknolojik sistem altyapısı. Bu aynı zamanda mo-
safra cihazları. Performant, hesaplama ve iletişimsel gerginlik anlamına gelir
bilgi-lojistik otomasyonu için düşüktür. Bu nedenle, bunu sağlamak önemlidir

---

Sayfa 19

akıllı sözleşme yaşam döngüsünün tüm aşamaları, istenen bir yanıt dahilinde gerçekleştirilir
zaman ve üstel bilgi işlem gücüne ihtiyaç duymadan.

3.2 Yaşam Döngüsü Yönetimi Örneği

Bölüm 3.1'deki hedef modeli, çalışırken projeksiyon yapmak için Şekil 8'de haritalandırıyoruz.
deniz mahsulleri vakası. Şekil 8'deki modelleme gösterimi iş süreci modelidir
BPMN [22] notasyonu ve tüm yaşam döngüsü [26, 27, 18] 'de resmileştirilmiştir.
Yeşil daire yaşam döngüsünün başlangıcını ve kırmızı daire yaşam döngüsünü gösterir.
son. Artı işaretli dikdörtgenler, karşılık gelen alt işlemlerdir.
Bölüm 3.1'deki yaşam döngüsü aşamalarına. Bir alt süreç, gizleyen bir bileşik faaliyettir.
alt düzey iş süreci ayrıntıları.
Şekil 8. Qtum akıllı sözleşme yaşam döngüsü yönetimi.
Şekil 8'deki her bir akıllı sözleşme yaşam döngüsünün başlangıç noktası,
Organizasyonlar arası bilgi gerektiren deniz ürünleri taşımacılığı durumu lo-
lojistik otomasyonu. Bir işbirliği merkezi [29] olduğunu varsayarsak,
bir tasarımcı, akıllı sözleşmelerin başlangıcı için bir hazırlık platformu oluşturur
hizmet türlerinin dahil olduğu bir iş ağı modeli (BNM) için bir şablon
rollerle birlikte eklenir.
BNM şablonu, doldurma aşamasına girer. Yeniden ilişkili roller
akıllı hizmet türleri, akıllı teknolojide işbirliği yapan kuruluşlarla doludur.
sözleşme, yani banka2, satıcı, buzdolabı1, taşıyıcı, buzdolabı2, alıcı ve banka1. Not
birkaç aday kuruluşun bir
belirli bir rol. Bir rolü yerine getirme arzusunu güçlendirmek için, potansiyel ortak veya-
ganizasyonlar, bir hizmet teklifini bir rolün bağlı olduğu hizmet türüyle eşleştirmelidir
ile. Bir hizmet tüketicisi teklifi değerlendirebilir ve bir hizmet teklifi olup olmadığına karar verebilir
kabul edilebilir.
Tüm roller doldurulduğunda ve hizmet türleri kabul edilebilir hizmetle eşleştiğinde
teklifler, akıllı sözleşme müzakereleri başlar. Hiçbir parti üstlenmiyoruz

---

Sayfa 20

Deniz ürünleri teslimatı davası yürütmek, aynı fikirde olmama ve kurulum aşamasını getirme arzusuna
sahiptir.
ani bir sona. Bunun yerine alıcı,
deniz ürünlerinin bulunduğu kapların içindeki sıcaklıkla ilgili yükümlülükler
saklanmış. Sevkiyat konteynerlerinin Nesnelerin İnterneti ile donatıldığını varsayıyoruz
(IoT) [15] gönderici, satıcı ve alıcıyı gerçek zamanlı olarak bilgilendiren sensörler
sıcaklık eşiği ihlali meydana gelir. Alıcının karşı teklifi,
bu durum, indirilene göre bir fiyat indiriminin ardından gelir.
deniz ürünlerinin kalitesi. Sıcaklık değişikliği deniz ürününün
artık tüketime uygunsa, alıcı satın almayı reddetme hakkına sahiptir.
varışta sevkiyat.
Karşı teklif diğer tüm taraflarca kabul edilir ve bir fikir birliği oluşur,
bir sözleşme kuruluşu için ön koşul olan budur. Akıllı sözleşme bir
dağıtılmış bir yönetişim altyapısının (DGI) sağladığı koordinasyon ajanı
çıkarılmalıdır. Böylece, devam eden vakanın her bir tarafı yerel bir sözleşme alır.

bir dizi ilgili yükümlülüğün çıkarıldığı kopya. Örneğin, bir zorunlu
Taşıyıcı için, bir deniz ürünleri nakliye kirasının içindeki sıcaklığın
tainer asla 20C'nin üzerinde olmamalıdır. Yükümlülükler gözetmenler tarafından gözetilir ve
IoT sensörlerine bağlanan atanmış iş ağı modeli aracıları (BNMA).
Ardından, işbirliği yapan tüm taraflar kendi özel süreçlerini atayabilir
[12] ortaya çıkan (DGI) içine. Örneğin, eşler arası ödeme varsayıyoruz
Alıcının önce Euro ile satın alması gereken Bitcoin ile. Bu satın alma ve
banka yoluyla ödeme1, uygunluk ve raporlamayı içeren bir süreci içerir.
Hükümet kripto para birimlerinin kullanımına ilişkin düzenlemeleri empoze ederken adımlar. İçin
satıcının banka1 ve banka2 arasında bilgi alışverişini sağlayan şirket,
iletişim uç noktaları oluşturulmalıdır. Bu şekilde satıcının yönetimi
uyumluluk verileri otomatiktir.
Etki alanında bir sıcaklık eşiği yükümlülüğünün ihlal edildiğini varsayarsak
buzdolabı1'de, atanmış bir BNMA olayı yükseltir ve alıcı,
ihlal şiddeti. Sıcaklık ihlali belirli bir süre devam ederse
daha düşük bir fiyata başarılı bir satışa izin veren azalmış deniz ürünleri kalitesinde
alıcının tahammül ettiğine göre, bir yanıt daha fazla soğutma talep edebilir
Buzdolabı1 rolüne giren farklı bir şirket tarafından. Deniz ürünlerinin olduğunu varsayarsak
ciddi şekilde şımarık ve hedef ülkede satılamaz, alıcı tetikler
işlemi daraltan yıkıcı bir geri dönüş. Deniz ürünleri sevkiyatı
Alıcı ile üzerinde anlaşmaya varılan durumda ulaşır ve ödemeyi satıcıya yapar
bank2 aracılığıyla tamamlanır, ardından sonlandırma aşaması DGI'yi çözer ve serbest bırakır
tüm işbirliği yapan taraflar.
Daha sonra ayrıntılı işbirliği öğeleri arasındaki ilişkileri vereceğiz.
Şekil 8 koordinatlarının yaşam döngüsü yönetimi.
4 Değer Aktarım Protokolü
Qtum çerçevesinin ayrılmaz bir parçası, bir değer aktarımı protokolu kavramıdır.
Organizasyonlar arası bilgi lojistiğini ve değerini düzenleyen col (VTP)

Sayfa 21

Transferler, değer önerisi doğrultusunda Şekil 7'de tasvir edilmektedir. Sonuç olarak, Sec-
4.1, bir VTP'yi oluşturan süreç türlerinin ilişkisini açıklar. Bölüm
4.2, yardımcı programla belirli bir akıllı sözleşme diline duyulan ihtiyacı tartışır.
VTP'leri belirtin. Son olarak, Bölüm 4.3, VTP destekli bir
Ethereum'un kullandığı Solidity'ye karşı dil.
4.1 Organizasyonlar Arası Süreçler
VTP, üç farklı işbirliği sürecinden oluşur. Figür 9
Deniz ürünleri teslimatı için BPMN gösteriminde basitleştirilmiş bir BNM gösterir.
3 tanıtım. BNM, bir dizi alt işlemin yer tutucular olduğunu varsayar
kuruluşların rollerini belirten etiketlere sahip hizmet türleri için [12, 13].
deniz mahsulleri teslimi
BNM
deniz mahsulleri teslimi
BNM
Şekil 9. Qtum BNM.
BNM'nin aynı zamanda hizmet tipi alt-
koreografi kontrol akışının oluşturulması için süreçler. Basit olması için Şekil 9
AND-split ve -join ile birlikte etiketlenmemiş koreografi görevlerini gösterir.
BNM, deniz ürünleri satıcısının bankayı hazırlaması için bilgilendirmesiyle başlar.
uluslararası bir para birimi işlemi için ve daha sonra deniz ürünleri daha önce soğutulur.
bir taşıyıcı varış noktasına nakliye gerçekleştirir. Hedef ülkede,
Yerel bir banka para birimi işlemini gerçekleştirirken deniz ürünleri tekrar soğutulur
iki ülke arasında. Son olarak, alıcı yerel satış için deniz ürünlerini alır.

taşıyıcı hizmet türü
süreç görünümü
taşıyıcı hizmet türü
süreç görünümü
Şekil 10. Dışsallaştırılmış hizmet tipi süreç görünümü.
BNM'nin taşıyıcı alt süreci için, varsayım şudur:
deniz ürünleri taşıyıcısının rolünü doldurmak için tarih organizasyonları mevcuttur. Şekil 10, bir

---

Sayfa 22

bir hizmet türü profesyonel şeklinde daha düşük düzeyli bir iyileştirme için basitleştirilmiş örnek
ara görünümü [12, 13]. Şekil 10'daki basitleştirilmiş süreç, bir taşıyıcının aldığını varsayar
kaynak ülkedeki buzdolabından elde edilen deniz ürünleri ve
satıcı. Daha sonra, üç paralel dal, sıcaklık izlemenin hazırlanmasını gerektirir.
Teslimat evraklarının alınması ve hedef şirketteki soğutma firmasının bilgilendirilmesi
eşzamanlı olarak gerçekleşir. Yalnızca aday bir kuruluş hizmet olabilir.
Bu basitleştirilmiş sürece bağlı kalmayı vaat eden taşıyıcı sağlamak. Unutmayın ki
işbirliği merkezi [30], eşleştirme için hizmet türü süreç görünümleri sunabilir.
ikincisi ilgili hizmet sunan kuruluşlarla.
yerel taşıyıcı sözleşmesi
yerel sözleşme
yerel taşıyıcı sözleşmesi
yerel sözleşme
Şekil 11. Yerel taşıyıcı sözleşmesi.
Üçüncü bir VTP öğesi olarak, Şekil 11, taşıyıcının kullandığı yerel sözleşmeyi göstermektedir.
dahili olarak. Şekil 10'daki hizmet türü süreç görünümünden farklı olarak,
yerel sözleşme, alıcıları bilgilendiren etiketlerle iki ek görev içerir
ve banka2'yi şarj edin. Bu nedenle, yerel sözleşme, hizmet türünün bir alt sınıfıdır.
canlandırma davranışı [12, 13] ile ilgili süreç görünümü, yani
Operatörün ekleme seçeneği varken işlem görünümü harici olarak deneyimlenir
mahremiyet sağlayan bir şekilde rekabet oluşturan gizli ek adımlar
avantajlıdır veya harici ekran için ilgi çekici değildir vb.

4.2 Qtum Akıllı Sözleşme Dili

Bölüm 4.1'deki VTP senaryosunu desteklemek için, mevcut akıllı sözleşme dili
franca Solidity, içerilenler açısından gerekli fayda düzeyine sahip değil
kavramlar ve özellikler. Bunun yerine, akıllı bir Qtum geliştirmenin amacı
nispeten daha iyi faydaya sahip sözleşme dili (QSCL) ve derleyici
VTP yönetimi için.
Yüksek seviyeli QSCL kavramları ve özellikleri, Şekil 12'de tasvir edilmektedir. VTP sce-
Bölüm 4.1'deki nario, adanmış bir eSourcing çerçevesine benzer.
dil mevcuttur, şu anda eSourcing Biçimlendirme Dili (eSML) [31]
anlamsal web alanı için belirtilmiştir. Kavramların haritasını çıkarmayı planlıyoruz ve
eSML'nin blok zinciri etki alanına, QSCL'yi bir
yeni bir Qtum sanal makinesi için dil derleyicisi.
Kısaca, daha fazla ayrıntı için okuyucuya [31] 'e başvururken, özellikler
Şekil 12'de kavramsal sorular doğrultusunda organize ediyoruz. Bir QSCL örneği

---

Sayfa 23

şirket verisi
company_contact_data
resource_section

data_definition_section
business_context_provisions
legal_context_provisions
exchange_value
süreç
yaşam döngüsü tanımı
yaşam döngüsü eşleme
active_node_label_mapping
izlenebilirlik
exchange_value
Qtum Sm
sanat-C
Ontra
ct Lan
ölçü
W
ho
W
o
yeniden
W
Ha
t
M
uygulama
pa
rty
(birleşme)
QSCL
Şekil 12. Gelecekteki Qtum akıllı sözleşme dilinin [31] özellikleri ve kavramları.
bir BNM tanımına benzer (Şekil 9). QSCL'nin Who kavramı şunları içerir:
Sözleşme taraflarını, dahil olanlarla birlikte benzersiz bir şekilde tanımlamak için yapılar
kaynaklar ve veri tanımları. Nerede kavramı iş bağlamını belirtir
ve ayrıca belirli bir akıllı sözleşmenin geçerli olduğu yasal bağlam hükümleri.
Değiştirilen değerleri ve hizmet türü sürecini tanımlamaya hangi kavram izin verir?
bu tür süreç görünümleri için yaşam döngüsü tanımlarıyla birlikte görünümler (Şekil 10) ve
ayrıca sırasıyla temel görevler için. Böylece, bir QSCL'nin hangi bölümünde-
duruşu, çeşitli hizmet türü süreç görünümleri Şekil ile karşılaştırılabilir şekilde tanımlanabilir
9. Son olarak, birleşim yapıları özellikle tanımlanmış değişim kanallarıdır.
kuruluşlar arası veri akışı. İzlenebilirlik yapıları esnek bir
Anket veya mesajlaşma kullanan özel görev izleme tanımı
prensip.

4.3 Karşılaştırmalı Tartışma

Akıllı sözleşme ontolojisini [31] kullanarak, gayri resmi olarak
Qtum çerçevesi için oluşturduğumuz QSCL'ye karşı mevcut Solidity. Gibi
Genel bir gözlem, Solidity, çoğunlukla düşük seviyeye odaklanan bir dildir.
JavaScript'e benzeyen sözdizimine sahip blok zinciri manipülasyon komutları. Yine de
üçüncü taraf API'leri içe aktarmak ve harici işlev çağrıları gerçekleştirmek mümkündür. Yani-
Solidity'de harici işlevler olarak adlandırılan bir akıllı sözleşme arayüzünün parçası olan
diğer sözleşmelerden ve işlemlerden çağrılabilir.
Solidity'nin Turing-bütünlüğü nedeniyle, prensipte mümkündür
smart'ın tüm kavramları ve özellikleri için hantal destekleri tanımlamak için

Alex Norta
QSCL'nin içerdiği kontrat ontolojisi. Bununla birlikte, desen temelli gibi kavramlar
tasarım, süreç bilinci, süreçlerin eşleştirilmesi vb. hiçbir şekilde benimsenmez.
Solidity'de yol. Hantal geçici çözümler icat etmekle ilgili olarak, yakın zamanda
konferans kağıdı yayını [43], Solidity'yi kullanarak fizibilitesini gösterir.
akıllı sözleşmelerde güvenilmeyen iş süreci izleme ve yürütme.
Solidity'nin tarihsel olarak resmi kaynaklar tarafından desteklenmediğini vurgulamak gerekir.
doğrulama, QSCL'nin [31] tasarım başlangıcından farklı olarak anlamına gelir. Böyle olmadan
resmi olarak doğrulanabilir ifade, yasalaşmadan önce bilmek mümkün değildir
bir sözleşme doğruysa ve güvenlik sorunları yoksa. Sağlamlıkla ilgili bir güvenlik
olay 16 , yalnızca çok yakın bir zamanda geliştirilmesini ve uygulanmasını tetikledi.
gibi doğrulama araçları Neden 17 , Sertleştiricisi 18 veya Casper 19 o a muhtemel potansiyel
müşteriler
hep birlikte Ethereum için iş kanıtı'ndan risk kanıtı'na geçiş.
5. Sonuçlar
Bu teknik inceleme, yeni bir akıllı sözleşme bloğu için Qtum çerçevesini sunar.
zincir teknolojisi çözümü. Spesifik Qtum işlem işleme teknolojisini gösteriyoruz
Proof-of-stake doğrulamasını kullanan plementasyon. Dahası, Qtum entegre olur
Bitcoin harcanmamış işlem ile birlikte Ethereum sanal makinesi (EVM)
tion çıktı protokolü. Qtum EVM'nin sürekli olarak geriye doğru kaldığını unutmayın
uyumlu. Ek olarak, Qtum çerçevesi akıllı sözleşmenin
yaşam döngüsü yönetimi, renklendirmenin uygun güvenlik incelemesini desteklemek için önemlidir.
emekçi partiler. Qtum yaşam döngüsü yönetimini desteklemek için, mevcut dil
franca Solidity uygunluktan yoksundur. Sonuç olarak, ortaya çıkan Qtum çerçevesi
gelişmiş yardımcı programa sahip yeni bir akıllı sözleşme dili gerektirir.
Proof of Stake'in Qtum'a benimsenmesi önemli bir tasarruf teşkil ediyor
hala kullanılan, ölçeklenmeyen Ethereum alternatifine göre hesaplama çabası
işin kanıtı. Ethereum, proof-of-stake'i de benimsemeyi planlasa da, belli değil
böyle yeni bir sürüm ne zaman piyasaya sürülecek. Ayrıca harcanmamış işlemlerin kullanımı-
puts, Ethereum'un hesap yönetimine kıyasla daha ölçeklenebilir. İçinde
Basit ödeme doğrulamasıyla birlikte Qtum, zaten akıllı bir
mobil cihaz çözümü ile sözleşme yapın. Ölçeklenmeyen Ethereum çözümü,
mobil çözümlere izin vermeyen Qtum, demokratik ve yüksek
mobil stratejisi ile dağıtılmış teminat kanıtı işlem doğrulaması.
Qtum çerçevesi, gelecekteki kalite kriterlerine ilişkin net bir anlayışa sahiptir.
gelişmeler tatmin etmelidir. İşlevsel gereksinimlerle ilgili olarak, Qtum planları
akıllı sözleşme yaşam döngüsü yönetimi için bir uygulama katmanı geliştirmek. Çoğu
daha da önemlisi, bu tür bir yaşam döngüsü yönetimi, işbirliğini incelemek için önemlidir.
Ethereum'un yakın zamanda yaşadığı gibi güvenlik ihlallerini azaltmak için taraflar,
ikincisinin birden fazla sert çatalına neden olur.
16 https://www.wired.com/2016/06/50-million-hack-just-showed-dao-human/
17 http://why3.lri.fr/
18 https://hack.ether.camp/idea/solidifier—formal-verification-of-solidity-programs
19 http://www.coindesk.com/ethereum-casper-proof-stake-rewrite-rules-blockchain/

Sayfa 25

Akıllı Sözleşme Bilgileri ve Değer Lojistiği
25
Qtum'daki bilgi lojistiği için değer aktarım protokolü,
İşbirliği yapan birkaç organizasyonun koreografisi için iş ağı modeli.
İkincisi, aşağıdakilerle uyuşması gereken yerel sözleşmelerle hizmetler sağlayabilir:
iş ağında hizmet türü işlem görünümlerinin belirtilen çalışma zamanı davranışı
model. Çok katmanlı akıllı sözleşme yönetim katmanıyla, işbirliği
taraflar, rekabet yaratan ticari sırlarının gizliliğini korurlar.
yerel sözleşmelerde uzatma adımlarını gizleyerek avantaj sağlar.

Özetle, Qtum çerçevesi akıllı sözleşmelerin çok-
Temel kalite gereksinimlerini de hesaba katması gereken cioteknik eserler-
yaygın kullanıcı benimsemesini sağlamak için. Devam eden gerçek hayattaki endüstri projeleri
Qtum uygulamaları ile sürekli ampirik gereksinim hasadı sağlar.
Yüksek oranda dağıtılmış hisse kanıtı işlemlerini destekleyen mobil strateji
işleme, en son teknolojide önemli bir ilerlemeyi amaçlamaktadır. Yine de, Qtum
ayrıca akıllı sözleşme yaşam döngüsü yönetiminin uygulama gerektirdiğini de kabul eder.
Gelişmiş ön uç kullanıcı deneyimine sahip katman geliştirme, şu anki
İfadeler yeterince dikkat etmiyor.
Referanslar
1. AM Antonopoulos. Bitcoinlerde ustalaşma, 2014.
2. I. Bentov, A. Gabizon ve A. Mizrahi. *İş Kanıtı Olmayan Kripto Para Birimleri* ,
sayfa 142–157. Springer Berlin Heidelberg, Berlin, Heidelberg, 2016.
3. K. Bhargavan, A. Delignat-Lavaud, C. Fournet, A. Gollamudi, G. Gonthier,
N. Kobeissi, N. Kulatova, A. Rastogi, T. Sibut-Pinote, N. Swamy ve S. Zanella-
Béguelin. Akıllı sözleşmelerin resmi doğrulaması: Kısa makale. In *Proceedings
2016 ACM Workshop on Programming Languages and Analysis for Security* ,
PLAS '16, sayfa 91–96, New York, NY, ABD, 2016. ACM.
4. A. Biryukov ve D. Khovratovich. Equihash: Asimetrik çalışma kanıtı,
genelleştirilmiş doğum günü problemi. *NDSSâ˘AZ16 Bildirileri, 21–24 Şubat
2016, San Diego, CA, ABD. ISBN 1-891562-41-X* , 2016.
5. B. Bisping, PD Brodmann, T. Jungnickel, C. Rickmann, H. Seidler, A. Stüber,
A. Wilhelm-Weidner, K. Peters ve U. Nestmann. A'nın mekanik doğrulaması
flp için yapıcı kanıt. In *İnteraktif Teoremi Konferansı
İspatlama* , 107–122. Sayfalar. Springer, 2016.
6. O. Bussmann. *Finansın Geleceği: FinTech, Teknoloji Bozulması ve Düzenleme
Innovation* , sayfa 473-486. Springer Uluslararası Yayıncılık, Cham, 2017.
7. C. Cachin. Hyperledger blockchain kumaşının mimarisi. In *Çalıştayına
Dağıtılmış Kripto Para Birimleri ve Konsensüs Defterleri* , 2016.
8. K. Christidis ve M. Devetsikiotis. İnternet için blok zincirleri ve akıllı sözleşmeler
şeyler. *IEEE Erişimi* , 4: 2292–2303, 2016.
9. L. Chung, BA Nixon, E. Yu ve J. Mylopoulos. *İşlevsel olmayan gereksinimler
yazılım mühendisliği* , cilt 5. Springer Science & Business Media, 2012.
10. K. Croman, C. Decker, I.Eyal, AE Gencer, A. Juels, A. Kosba, A. Miller, P. Sax-
ena, E. Shi, E. Gün Sirer, D. Song ve R. Wattenhofer. *Merkezi Olmayan Ölçeklendirmede
Blok zincirleri* , sayfalar 106–125. Springer Berlin Heidelberg, Berlin, Heidelberg, 2016.
11. N. Emmadi ve H. Narumanchi. İzin verilenin değişmezliğini güçlendirmek
anahtarsız imzaların altyapısına sahip blok zincirleri. *18.* In *Tutanaklarında*

Dağıtık Hesaplama ve Ağ Oluşturma üzerine uluslar arası *Konferans* , ICDCN '17,
sayfa 46: 1–46: 6, New York, NY, USA, 2017. ACM.
12. R. Eshuis, A. Norta, O. Kopp ve E. Pitkanen. Süreç ile hizmet dış kaynak kullanımı
Görüntüleme. *Hizmet Hesaplamasında IEEE İşlemleri* , 99 (Ön Baskı): 1, 2013.
13. R. Eshuis, A. Norta ve R. Roulaux. Gelişen süreç görünümleri. *Bilgi ve
Yazılım Teknolojisi* , 80:20 - 35, 2016.
14. D. Frey, MX Makkes, PL Roman, F. Taıani ve S. Voulgaris. Güvenli hale getirmek
akıllı telefonunuza bitcoin işlemleri. In *15 Uluslararası Proceedings
Uyarlanabilir ve Yansıtıcı Ara Yazılım Çalıştayı* , ARM 2016, sayfalar 3: 1-3: 6, Yeni
York, NY, ABD, 2016. ACM.
15. J. Gubbi, R. Buyya, S. Marusic ve M. Palaniswami. Nesnelerin İnterneti (IoT): A
vizyon, mimari unsurlar ve gelecekteki yönler. *Gelecek Nesil Bilgisayar
Sistemler* , 29 (7): 1645 - 1660, 2013.

16. A. Kiayias, I. Konstantinou, A. Russell, B. David ve R. Oliynykov. Kanıtlanabilir bir güvenli kanıtı blok zinciri protokolü, 2016.
17. G. Kotonya ve I. Sommerville. *Gereksinim mühendisliği: süreçler ve teknoloji niques* . Wiley Yayınları, 1998.
18. L. Kutvonen, A. Norta ve S. Ruohomaa. İşletmeler arası ticari işlem açık hizmet ekosistemlerinde yönetim. In *İşletme Nesne Dağıtılmış Uyum- puting Conference (EDOC), 2012 IEEE 16th International* , sayfa 31-40. IEEE, 2012.
19. L. Luu, DH Chu, H. Olickel, P. Saxena ve A. Hobor. Akıllı Sözleşmeler Yapmak Daha akıllı. In *Bilgisayarda 2016 ACM SIGSAC Konferansı Tutanakları ve İletişim Güvenliği* , CCS '16, sayfalar 254–269, 2016.
20. L. Luu, V. Narayanan, C. Zheng, K. Baweja, S. Gilbert ve P. Saxena. Güvenli açık blok zincirleri için parçalama protokolü. In *2016 ACM SIGSAC Proceedings Bilgisayar ve İletişim Güvenliği Konferansı* , CCS '16, sayfalar 17–30, New York, NY, ABD, 2016. ACM.
21. J. Marshall. Dijital medya tasarımında duygusal hedeflerin ajana dayalı modellemesi projeleri imzala. *Uluslararası İnsan Odaklı Programlama Dergisi (IJPOP)* , 3 (1): 44–59, 2014.
22. İş Süreci Modeli. Gösterim (bpmn) sürüm 2.0. *Nesne Yönetim Grubu şartname* , 2011. http://www.bpmn.org.
23. S. Nakamoto. Bitcoin: Eşler arası elektronik nakit sistemi. *Danışıldı* , 1 (2012): 28, 2008.
24. NC Narendra, A. Norta, M. Mahunnah, L. Ma ve FM Maggi. Ses çatışması sanal kurumsal işbirlikleri için yönetim ve çözüm. *Servis Odaklı Hesaplama ve Uygulamalar* , 10 (3): 233–251, 2016.
25. A. Norta. *Dinamik Kuruluşlar Arası İş Süreci İşbirliğini Keşfetmek- yon* . Doktora tezi, Eindhoven Teknoloji Üniversitesi, Bilgi Bölümü Sistemler, 2007.
26. A. Norta. *Merkezi Olmayan Au- için Akıllı Sözleşme İşbirliklerinin Oluşturulması tonom Organizasyonlar* , sayfalar 3–17. Springer Uluslararası Yayıncılık, Cham, 2015.
27. A. Norta. *Çapraz Süreçlerin Uygulanmasına Yönelik Dağıtılmış Yönetişim Altyapılarının Kurulması Organizasyon İşbirlikleri* , sayfalar 24–35. Springer Berlin Heidelberg, Berlin, Hei- delberg, 2016.
28. A. Norta, P. Grefen ve NC Narendra. Yönetmek için bir referans mimari dinamik organizasyonlar arası iş süreçleri. *Veri ve Bilgi Mühendisliği* , 91 (0): 52 - 89, 2014.

---

29. A. Norta ve L. Kutvonen. Bir hizmet olarak iş süreçlerine aracılık etmek için bir bulut merkezi mengene: Yarı otomatik arka plan kontrolünü destekleyen bir "buluşma" platformu kurumlar arası işbirliği için iş ortağı keşfi. In *SRII Küresel Konferansı (SRII), 2012 Yıllık* , sayfalar 293–302, Temmuz 2012.
30. A. Norta ve L. Kutvonen. Bir hizmet olarak iş süreçlerine aracılık etmek için bir bulut merkezi mengene: Yarı otomatik arka plan kontrolünü destekleyen bir "buluşma" platformu kurumlar arası işbirliği için iş ortağı keşfi. *Yıllık SRII Küresel Konferansı ence* , 0: 293–302, 2012.
31. A. Norta, L. Ma, Y. Duan, A. Rull, M. K˜olvart ve K. Taveter. eContractual Organizasyonlar arası iş birliğine yönelik koreografi-dil özellikleri- yon. *İnternet Hizmetleri ve Uygulamaları Dergisi* , 6 (1): 1–23, 2015.
32. A. Norta, AB Othman ve K. Taveter. Hükümet için anlaşmazlık çözme yaşam döngüleri

Merkezi olmayan özerk organizasyon işbirliği. In *Proceedings 2015 2Nd Uluslararası Elektronik Yönetişim ve Açık Toplum Konferansı: Eurasia'daki Zorluklar* , EGOSE '15, sayfalar 244–257, New York, NY, ABD, 2015. ACM.
33. Aafaf Ouaddah, Anas Abou Elkalam ve Abdellah Ait Ouahman. *A doğru Blockchain Teknolojisine Dayalı Yeni Gizliliği Koruyan Erişim Kontrol Modeli Iot içinde* , sayfalar 523-533. Springer Uluslararası Yayıncılık, Cham, 2017.
34. E. Paja, AK Chopra ve P. Giorgini. Sosyotekniklerin güvene dayalı spesifikasyonu sistemleri. *Veri ve Bilgi Mühendisliği* , 87: 339 - 353, 2013.
35. J. Poon ve T. Dryja. Bitcoin yıldırım ağı: Ölçeklenebilir zincir dışı anlık ödemeler, 2015.
36. M. Rosenfeld. Renkli madeni paralara genel bakış. *Beyaz kağıt, bitcoil. co. il* , 2012.
37. P. Serguei. Nxt dövme algoritmasının olasılık analizi. *Defter* , 1: 69–83, 2016.
38. L. Sterling ve K. Taveter. *Ajan odaklı modelleme sanatı* . MIT Press, 2009.
39. T. Tenso, A. Norta ve I. Vorontsova. Yeni bir çevik gereksinimleri değerlendirme mühendisliği Neering yöntemi: Bir vaka çalışması. In *11. Uluslararası Konferansı Tutanakları Yazılım Mühendisliğinde Yeni Yazılım Yaklaşımlarının Değerlendirilmesi - Cilt 1: ENASE*, sayfa 156–163, 2016.
40. P Vasin. Blackcoinâ˘AZs proof-of-stake protokolü v2, 2014.
41. M. Vukolic. Ölçeklenebilir blockchain dokusu arayışı: Proof-of-work ile bft repli-katyon. In *Ağ Güvenliği Açık Sorunları Uluslar Atölye* , sayfalar 112–125. Springer, 2015.
42. M. Vukolic. *Ölçeklenebilir Blok Zinciri Yapısı Arayışı: İş Kanıtı - BFT Çoğaltma* , sayfa 112–125. Springer Uluslararası Yayıncılık, Cham, 2016.
43. I. Weber, X. Xu, R. Riveret, G. Governatori, A. Ponomarev ve J. Mendling. *Blockchain Kullanarak Güvenilmeyen İş Süreci İzleme ve Yürütme* , sayfalar 329–347. Springer Uluslararası Yayıncılık, Cham, 2016.
44. G. Wood. Ethereum: Güvenli bir merkezi olmayan genelleştirilmiş işlem defteri. *Ethereum Projesi Sarı Kağıt* , 2014.