Bitcoin'de Mahremiyet

Faruk Terzioğlu

26.09.2019

Bitcoin'de Mahremiyet

+ Bitcoin’in Bazı Teknik Özellikleri
+ Bitcoin’in Fungible Olması
+ Muhtemel Mahremiyet Eksiklikleri
+ İşaretlenmiş ve Dokunulmamış Bitcoin’ler
+ Mahremiyete Bir Çözüm: Liquid Network

Bitcoin

+ Günümüzdeki bir çok blokzinciri ya ‘harcanmamış işlem çıktısı tabanlıdır’ veya ‘hesap/bakiye’ tabanlıdır.

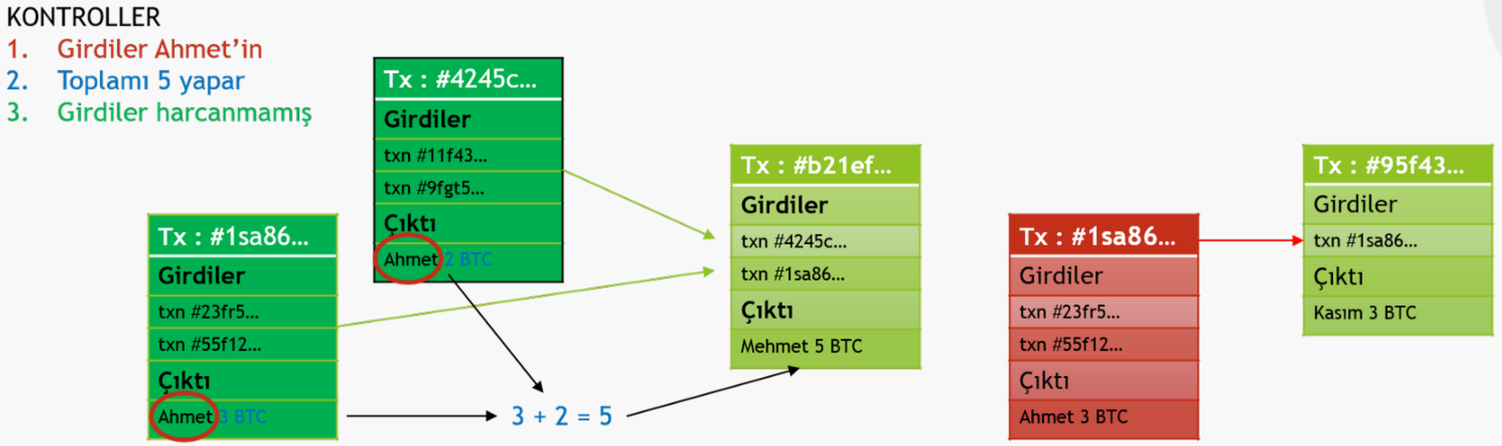
+ Bitcoin blokzinciri, harcanmamış işlem çıktısı tabanlı bir blokzincirdir.

Transfer İşlemleri

+ Bitcoin' deki her işlem daha önceki bir işlemin çıktısını harcar ve daha sonra harcanmak üzere yeni bir çıktı oluşturur.

+ Her bir transfer işlemi bu harcanmamış işlem çıktısı kümesindeki bir değişimi temsil eder

+ Bu harcanmamış işlem çıktısına da kısaca UTXO denmektedir.



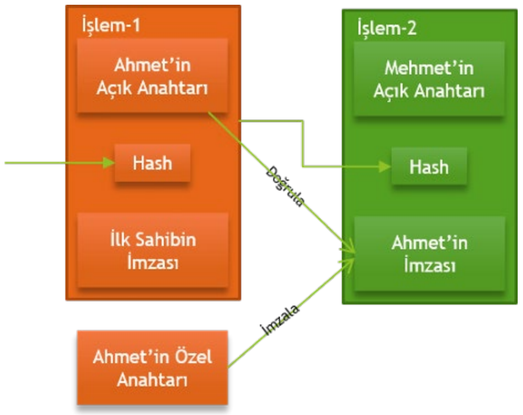
Transfer İşlemleri

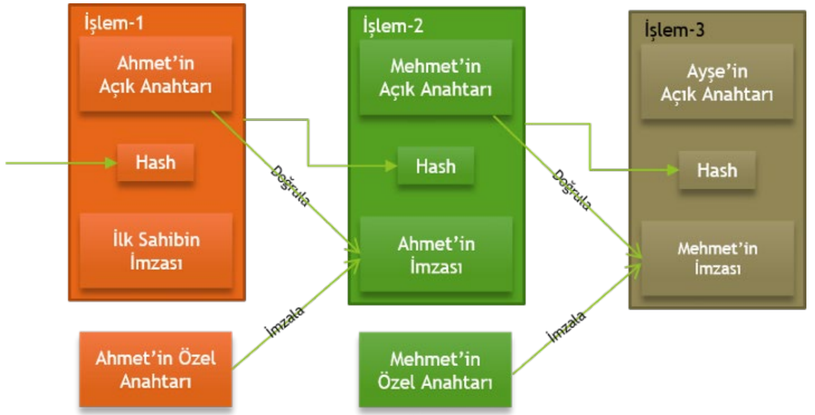
+ UTXO modelinde herbir transfer işlemi bir veya daha fazla UTXO'yu referans alır.

+ Böylece bir işlemler zinciri meydana gelir.

+ Bu ilişki zinciri sayesinde, bir aracı olmaksızın herhangi biri, işlemlerin bütünlüğünü doğrulayabilir.

+ Her bir işlem sonsuza kadar saklanır.

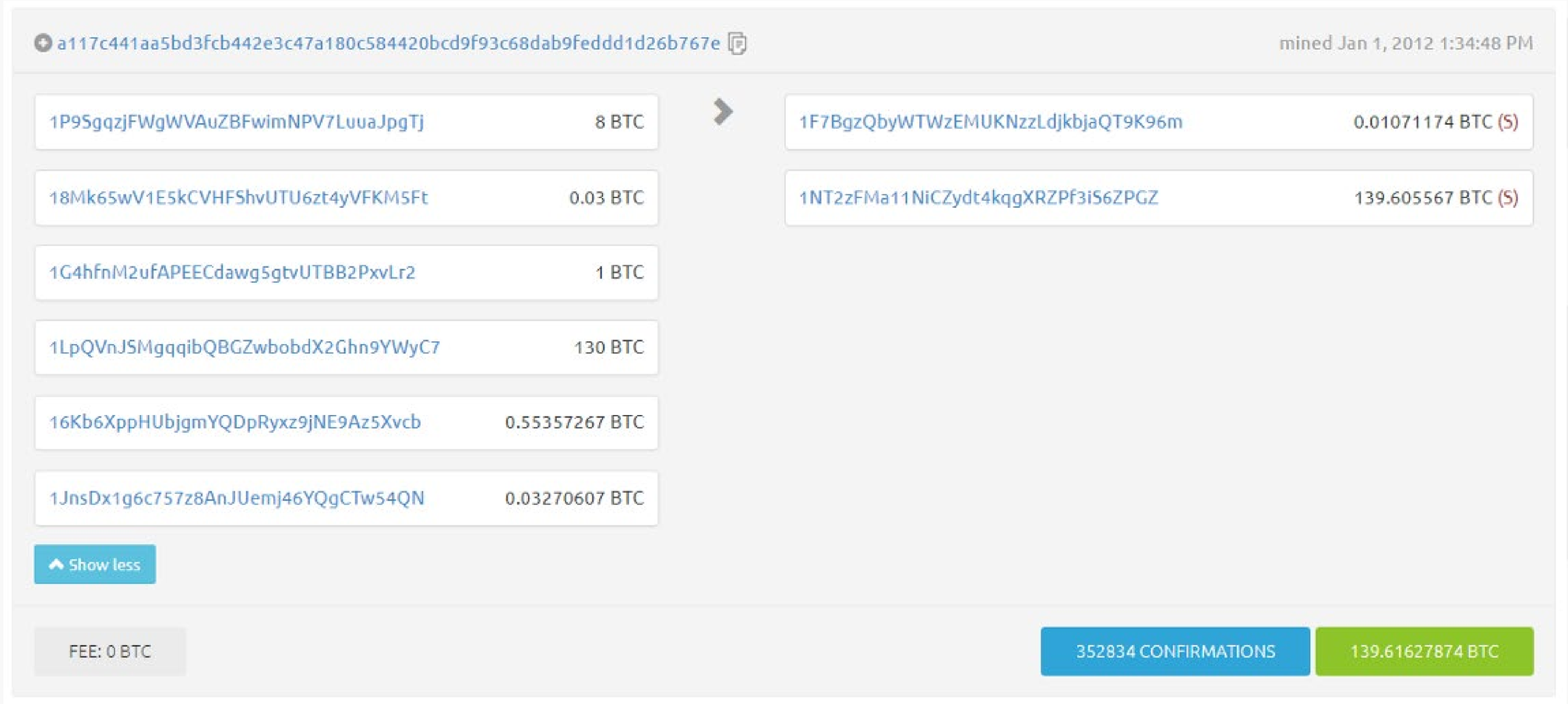




Transfer İşlemleri

- **Bakiye** : Kişilere tanımlı harcanmamış çıktıların toplamı

Transfer İşlemleri



Transfer İşlemleri

+ 5 Btc'lik transfer için 100 Btc'lik UTXO referans alınabilir.

+ Size tanımlanacak 95 Btc'lik başka bir işlem çıktısı oluşur.

+ Oluşan 95 Btc'lik paraüstü ağdaki herkes tarafınan görülebilir.

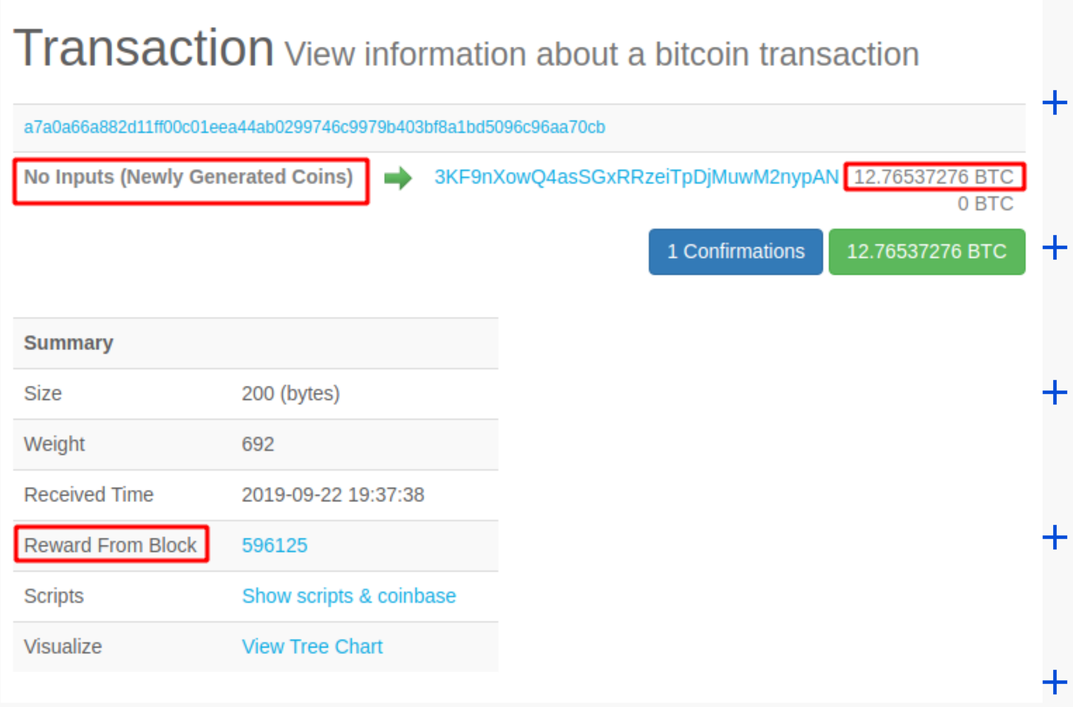
+ Adresler anonimdir, fakat alıcı sizin 95 Btc'ye sahip olduğunuzu bilebilir.

Defter

Kimden	Kime	Nekadar
34jsdfklk5j31...	13kjhFg34daz...	2.0
d1123l212354...	e44ds23211d...	15.0
43fvdsq2vsd1f...	13kjhFg34daz...	3.0
21kjhFg34dza...	d1123l212354...	6.0
d1123l212354...	34jsdfklk5j31...	0.005

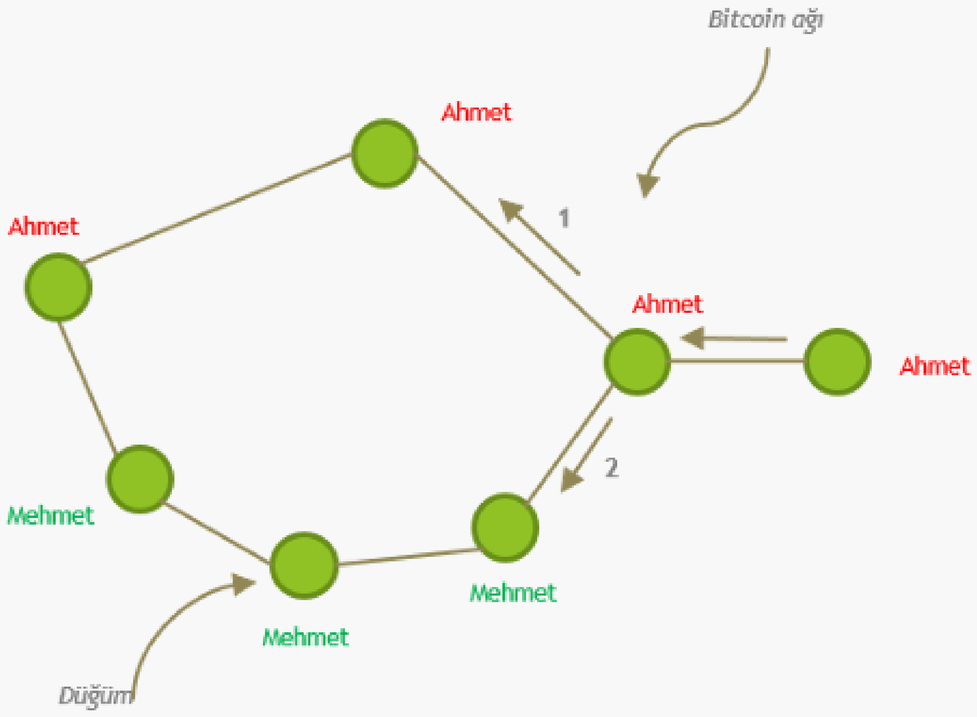
13kjhFg34daz56hyy65674
5 BTC

Coinbase İşlemler



+ İstisnai bir işlem: Coinbase işlemi
+ Madenciler yeni blok bulduğunda ödül alır.
+ Kendilerine transfer tanımlar: 12.5 BTC
+ Hiçbir işlemi referans almaz, geçmişi yoktur.
+ Madenci tarafından o anda üretilir.
+ Yeni bitcoin'lerin girişi sağlanır.

İşlemlerin Doğrulanması



+ Güvenliği evrensel bir doğrulama sistemi sağlanır.
+ Ağa dahil olan herkes işlemlerin doğrulunu onaylar.
+ Herhangi bir 3. partiye güven gerektirmez.
+ Doğrulama için işlem detayları açık olmalı.
+ Geçersiz bitcoin üretilmediğinden enim olunur.

Özetle

+ Transferlerin kimden kime yapıldığı herkese açık, fakat anonim.

+ Hangi varlıktan ne kadar gönderilmiş herkese açık ve sonsuza kadar saklanır.

+ İşlemler arası ilişki.

+ İstisna bir işlem: Coinbase.

Fungibility

+ Fungibility (takas edilebilirlik),
Bir malın veya emtianın her biriminin kendi cinsinden başka bir mal ile takas edilebilirliği ve her parçasının diğer parçasından ayırt edilememesidir.

+ Fiat paralar gibi.
Bir adet 10 liralık banknot ile diğer bir 10 lira veya 2 adet 5 liralık banknot aynı değere sahiptir.

+ Bir kilo altın, başka bir kilo altın ile her zaman aynı değere sahiptir.

Fungibility

+ Bitcoin de benzerdir. Her bir bitcoin, başka bir bitcoin ile aynı değere sahiptir.

+ İki farklı 1 bitcoinlik işlemi birleştirerek 2 bitcoin transfer edilebilir.

+ 0.5 bitcoinlik transfer için 1 bitcoin gönderdiğinizde, aynı değerde 0.5 bitcoin para üstü gelir.

+ A borsasından aldığınız 1 bitcoin ile B borsasından aldığınız 1 bitcoin aynı değerdedir.

+ Bir birinin yerine geçebilirdir, yani fungible'dır.

Fungibility

+ Blokzincir analiz araçları ile bitcoin transfer işlemlerini takip etmek ve kim tarafından kullanıldığını tesbit etmek mümkün oluyor.

+ Bitcoinlerin takip edilebilir olması, fungible olmasına engel teşkil edebilir.

+ Peki nasıl oluyor?

Fungibility

+ Bitcoinde işlemlerin geçmişinin tutulur ve işlemler arası ilişki vardır.

+ Kötü amaçlı bir işlemde kullanılan bitcoin başka işlemlerde kullanılabilir.

+ Kara para aklama ile ilişkili bir hesaptan geliyorsa, bu UTXO'yu kullanamayabilirsiniz.

+ Transfer gönderebilirsiniz fakat karşılığı olan hizmeti alamayabilirsiniz.

+ Borsalar, kara listelerindeki bir adresten dolaylı olarak da transfer alan hesapları dondurabilir.

Fungibility

+ 1 bitcoinin değeri başka bir yerden aldığınız 1 bitcoinden düşük olabilir.

+ Bu tarz bitcoin daha düşük fiyatlardan alıcı bulabilir.

İşaretlenmiş Bitcoin

+ Geçmişinde kötü amaçlı bir işlem barındıran (Silk Road, kumar siteleri, sahtekarlık projeleri) bu tarz koinlere, ‘tainted’ yani lekeli koin deniyor.

+ Bunların lekeli olma dereceleri var.

+ Çeşitli firmalar bitcoin üzerinde leke analizini yapıyor.

+ Bir bitcoin, kötü amaçlı kullanılmış başka bir bitcoin ile ne kadar ilişkiliyse o seviyede lekeli oluyor.

İşaretlenmiş Bitcoin

Taint Analysis 1F1tAaz5x1HUXrCNLbtMDqcw6o5GNn4xqX

Taint is the % of funds received by an address that can be traced back to another address.

This pages shows the addresses which have sent bitcoins to 1F1tAaz5x1HUXrCNLbtMDqcw6o5GNn4xqX. The data can be used to evaluate the anonymity provided by a mixing service. For example Send Coins from Address A to a Mixing service then withdraw to address B. If you can find Address A on the taint list of Address B then the mixing service has not sufficiently severed the link between your addresses. The more "taint" the stronger the link that remains.

Received (Origin) Taint

Branch	Address	Taint (%)	Count	Top IPs
	1ECNHmKyKFguDCyQGed2Cs15M9E2WXXxdr	56.2902868656%	6	
	19EzWn1vQTEoeti42nRna872Gpfs5KKiJb	20.5996335831%	1	
	1GwgrgrQU1dmQZ1KeNxoj82DfxkSrYKd62	16.1361777982%	2	
	15MwTft5QSnYGENERub91MLZ8bxsfQTViN	15.0910196993%	1	
	16rkU8tFXtBDE3LKZezW6RuzVLhqD8VC2W	13.9353582395%	1	
	1Fsa4M1gL8ezhoJGMWCDLog7LMS8aJDLP1	11.7712191904%	8	
	1FAv42GaDuQixSzEzSbx6aP1Kf4WVWpQUY	11.3477648654%	1	
	18DQ8tmKytHaTVyymwe6qi8fDhZKAxW9f7	10.5431296852%	1	
	1JKuNCLPKjThvNs3HE8CK4CitCQzyM24FX	10.5431296852%	1	
	1MHHQ84VAgPGEGmsGYXP5Ut3idg31PbUTs	10.5431296852%	1	
	1KsDTCSj9TF2bSMWMNj7BdBDP137dV3Gsu	10.5431296852%	1	
	15T4SK1MTo3ELCAnTCSAq4PBM3uqqomZvu	10.5431296852%	1	
	1KFJyCwArFMt6eBEh934p1JQWuCkmxAwLy	10.2610777754%	1	

İşaretlenmiş Bitcoin

Silkroad Seized Coins Addresses are identifiers which you use to send bitcoins to another person.

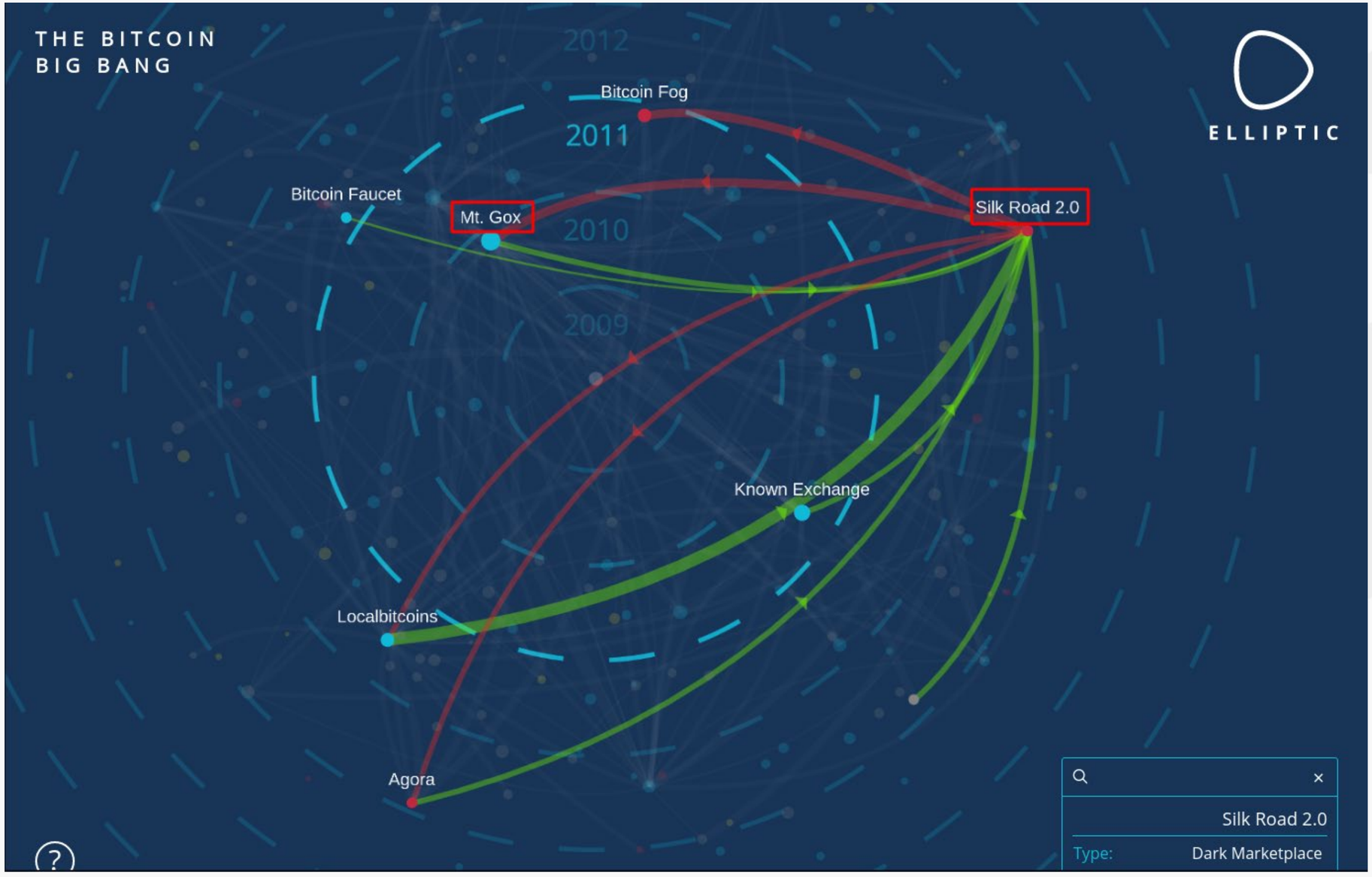
Summary	
Address	1F1tAaz5x1HUXrCNLbtMDqcw6o5GNn4xqX
Total Received	29,679.07451498 BTC

Transactions (Oldest First)

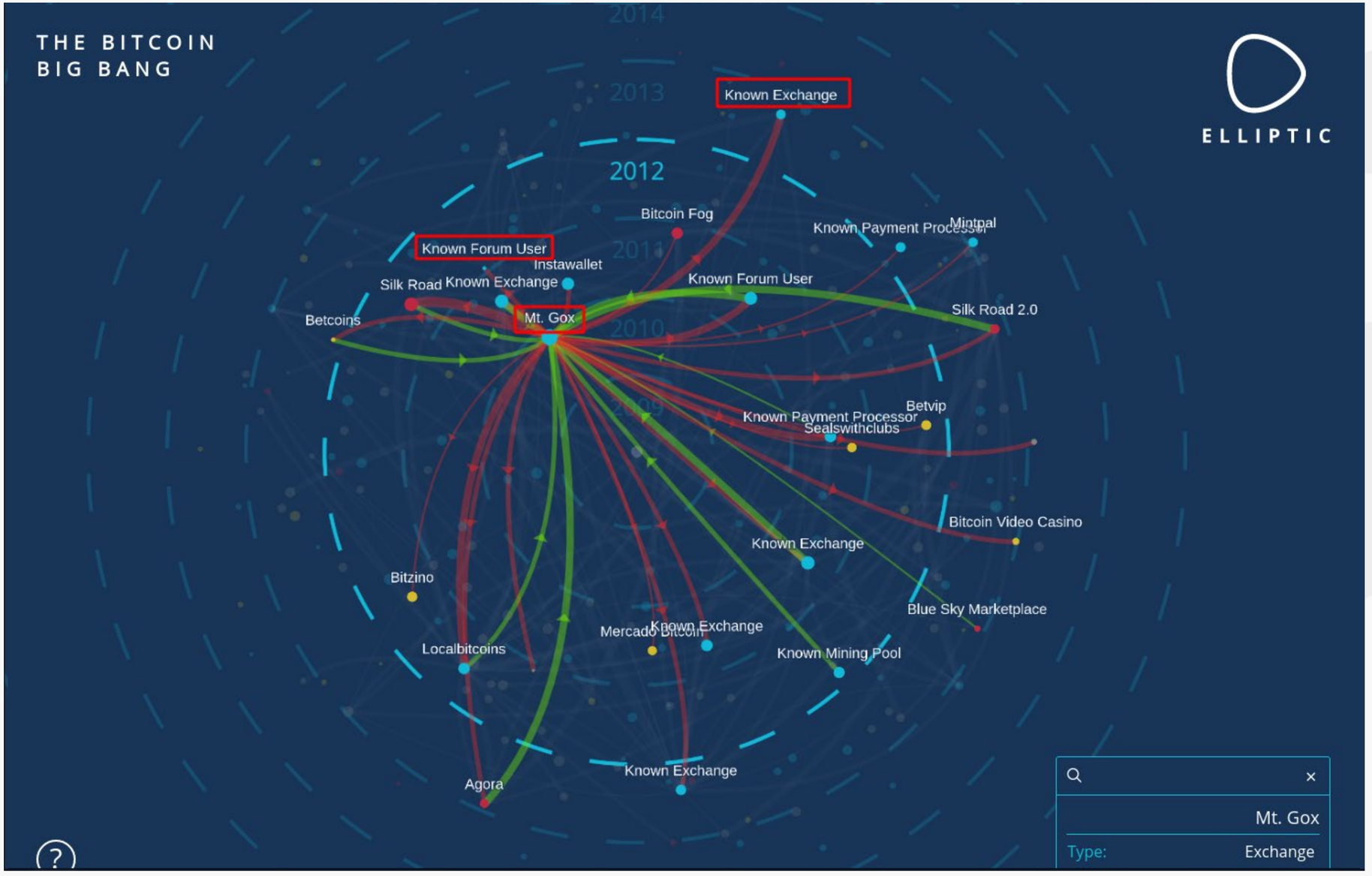
Filter

5c31b8005f4263cb371b9b3250444575cb2d286c18333d7f335bbac77dc0aeae			2019-09-22 10:04:04
3EeRQ21sLzAJAkX1nCjzfs5ZPwdovWLmeW	→	Silkroad Seized Coins	0.00324 BTC
			0.00324 BTC
a94f2a3c5a71bd8c2149935c449e4fe56f261400bac206dd71aa392e623d2a9e			2019-09-21 23:18:38
35NSxM5eBU96ysziZDGZACM1qxydwc7ADb	→	Silkroad Seized Coins	0.00094372 BTC
			0.00094372 BTC
791d831de97efcea5ef00abb79f98b9c28ea6f603903d9522d78106c74892875			2019-09-20 22:59:15
3AtdQYRXP5jEtvRHqjumdV8dRDM99gcJfi	→	Silkroad Seized Coins	0.00003 BTC
			0.00003 BTC
ddeaa2a14dd1fbb7abf59b51875b606aa57e4aac2196e5bb2232a800da5b3366			2019-09-20 13:44:04
3ChvSqQzLjk2paqeXshpeqHCgu9EqQNdm2	→	Silkroad Seized Coins	0.00952986 BTC
			0.00952986 BTC

İşaretlenmiş Bitcoin



İşaretlenmiş Bitcoin



Dokunulmamış Bitcoin

+ Düşük değerli bitcoinlerin tam tersi bir durum.

+ Herhangi bir kötü işleme karışmadığından emin olunan bitcoinler.

+ İşlemlerin tüm geçmişi kayıtlı olduğu için bunu anlamak oldukça kolay .

Dokunulmamış Bitcoin

+ Kendi başına bir piyasa bile oluştu: bakir bitcoin piyasası.

+ Yeni üretilmiş bitcoinler satılmaya başlandı.

+ Bu bitcoinler direkt olarak madenciden alınmakta.

+ Bu bitcoinler, normal piyasa fiyatınının üstünde (%20 gibi) satılmakta.

+ Hiç bir kötü geçmişinini olmadığından emin olunabilir.

Dokunulmamış Bitcoin

Transaction View information about a bitcoin transaction

249807c0118b4edd51799f94be3f35d7318c12a9261fda08b30a195ab5e0be0d

No Inputs (Newly Generated Coins)	1MUz4VMYui5qY1mxUiG8BQ1Luv6tqkvaiL - (Unspent)	12.97508812 BTC
	Unable to decode output address - (Unspent)	0 BTC
	Unable to decode output address - (Unspent)	0 BTC

10 Confirmations | 12.97508812 BTC

Summary	
Size	310 (bytes)
Weight	1132
Received Time	2019-09-23 18:55:06
Lock Time	1987-04-20 09:19:43
Reward From Block	596250
Scripts	Hide scripts & coinbase
Visualize	View Tree Chart

CoinBase

Bitcoin’de Fungibility

+ Bitcoinin "kimden" geldiği bilgisi (yani geçmişi),
bir bitcoini diğer bir bitcoinden değerli veya değersiz kılabilir.

+ Bitcoinin çalışması için gerekli olan 'kimden' bilgisi, fungibility sorununa sebep oluyor.

+ Hem işlemler arası ilişki sağlanmalı (merkezsiz bir şekilde)
ve hem de her bir koin diğeriyle eş değerli olmalı (fungible)

+ Hali hazırda bazı çözümler var; Coinjoin, mixin servisler gibi.

Miktar Bilgisi

+ Transferlerinin merkezsiz bir şekilde doğrulanabilmesi için işlemlerin miktar bilgisi de açıktır.

+ Yetkisiz olarak sıfırdan bitcoin üretilmediğinden emin olunabilir,
gönderenin bakiyeye sahip olup olmadığı merkezsiz bir şekilde kontrol edilebilir.

+ Bu bilgilerin açık olma durumu istenmeyen sonuçlara sebep olabilir.

+ Finansal gizliliğin yetersiz olmasının önemli güvenlik ve mahremiyet sonuçları olabilir.

+ Hırsızlar veya dolandırıcılar bilinen yüksek bakiyeli hesaplara saldırabilir.

+ Rakipler önemli ticari bilgileri elde edebilir.

Miktar Bilgisi

+ Kimin hangi adresi kullandığı bilinmiyorsa mahremiyette bir sıkıntı olmuyor.

+ Yeni bir transfer yapıldığında, o kişinin en azından bir adresini öğreniyorsunuz.

+ Diğer bağlantılı adresleri öğrenebilir, transfer işlemlerinin miktarını veya kişinin toplam varlığını öğrenebilirsiniz.

+ Örneğin Bitcoin ile maaş aldığınız bir senaryoda; bu bitcoin ile kira veya alışverişinizi öderseniz, hem ev sahibiniz hem de marketiniz ne kadar maaş aldığınızı öğrenebilir.

Bitcoin

+ Değindiğimiz özellikler; kimden, kime, ne kadar ve hangi varlık transfer edildi.

+ Bitcoin'in çalışması için açık olması gereken bilgiler.

+ Yalnız bunların açık olmasının da saydığımız gibi istenmeyen etkileri var.

Bitcoin

+ Bitcoin kullanımında bu gibi istenmeyen sonuçlarını engellemek için geliştirilen bir çözüm;

Liquid Network

Liquid Network

+ Liquid ağı borsalar, brokerlar ve piyasa yapıcılar için geliştirilmiş, yan-zincir tabanlı, borsalar arası bir blokzincirdir.

+ Hızlı ve gizli bir şekilde bitcoin transferleri gerçekleştirebilir,

+ Fiat paralar, herhangi bir kripto para veya emtia tokenize edilebilir.

Liquid Network

Başlıca özellikleri;

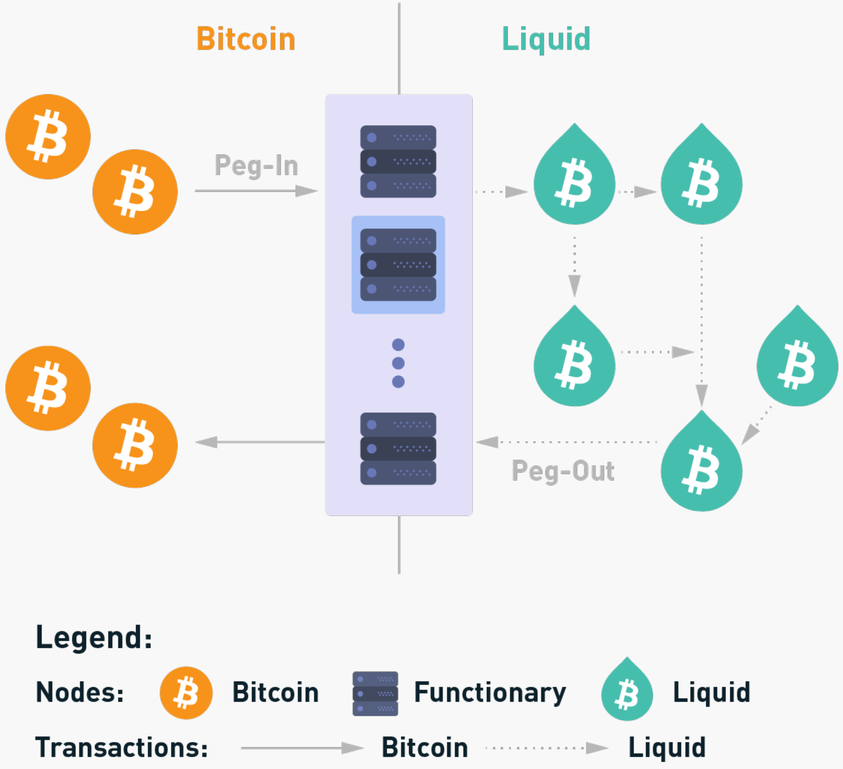
+ Yan zincir kullanımı sayesinde hızlı ve gizli transferler.
Her 1 dk'da yeni blok üretilmektedir.

+ Gerçek varlıkların tokenize edilmesi ve ağ üzerinden gönderilip alınabilmesi,
bunlara fiat paralar ve kripto paralar da dahil.

+ Tüm varlıklar Liquid ağı üzerinden transfer edilmekte,
bu sayede farklı entegrasyonlar veya birden çok blokzincir istemcileri gerekmemekte.

+ Açık kaynaklı Elements projesi ile geliştirilmiştir.

Liquid Network



+ Bitcoin için bir yan zincirdir

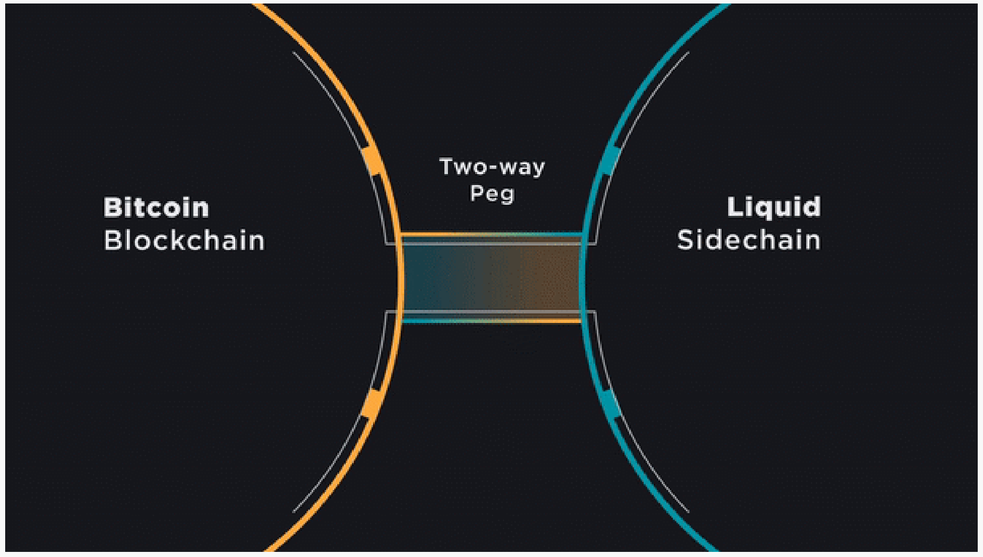
+ Kullanıcılar Liquid ağı ile Bitcoin ağı arasında iki yönlü olarak bitcoin taşıyabilmekte.

+ Liquid ağındaki bitcoinlere LBtc denilmekte.

+ Karşılığı olan bitcoinler Liquid ağının üyeleri tarafından tutulmakta.

+ Bu bitcoinler ağ üzerinden her an doğrulanabilir.

Liquid Network

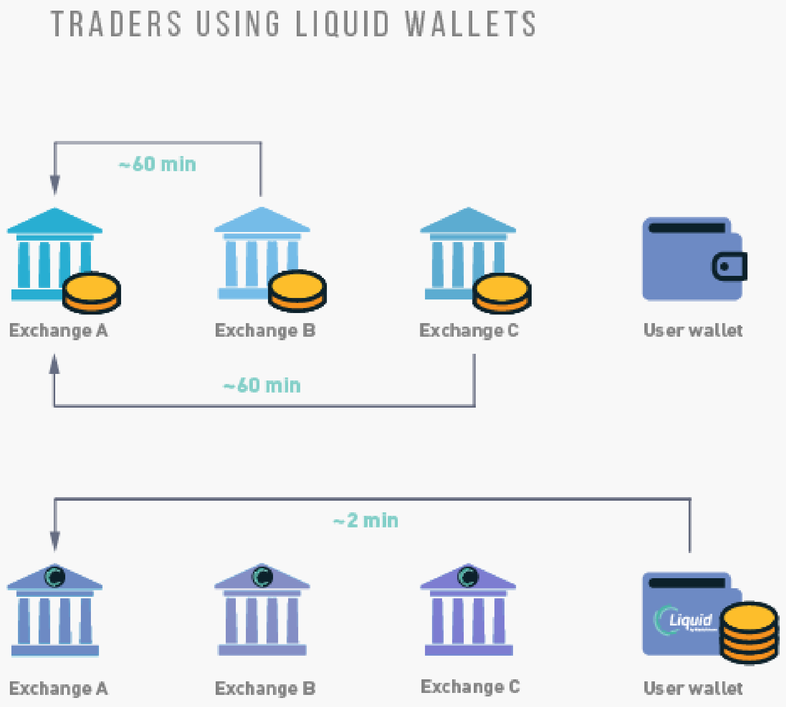


+ Bitcoin ağında, özel bir adrese gönderilen bitcoin'ler kilitlenir.

+ Bunun sonucunda aynı miktarda LBtc, Liquid ağında tanımlanmaktadır (Peg-In)

+ Herhangi bir anda tekrar Bitcoin ağına geri çekilebilir (Peg-Out)

Liquid Network



+ Liquid ağı bir grup borsa ve finansal kuruluş tarafından yönetilmektedir.

+ Üyelerin herbiri aynı zamanda ağın bir düğümüdür.

+ Normalde ~60 dakika süren borsalar arası bir bitcoin transferi, Liquid Network ile ~2 dk sürmekte.

+ Bireysel yatırımcılar isterlerse varlıklarını cüzdanlarına çekebilirler.

Liquid Network

Liquid Network üyeleri;

Altonomy, Bitbank, Bitfinex, Bitmax, BitMEX, Bitso, Blue Fire Capital, BTCBOX, **BTCTrader/BtcTurk**, BTSE, Cobo, Coinone, Coinut, Crypto Garage, DGroup, DMM Japan, FRNT Financial, Gate.io, GOPAX, Huobi, L2B Global, OKCoin, OpenNode, Poolin, Prycto, Sideshift AI, The Rock Trading, SIX Digital Exchange, TaoTao, Tilde, Unocoin, Xapo, XBTO, and Zaif.

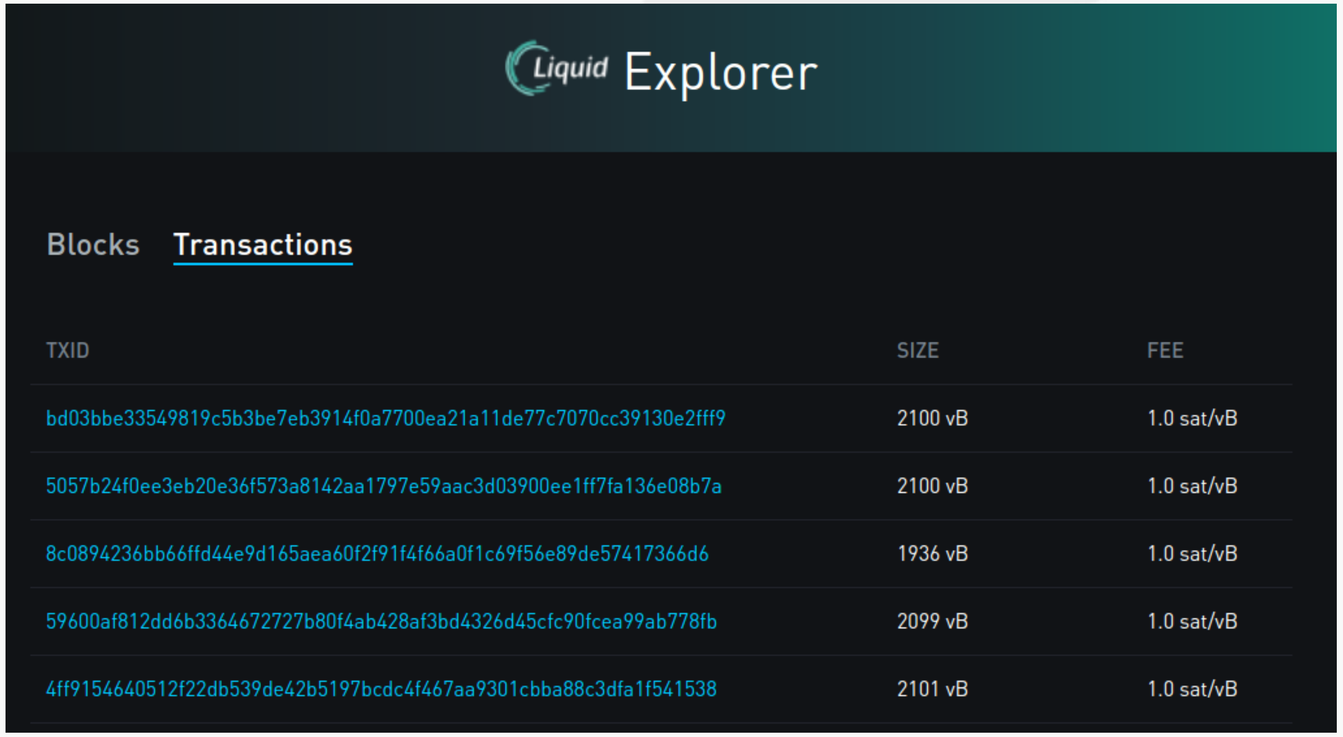
Türkiye’den tek üye BtcTurk'tür.

Gizli İşlemler

+ Liquid Ağının en temel kullanımı alanı "Gizli İşlemler" dir.

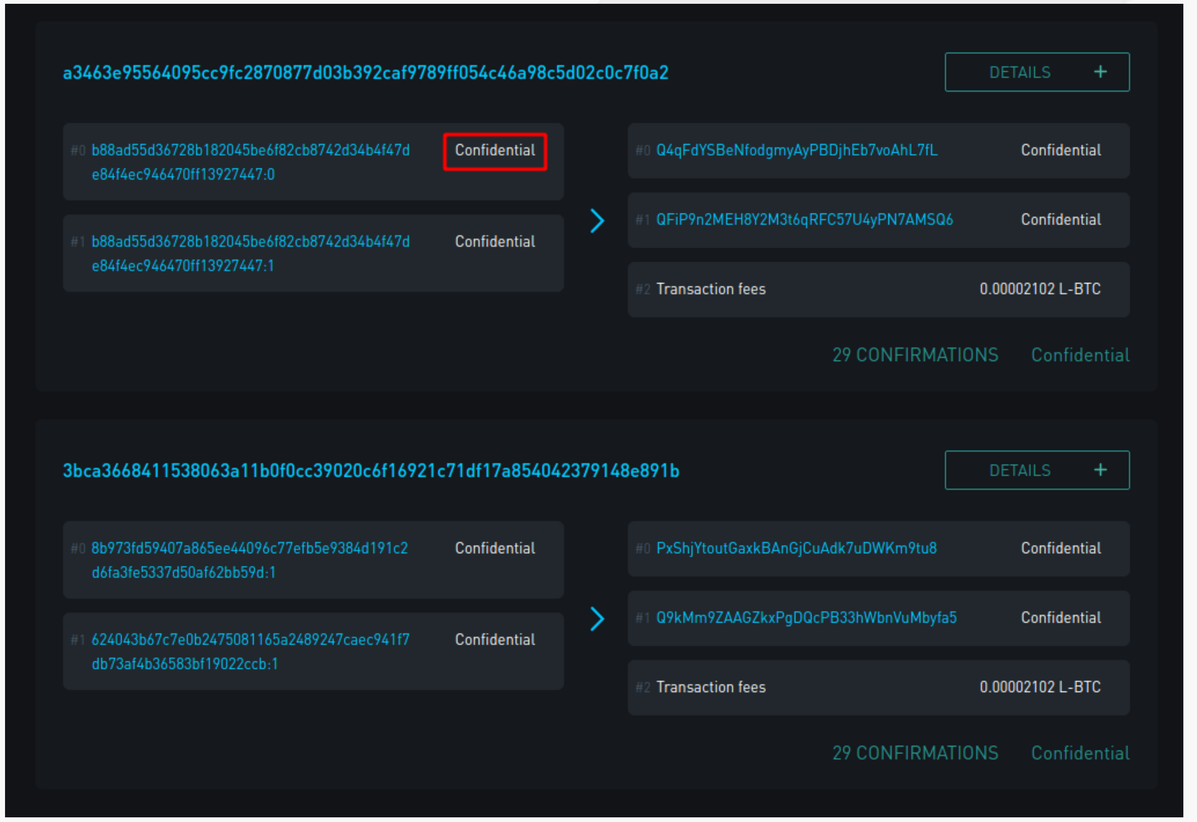
Liquid Network

+ Bitcoin ağında olduğu gibi,
Liquid ağında da transferler ağdaki herkes tarafından görüntülenebilmekte.



Liquid Network

+ Fakat Liquid ağındaki işlemlerde miktarlar ve varlık tipleri 3. partilerden gizlenmiştir.



Liquid Network

+ Bu bilgiler sadece transfer işlemine dahil olan taraflar ve yetki verilmiş kişiler tarafından görülebilir.

+ Buna rağmen harcanan koinlerin geçerliliği kriptografik olarak doğrulanabilir.

+ Liquid transferlerinde gizlenilmiş adresler kullanılır ve sadece alıcı gönderilen miktarı görebilir.

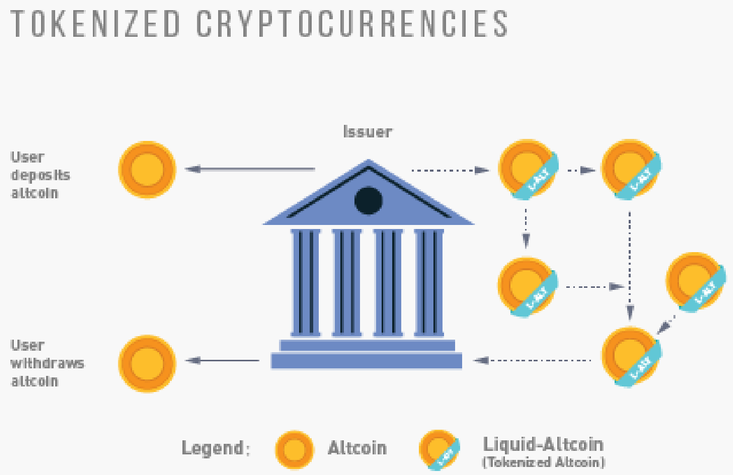
+ Alıcı sahip olduğu çözücü anahtarı 3. partiler ile paylaşarak işlem miktarlarının ve varlık tiplerinin görülmesini sağlayabilir.

Liquid Network

+ Liquid ağının temel özelliklerinden biri de kendi varlıklarınızı tanımlama olanığıdır.

+ Fiat paralar veya bitcoin harici kripto paralar tokenize edilebilir.

+ Kupon, mevduat, tahvil ve hisse senedi gibi varlıkların temsil edilebilir.



Liquid Network

+ Tüm bu yeni oluşturulacak varlıklar varsayılan olarak gizli işlemler özelliğini barındırmakta.

+ Hem miktar bilgisi hem de gönderilen varlık türü gizlenmiştir.

+ İstenirse "çözücü anahtar" 3. parti ile paylaşabilir ve transferin detaylarını açık edebilir.

Liquid Network

+ Bitcoin'i, sabit kripto paraları veya diğer varlıkları tek bir blokzincirde tanımlamak hem farklı farklı blokzincirler ile gereken entegrasyon zorluklarını eliyor,

+ Hem de yatırımcıların tüm varlıklarını bir cüzdan uygulamasından yönetebilmesini sağlıyor.

Bitcoin'de Mahremiyet

Faruk Terzioğlu

26.09.2019