BİTPARALAR VE BLOKZİNCİRİ

CMPE 444

CEMİL ŞİNASİ TÜRÜN
@JETWELL (TWITTER)
MEDIUM.COM/@CEMILTURUN

BLOKZİNCİRİ-101: BITCOIN MAKALESİ

HERŞEY 2009'DA BU MAKALE İLE BAŞLADI

Bitcoin: A Peer-to-Peer Electronic Cash System

Satoshi Nakamoto
satoshin@gmx.com
www.bitcoin.org

Abstract. A purely peer-to-peer version of electronic cash would allow online payments to be sent directly from one party to another without going through a financial institution. Digital signatures provide part of the solution, but the main benefits are lost if a trusted third party is still required to prevent double-spending. We propose a solution to the double-spending problem using a peer-to-peer network. The network timestamps transactions by hashing them into an ongoing chain of hash-based proof-of-work, forming a record that cannot be changed without redoing the proof-of-work. The longest chain not only serves as proof of the sequence of events witnessed, but proof that it came from the largest pool of CPU power. As long as a majority of CPU power is controlled by nodes that are not cooperating to attack the network, they'll generate the longest chain and outpace attackers. The network itself requires minimal structure. Messages are broadcast on a best effort basis, and nodes can leave and rejoin the network at will, accepting the longest proof-of-work chain as proof of what happened while they were gone.

1. Introduction

Commerce on the Internet has come to rely almost exclusively on financial institutions serving as trusted third parties to process electronic payments. While the system works well enough for

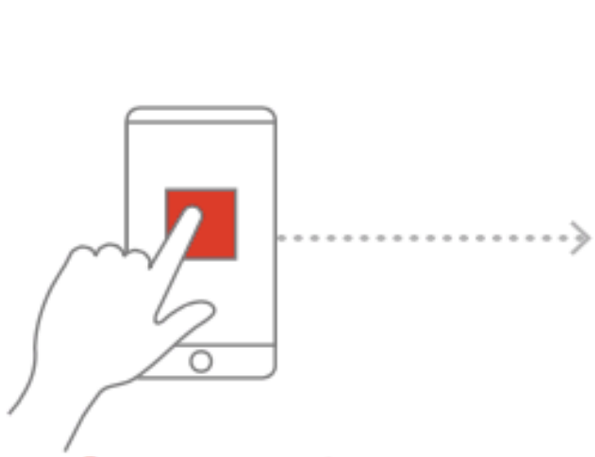
BITCOIN VE BLOKZİNCİRİ

BU İKİ KAVRAM NASIL İLİŞKİLİ?

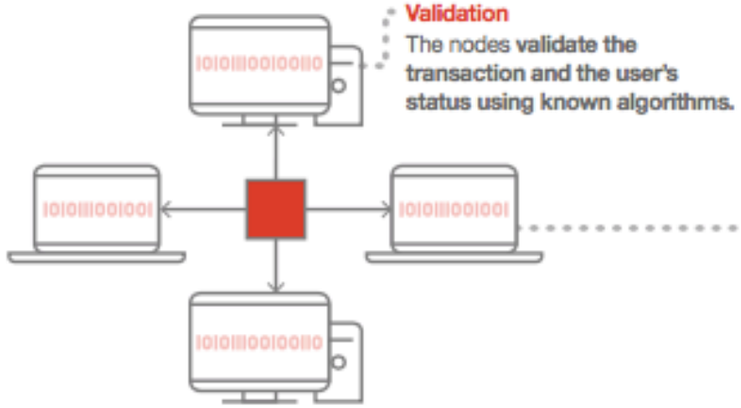
- Blockchain kelimesi makalede yer almıyor
- Bit-torrent ile gelişen peer-2-peer veri yollama nosyonu
- Public Key Cryptography
- Digicash, eCash gibi sistemler,
- Akıllı kontratlar
- P2P para yollama!

BLOKZİNCİRİ MEKANİZMASI

ALTI ADIMDA BİR DÖNGÜ



Someone requests a transaction.

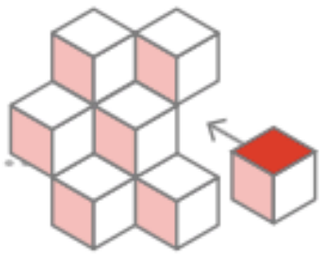


Validation
The nodes **validate the transaction and the user's status using known algorithms.**

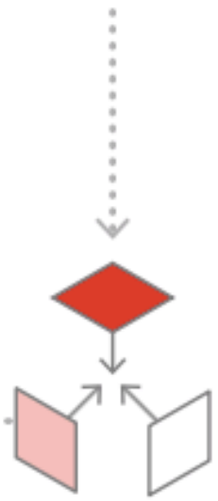
The requested transaction is broadcast to a peer-to-peer **network consisting of nodes.**

A verified transaction can involve cryptocurrency and other **digital tokens,** records, or other information.

The transaction is complete.



The new block is then added to the existing blockchain, in a way that is permanent and unalterable.



Once verified, the transaction is combined with other transactions **to create a new block of data for the ledger.**

INTERNET İLE BLOKZİNCİRİ İLGİSİ

BU RESİM TCP/IP PROTOKOLÜ HAKKINDA

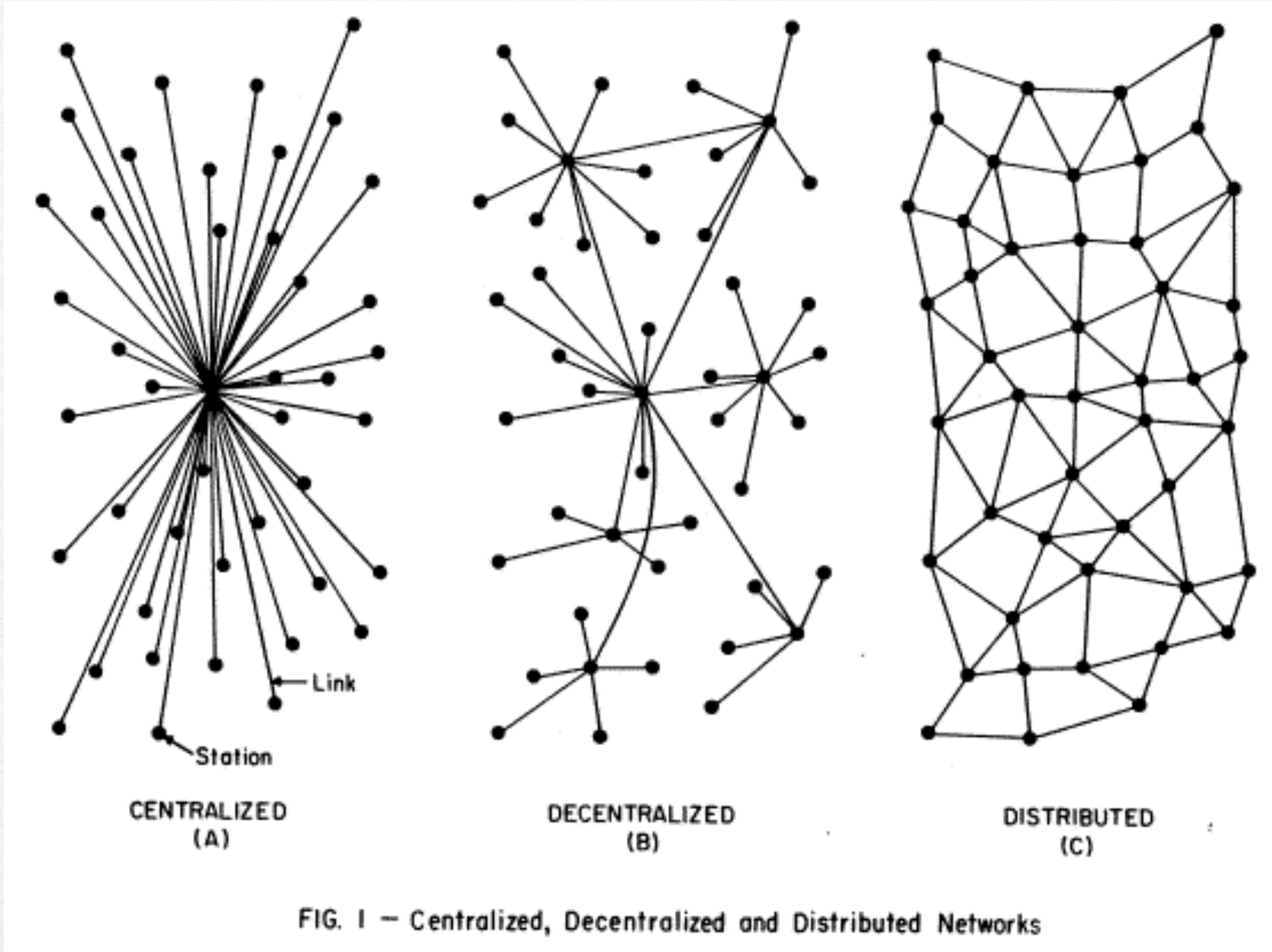


FIG. 1 — Centralized, Decentralized and Distributed Networks

DAĞITIK MUHASEBE DEFTERİ

BLOKZİNCİRİ = ZİNCİRLİ DEFTER-İ KEBİR

Transaction View information about a bitcoin transaction

f436745d70a137796b039decddfa55368b58812ba709699546bcd46cfeaf4154

14AXCDavT8Puvth6qzdXhBTgATCbRCdaEt	→	19LFZUL9MNz6w924Qq87WLx9myKZfYEXKS	0.02964208 BTC
		1H9ioDEd1Vop9HbDGFCgpynmVKmJAVWb6x	0.0198 BTC
			0.04944208 BTC

Summary	
Size	224 (bytes)
Weight	896
Received Time	2017-04-10 09:57:49
Lock Time	Block: 461249
Included In Blocks	461251 (2017-04-10 10:18:09 + 20 minutes)
Confirmations	79812
Visualize	View Tree Chart

Inputs and Outputs	
Total Input	0.04948728 BTC
Total Output	0.04944208 BTC
Fees	0.0000452 BTC
Fee per byte	20.179 sat/B
Fee per weight unit	5.045 sat/WU
Estimated BTC Transacted	0.0198 BTC
Scripts	Show scripts & coinbase

TEMEL KAVRAMLAR

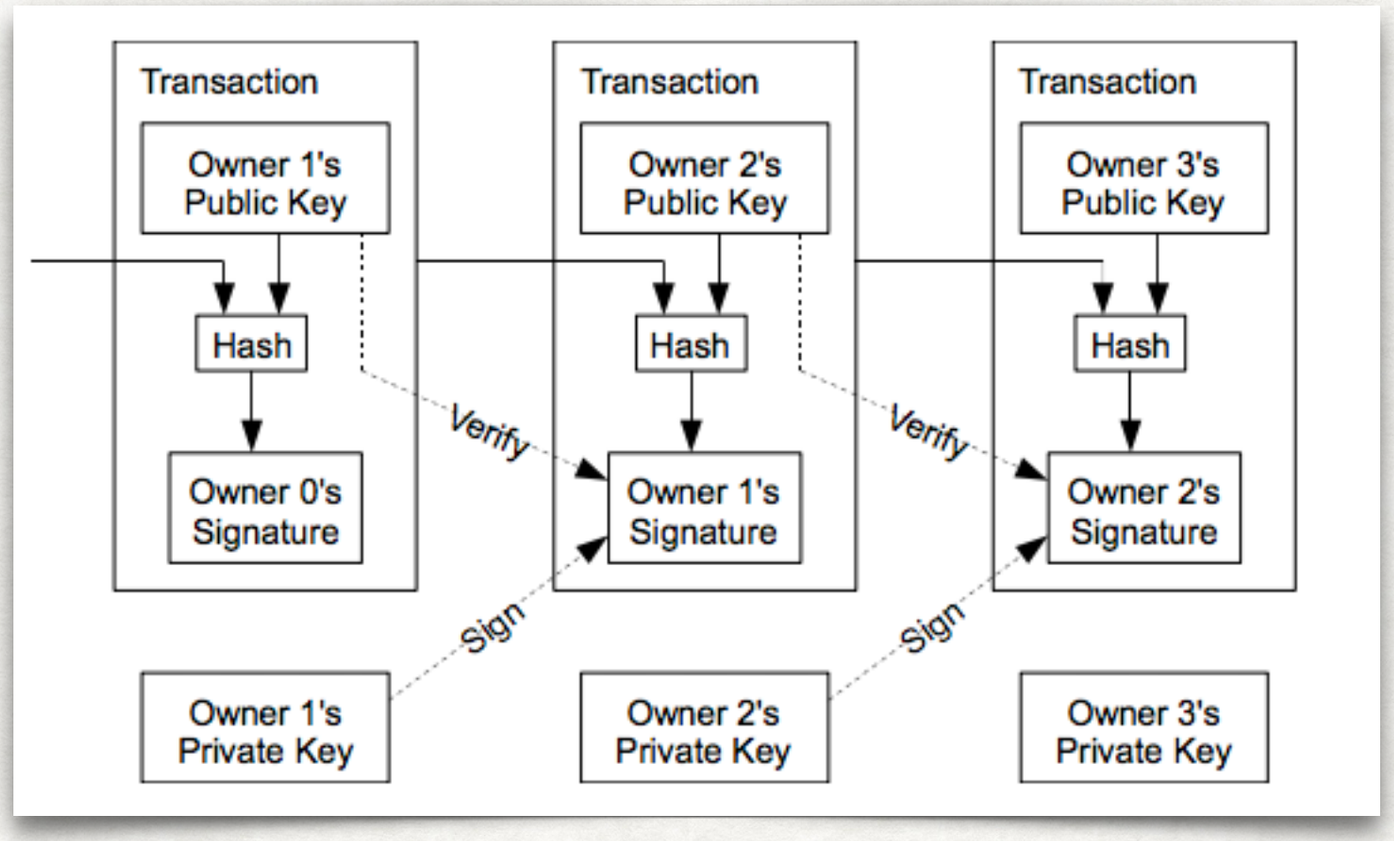
SIRAYLA İNCELEYELİM

- Private ve Public Blockchain (Özel ve Kamusal Blokzinciri)
- Platform ne Protokol ne? Ethereum bir platform mu?
- Akçe (Currency) Emtia (Commodity) ve Menkul Kıymet (Security) farkı
- DLT nedir? (Distributed Ledger Technology)
- Proof of Work / Proof of Stake
- Adres / Hash / Node
- Stable Currency: Sabitlenmiş Akçe

VADELİ ÇEKLER

YİNE AYNI MAKALEDEN BİR RESİM

- Satoshi makalesindeki ilk figür.



VADELİ ÇEKLER

BİZİM YERLİ BLOCKCHAIN'İMİZ!

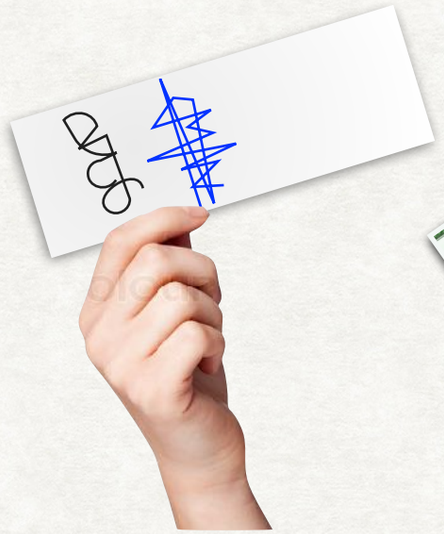
10,000 TL

20,000 TL

30,000 TL

40,000 TL

Bankadan görünen işlem: 10,000 TL



1

2

3

4

5

Ali

Bora

Ceren

Demir

1

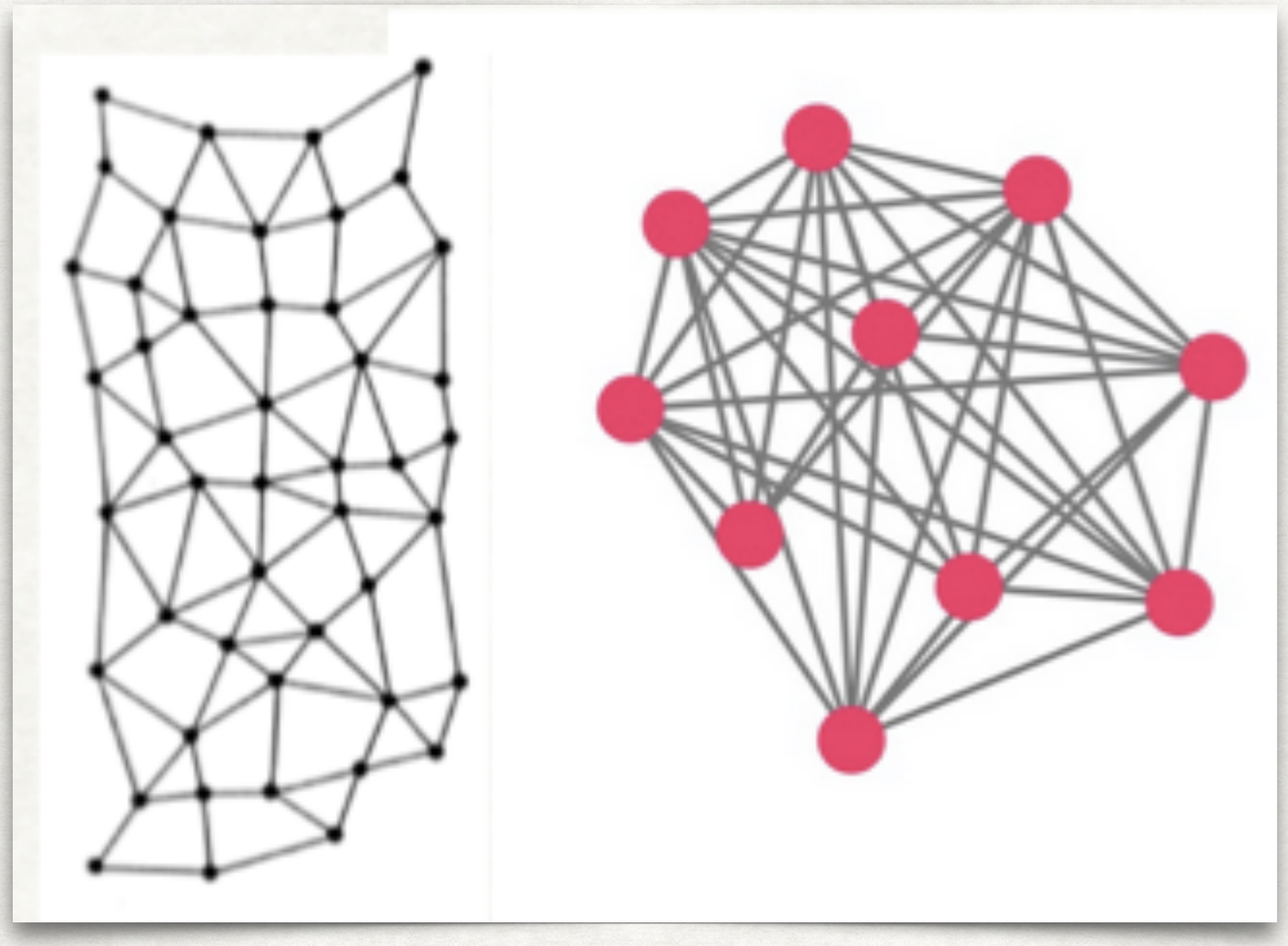
2

3

4

BITCOIN'DE YOLUN SONU!

EMTİA VE KREDİ FARKI



SİHİRLİ BLOKZİNCİRİ VADELİ ÇEK

VADELİ ÇEKLERİN BAZI ÖZELLİKLERİ

- Her VÇ bir hizmet ya da mal karşılığı üretilen bir tür vatandaş kredisi. Vatandaşın para basması yani…
- Her VÇ'nin bir de alıcısı var. Alıcı olmadan kredi yaratımı olmuyor. Kredi yaratımı tamamen kişiler arasında yapılan SÖZLÜ/YAZILI AKİTLERE dayalı.
- Eğer sözü veren kişi, sözünü tutmayıp (ya da tutamayıp) çekini vadesinde ödemezse cemiyet içinde kredisini yitiriyor. Ancak blockchain'e yazılan VÇ'lerde sözünü tutma garantisi geliyor zira blockchain kişileri ya da firmaları asla unutmuyor.
- Elden ele geçen çeklerle çarpan etkisi oluyor ve işlem hacmi büyüyor.
- Tamamen gayri-merkezi bir kredi yaratımı söz konusu. Banka arada bir yerde yok. Bu da blockchain'in asıl iş modeli olmaya aday.

PARANIN İCADI?

SÜMERLERDE VADELİ SENET (MÖ 2500)

ASUR BORÇ SENEDİ M.Ö. 1800

LİDYA ALTINI

KARUN VE LİDYA'NIN ALTIN ASLANI

- Bitcoin Lidya'nın altın parası gibi, çok önemli bir icattı.Bugün adını hep duyduğumuz Eski Yunan uygarlığı şehir devletler arası ticaretle gelişti.

- Ancak yeterli değildi! Muhasebe kavramı, yani **borç ve alacak** ve de asıl ***kredi*** olmadan şehir insanlarının üretimi mümkün değildi. Zira, eğer baban zengin değilse cebinde altın olması mümkün değildi.

- **Karun'a babasından Menderes nehri ve altınları kalmıştı.**

BITCOIN = DİJİTAL ALTIN

- Teknoloji olarak blockchain çok büyük potansiyel vadediyor.
- Ancak, Bitcoin'de de tarihteki parada olduğu gibi bir Ver 2.0 ihtiyacı var. Gündelik iş hayatı ile bitcoin birleşip, kredili kripto para çıkmalı.
- Şu anda dünyada kredili bir kripto para yok. Ancak iş hayatının ve ticaretin kredi (borç-alacak) ilişkisi olmadan yürütülmesi mümkün değil.

PARA VE ÖDEME SİSTEMİ FARKLARI

BITCOIN TABLONUN NERESİNDE?

Type	Sample	Present Value	Currency?	Fatura?	Kim Bakıyor	Kanun
Money / Credit	• 100 TL nakit, • 100 liralık vadeli çek veya senet • Credit card	• 100 TL (!) • Vadeye/kimin imzaladığına bağlı • 100 TL credit	YES YES (only in Turkey YES	NO YES/NO depends!! YES	• TCMB • GümrükBak. • BDDK	Bankalar Borçlar, Kambiyo Kanunları
Points (Non-Bank)	Money, Hopi, Paro, BP Puan	Depends on the issuer	YES (one time only)	YES	GİB, Maliye	TTK
Points (Bank)	Bonus, Axess, Vada, Maxipuan	Depends on the issuing bank	YES (multi-ple stores)	NO	BDDK	Bankalar
Electronic Money	İninal, Pasolig, Western Union	1 unit = 1 TL	YES	NO	TCMB, BDDK	EPK
Security-Type 1	Hisse senedi, Tapu,	Floating acc to market	NO	NO	SPK	
Security-Type 2	Bitcoin, Ether, Litecoin, Augur	Floating acc to market	NO	NO	??	??
Commodity	Gold, Silver, PT	Floating acc to market	NO (used in the past)	YES but	SPK	
Payment System	**İyzico, PayU, PayPal, 3Pay, Ödeal**	No value, just transfer of funds	**NO**	Only for the service	TCMB	Banka ve EPK

ICO/SECURITY TOKEN SALE

BİR TÜR KİTLE FONLAMASI

- ICO, crypto-paranın baştan halka arzı anlamına geliyor.
- Şirketlerin halka açılması anlamına gelen IPO yerine 2016 yılının başından bu yana yeni bir kavram var: ICO, ya da daha yeni tabiriyle “Security Token Sale”.
- Token sale ile iş modelini taşıyacak bir token icat edip, sonra bunu halka baştan satarak yatırım topluyorsun.
- Biraz Kickctarter’dan projelere finansman almaya benziyor.
- Türkiye’de de bu iş için hazırlıklar yapılıyor.

AKILLI KONTRATLAR

GÜNDELİK HAYATIMIZDAN ÖRNEKLER

1. Kar zarar hesabına göre vergi diliminde nereye girecek?
2. “if then else” içeren her türlü kontrat,
3. Ev sahipleri ve kiracılar arasında yapılan kontratlar,
4. Genel kurullardaki oylamalar,
5. Tapu değiş tokuşu,
6. Çek takası
7. Bilet satın alınan durumlar (uçak, sinema, vb)
8. Noterde yapılan tüm işlemler,
9. Şirket sözleşmeleri
10. İçerik satın alma işlemleri (şarkı, oyun vb)
11. Sigortacılık uygulamaları,
12. Sadakat puanları üzerine akıllı sözleşme yazılması,