

CMPE 444

10 dk

12.5 tane

- BITCOIN ?

1 → currency

2 → emtia (commodity)

↳ altın/gümüş/petrol

3 → menkul kıymet (security)

ASSET (VARLIK)

BLOCKCHAIN : teknoloji

VADELİ ÇEK

↓ TÜRKİYE'DE YASAL
DÜNYADA YOK.

ONUR KILIÇ
SAIT İMAMOĞLU

21.09.18

@Jetwell

medium.com/@cevilturun

cemil.turun@gmail.com

blockchain
blok zinciri

PUBLIC KEY CRYPTOLOGY
(Komusal (cumumi))

PRIVATE
(Hususi)

OBJECT = CONTRACT

Peer-to-peer = estene se

TCP / IP / HTTP / SMTP / IMAP / FTP

→ Blockchain bir protokoldür.

MØ = kağıt ve metal paraların
topluluğu

→ Blockchain aslında bir database, herhangi bir durum için yokbasık dosya kopyası var.

gayrimerkul
tasnifmaya →

* ~~Bitcoin (teknoloji)~~ → Blockchain
Bitcoin (para birimi)

* 2004'ten beri şirket hisseleri koatta tutulmaya.
(Oracle) digital obrak saklıyor.

(MKK) → hisse senedi kayıtlarını tutuyor.
↳ Borsaya bağlı. (Borsa İstanbul)

(banka ismi) yatırımı → hisse senedi alıp satıyor.
"SEC" = "SPK"
↳ Türkiye (Elon Musk'a dava açıyor.)

* ~~Ethereum'ün~~ içinde başka asset (varlık) var.

Ethereum

- PLATFORM
- Solidity
- Smart Contract

$$\text{cap} = \text{ca}$$

circulating supply

$$\text{Market cap} = \text{Price} \times \text{CS}$$

Takasbonk: (hisse değişim-taksisi) + MKK = $\frac{\text{BÖRSA}}{\text{IST}}$

* Circulating Supply (total üretilen miktar)

Tüm transferler gözüküyor.

price → arz ve talep ettiyor.

IPO → halka arz (hisselerin halka açılması)

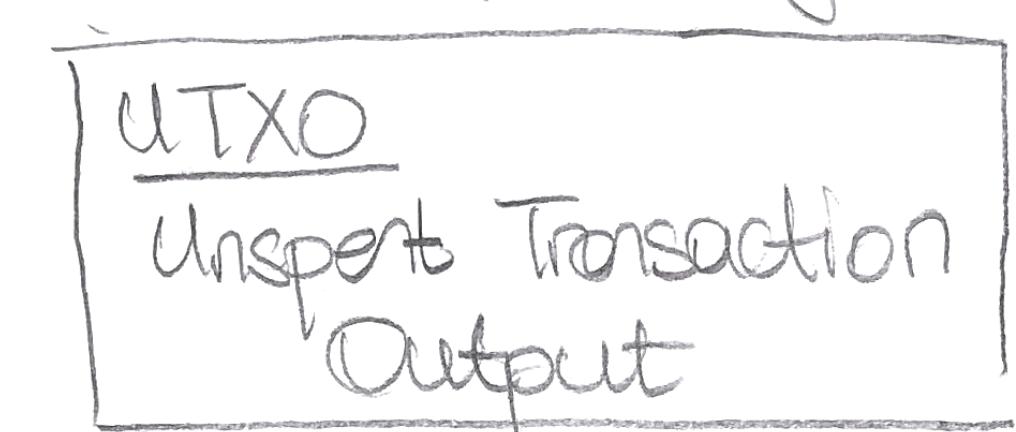
ICO → (Initial COIN offering)

- Hash
- One way function can not be reversed.
- Deterministic same input produces same output
- Hiding, No correlation output does not reveal inf. on input
- Hard to find collusion difficult to find two diff. messages
- Fixed size output

PoW (Proof of Work)

memory pool
miner

conses (mitobik)
transaction



→ Proof of Work mekanizmasına bak!
(Sınırda sorumluluk.)

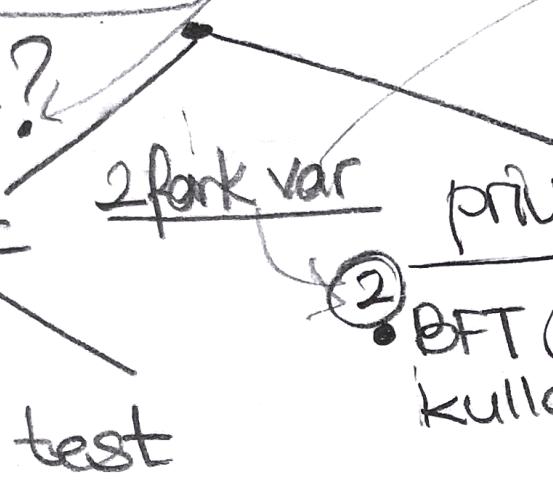
smart contract

- POW → fork?
- PoS ← public
- enerjiye gerek yok.
- main

production

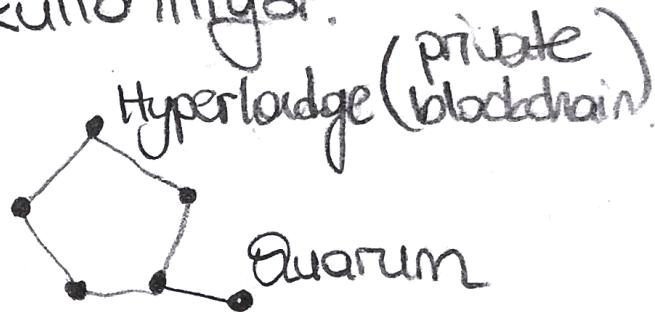
- Bitcoin
- Ethereum
- Neo
- Zcash

public blockchain
örmekleri



private

- ② BFT (Byzantine Fault Tolerans)
kullanıyor.



Bitcoin + Turing Completeness = Ethereum

ABI

contractların metotlarını
görmek için kullanıyor.

btc-like

- size:
- sizeonly:

eth-like

- size:
- Storage (size)
- computational cycle

sorulabilir

PKCS #11, ERC20 → token

[TOKENIZATION]

- ① Utility Token
- ② Commodity Token
- ③ Security Token

Kurumlu
Kurumlu
(SPK Dayı)

P.K.C

ICO / IPO

Initial Coin
Offering

I. Token Sale

Security Token Sale
(STS)

Peer-to-peer
P2P

Initial Public
Offering (SEC)
(SPK)

2UG

[Crypto Asset]

- 1) Currency
- 2) Commodity
- 3) Security

STABLE
COIN

1 TL = 1 TBL

Quiz 1
POPULOUS

- ① How many tokens issued
- ② Founder tokens
- ③ Price in the beginning

Banka
sistemi

TCP/IP PROTOKOLÜ

DECENTRALIZED
DISTRIBUTED

gecis

sebep
soruk
sorus

- Tümlen

kaupbedilmesin

- Ayni ayri islem yapilmasin

CMPE 444

26.10.18

Friday

① V.G ≈ B.G

② Toplumsal

③ B.C: commodity emtia

→ *kredi olmadiği

SOVEREIGN FUND (~~Egenlik Fonu~~)

- Ülkenin kendihe ait doğal kaynakları dması
gerek. (Gaz) Petrol

Narvee (zengin)

Türkmenistan (fakir)

Know Your Customer

KYC/AML

* BLOCKCHAIN = PUBLIC, (Kamusal)

Aynı miktar gaz
Aynı miktar önfus
Sebeep lider

CALTUR

Protokol = set of rules.

Her protokol bir platform fakat her platform bir protokol değildir.

* DLT ⇒ "private blockchain"
(Distributed Ledger Technology)

FED: ABD Merkez Bankası

CONSENSUS = Mutabakat

Gelişkotul etme
durumu. Anlaşma
Güvenlik

Security: Emniyet

Trust: Güven

TÜRKİYE'NİN
SİSTEMİ

VADELİ ÇEK

MİTİFERİT SORUSU

CMPE 444 10 dk ONUR KILIÇ 21.09.18
- BITCOIN 12.5 tane SAIT İMAMOĞLU @Jetwell
1 → currency blockchain medium.com/@ceviltur
2 → em Blockchain ceviltur@mail.com
3 → me

CMPE 444

②

26.10.18

Bitcoin → security var.

Trustless system (KREDİ YOK)

- Bankaya güvenmipr. (Public debt)
 - Vadeli çek muhabbetini bilmiyorlar.
(Vatandaş mekonizması)
devlete bağlı değil
- Sumer Vadeli Senet
Asur Borsa Senedi
- By select bitcoin yapmak gerek.
Vadeli çek sisteminin başlıcaudur.

keypair

Pub

Priv

From :

to

amount(value): +

MEW send(token)

SignedTx.

[JSON]

eth vanity

optional
geth kurulumu
[go ether]

geth account new

get attach

eth sendTransaction/sendRawTransaction(→)

rinkeby.etherscan.io

CMPE 644

Truffle Odəvi

ERC20 →

Vault (kasa) yazılım.

① transfer
 ② constructor
 owner = msg.sender

Rinkeby

MetaMask key.json

Remix Browser IDE

Ethercan()

- Contrata, ulasmak igin gereklili iki ozellit.

Address
 ABL (arayik)

- 1.) Protokol
 2.) Government
 3.) Decentralization →
 4.) Scaling ?

Architecture / Political / Logical
 decentral de-oc central
 implement SIVAN SORUSU

* Neden gesitli implement kullaniyoruz.

↳ Tek dile yasayik katoldur
 geldiginde bitcoin olur.

Layer 1: protokol
 Layer 2 protokolle
 aalison
 yugulma

Stake Channel

- lightning network
- plasma
- raiden

↳ tek satırda
 bir sürü yazın işlendiyor