BLOCKCHAIN TECHNOLOGIES

Student(s)

Ekin Oskay Görkem Kir
Umut Barut Orhun Barış

Faculty Member(s)

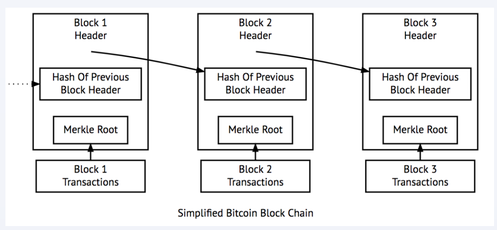
Kamer Kaya

Sabancı Üniversitesi

PURE
PROGRAM FOR UNDERGRADUATE RESEARCH

What is Blockchain ?

A **blockchain** is a distributed ledger that basically holds a list of records in semi-ordered manner. A copy of this list exists at every computer within the Blockchain network. In this project, we are interested in the technical details and use cases of this new technology.



Simplified Bitcoin Block Chain

Blockchain could be public or private, it depends on the cryptocurrency, but in Bitcoin, the blockchain is public.

In blockchain, every block has many transactions which contain key information like amount, sender, receiver (in our bitcoin case).

Every block has a header which holds “Merkle Root” and “Hash of previous block header” and every block has a list of transactions within its body.

In header, hash of previous header is there for making sure that block is not altered. When someone changes the previous block, its hash value changes which affects all the chain and makes the malicious activity visible to anyone.

Merkle root is a sort of signature of transactions witin that block’s body part.

Here, when someone changes a transaction it would change specific hashes and it will result in a different Merkle root and which makes blockchain unconsistent

Hash of the previous block, merkle root and nonce must be smaller than the target.

```
H(prevBlockHash || merkleRoot || nonce) < target
```

Computers are continually tries to guess this value. They try random values at hash them together and check if it satisfies the condition, if not they try it again until target is reached.

MINING PROCESS

Miners are people that are trying to find a “Nonce” that satisfies that given target. It could be assumed as throwing darts blindfolded. While you are blindfolded, throwing to any place is equally likely but if you throw faster, you can hit the target faster. In Bitcoin, if you have superior hardware, you have the advantage in this challenge. Miners are earning bitcoin by verifying the blocks

Blok #533088

özet	
İşlem Sayısı	2027
Çıktı Toplam	11,680.15888807 BTC
Tahmini İşlem Hacmi	1,283.87134135 BTC
İşlem ücretleri	0.16554144 BTC
Yükseklik	533088 (Ana Zincir)
Zaman Damgası	2018-07-22 11:38:03
Alınan Saat	2018-07-22 11:38:03
Tarafından Geçiş Yapan	BTC.com
zorluk	5,178,671,069,072.25
Uçları	389437975
Boyut	987.821 kB
Ağırlık	3417.626 kWU
versiyon	0x20000000
şimdiki zaman	897708578
Blok Ödülü	12.5 BTC

Hash'ler	
esrar	00000000000000000018f870394297a99837d75ff0a275d4e6bb61985b4797fb
Önceki Blok	00000000000000000013bc3e7abaea85bf8b5050f917b32ef1889664af21641f
Sonraki Blok (lar)	00000000000000000002951d3e7c55d648db084a352ece44c74e99a675d4cabd0
Merkle Kök	22db4c24856fe432a1d4fb845b17c1ce1a9690bff843a850aa6510e4ae539dfa

Puregold

Puregold is a cryptocurrency idea that was designed by team and supervisor in order to research the common uses of blockchain and cryptocurrencies and implement a version for in-campus usage.

Puregold rewards a discount for in-campus purchases with respect to currently stored puregold count in users account. This idea was designed to raise awareness about blockchain in general.

- As diagram states, puregold idea aims to bring a in-campus usage for blockchain within cryptocurrencies. Puregold is being generated by school and distributed via work salary/direct purchase. After discount benefit is used. Puregold is collected by service providers in campus and then exchanged with money with school to complete the cycle.

What is Bitcoin?

Bitcoin is a kind of cryptocurrency which exists purely in the digital realm first time used in 2009. It born out of the Cypherpunk movement, a libertarian struggle for privacy and self-governance. Invention of blockchain inspired the creation of Bitcoin by Satoshi Nakamoto who an anonymous identity.

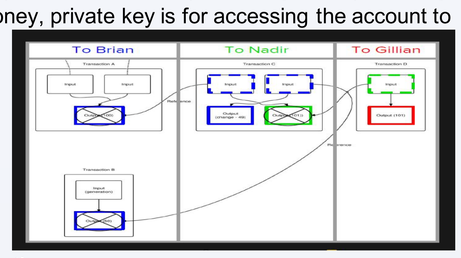
What does Bitcoin provide?

- Account and identity management: Every user has an address and each of them relevant with amounts of currency.
- Services: Users can do transactions between each other via other users.
- Record management: Redundant information is stored by other users which are on the system via a blockchain.
- Trust: Trust comes from personal encouragement aligning with community goals.

bitcoin
Be Your Own Bank

Identity

With identity, people can receive, claim, spend the Bitcoin. Identity provides a random private key, then public key is created corresponding private key. Public key is for receiving money, private key is for accessing the account to manage.



Transaction

Transaction is valid when three conditions are satisfied;
Proof of ownership: There must be a signature of ownership.
Available funds: Users must have enough amount of Bitcoin.
No double spending: Other transactions can’t use the same funds.

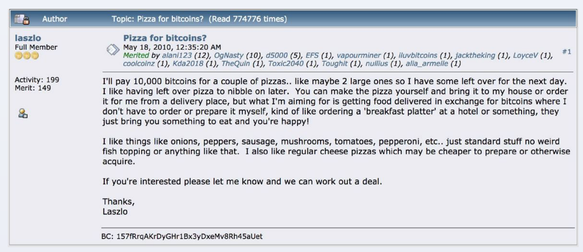
Record Keeping:The Blockchain

Transaction ledger is stored with distributed database, everyone on the system stores the ledger.

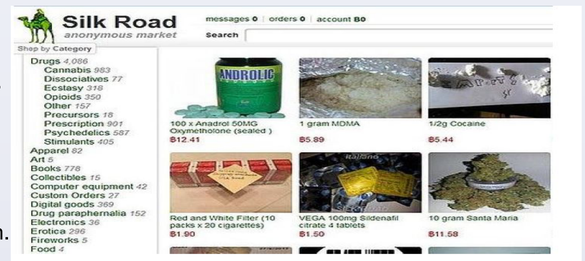
Consensus (Proof-of-Work)

To prevent double spending, every transaction must be validated by the other peers. Bitcoin has anonymous identity, so people can have multiple accounts to take opportunities of cast vote. That is why Bitcoin validation protocol uses resources instead of cast votes. Peers use their CPU power to vote. They have voting power as much as used power. (System assumes majority of the network is honest)

Some History of Bitcoin



- **$74 million = 2 Pizzas**
  Bitcoin is the most valuable cryptocurrency today. Before the Bitcoin gets valued, there was a trade which a guy bought two pizzas for 10,000 Bitcoin, today it’s value is ~$74 million.
- **Bitcoin Theft**
  Mt. Gox was the biggest online bitcoin exchange market. More than %70 of transactions were being occurred via Mt. Gox. In 2014, Mt. Gox lost 744,408 bitcoins in a theft, then Mt. Gox declared bankruptcy.
- **Bitcoin in Illegal Use**
  Due to Bitcoin anonymous protocol, it is used in the black market for illegal goods. Silk Road was one of them, it was sold goods for Bitcoin via Tor network. It was shut down by FBI with seizing $3.5m in Bitcoin.



What is Ethereum?

Ethereum

Ethereum is a decentralized platform that use smart contracts to run applications on a custom blockchain. This blockchain has powerful associated global connections that can share valuable items and contain ownership of possessions.

This features give opportunities to create markets, store given promises or record of charges, make action with funds based on instructions given in past and many different things that have not been think about yet.

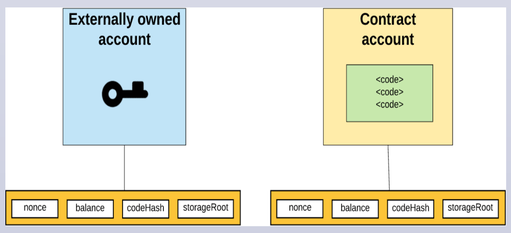
Vitalik Buterin is a developer from Toronto who is the creator of Ethereum. He focused on the blockchain, crypto technologies and Bitcoin in 2011. Then, he came up with an idea of a platform that gives the opportunity to develop other decentralized application beyond the financial usage with the smart contract.

Ethereum design based on the following 5 principles:

- **Simplicity**: Ethereum protocol should be as simple as possible to protect over data storage or time efficiency.
- **Universality**: Ethereum provides its own script language which developers can use to create contract or transaction type.
- **Modularity**: Ethereum created as possible as modular and separable.
- **Agility**: There is the opportunity to make the change on high-level constructs
- **Non-discrimination and Non-censorship:** Ethereum protocols should prevent to attempt any restriction and any discrimination which come from central authorities.

Accounts

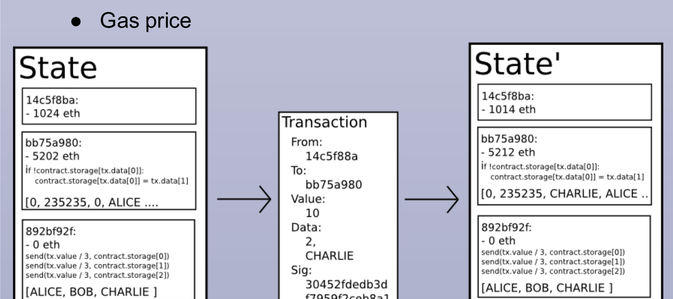
Accounts are objects that able to interact with each other. There are two types of account which are external owned account and contract account. External owned accounts can create signed transaction with its own private key then can send a message to any other external owned account or contract account. Ethereum accounts occurred by four states which are nonce, ether balance, hashed code and storage.



Transaction and Messages

Basically, transactions are data package that generated and singed by external owned accounts and includes message, then submitted to blockchain.
All transactions contain:

- Nonce : count of number of transactions sent by sender.
- The recipient of the message
- The address of the sender
- The amount of the ether to transfer
- Optional data field
- The maximum amount of the gas that sender will pay to execute transfer
- Gas price



Proof of Stake

Proof of Stake is the consensus protocols as an alternative to proof of work, to use consensus on which block will be the next in blockchain. Creator of next block selected by the randomized system according to how much cryptocurrency account have or how long account has been holding that particular currency rather than computational power as proof of work system.
Possible advantages of proof of stake against proof of work are that:

- It reduce to energy consumption while add the new block on blockchain.
- There is no need to create many new coins in order to encourage miner to continue mining process.
- Proof of stake more secure against %51 attack than the proof of work.

BIBLIOGRAPHY

https://www.g2crowd.com/categories/blockchain
https://medium.com/fluree/blockchain-for-2018-and-beyond-a-growing-list-of-blockchain-use-cases-37db7c19fb99
https://hackernoon.com/bitcoin-ethereum-blockchain-tokens-icos-why-should-anyone-care-890b868cec06 -resim2
https://www.youtube.com/watch?v=Lx9zgZCMqXE
https://www.youtube.com/watch?v=V6gLY-1G4Mc
Lecture 01 - Bitcoin Protocol and Consensus_ A High Level Overview- Blockchain at Berkeley.
Lecture 02 - Bitcoin to Blockchain History- Blockchain at Berkeley
Lecture 03 - Bitcoin Mechanics and Optimizations_ A Technical Overview- Blockchain at Berkeley. (3 ve 4. resimler)