ORTA DOĞU TEKNİK ÜNİVERSİTESİ
MIDDLE EAST TECHNICAL UNIVERSITY

BLOCKCHAIN 1.0

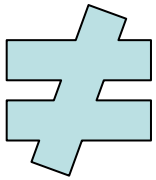
PELİN ANGIN
BİLGİSAYAR MÜHENDİSLİĞİ BÖLÜMÜ

07.03.2022

OUTLINE

- What is a blockchain?
- Brief history of Bitcoin/blockchain
- How does a blockchain work?
- Bitcoin and other cryptocurrencies
- Other blockchain projects
- Why/why not blockchain?

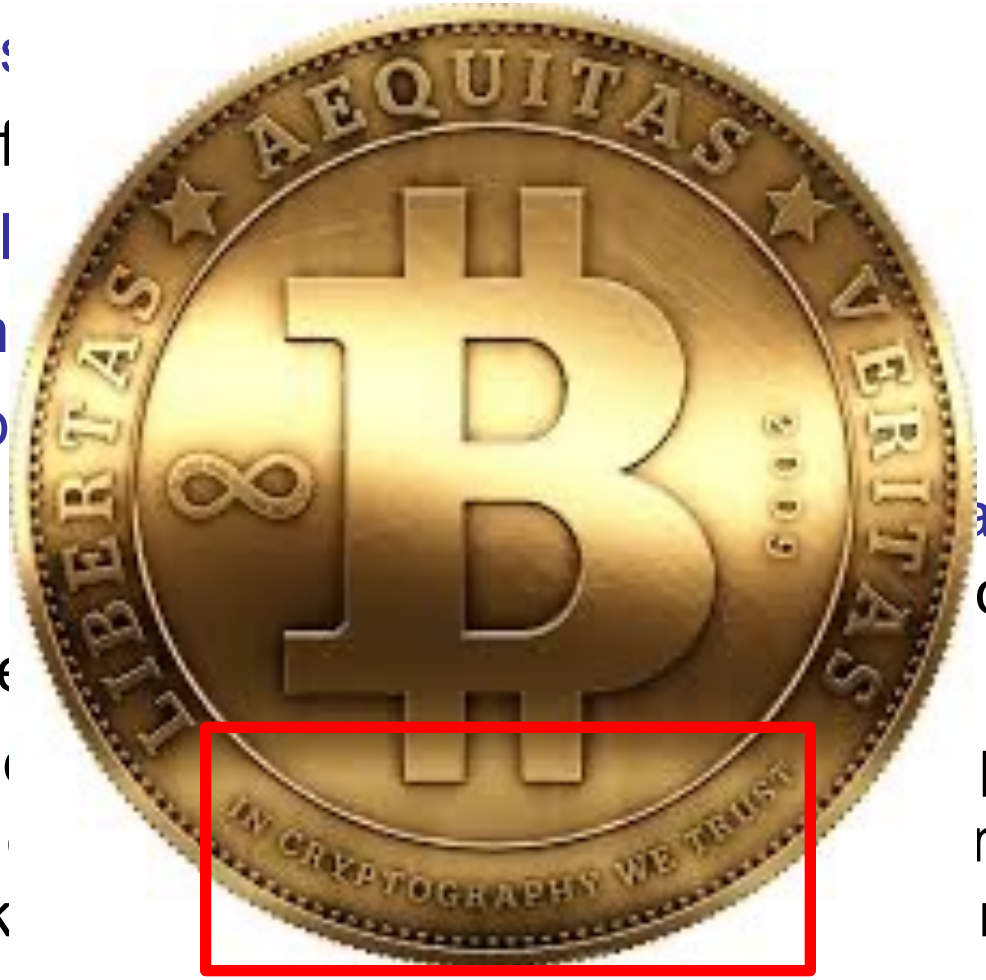
WHAT IS A BLOCKCHAIN?

Blockchain  Bitcoin

- Seen as the fifth **disruptive** technology in computing (after mainframes, PC, Internet, social media)
- A **distributed** database (ledger)
  - Shared & controlled by a group of **networked** independent parties
    - Not necessarily based on **trust**
      - Using cryptography to manage data in a secure way, with **no central authority** for rule enforcement

SOME IMPORTANT FEATURES

- Continuous
- Protected f
- Records al
- Provides n
- Provides p
- Upon new
  distributed
  block in the
- Blocks ma
  /software)
  each block



across
on as the next
pment
nsactions fit in
n the chain

Security provided by mathematical properties

Image source: http://knowyourmeme.com/photos/1293152-bitcoin

BLOCKCHAIN TYPES

Public blockchains (e.g. Bitcoin): Large distributed networks open for everyone to participate, with open source code.

Permissioned blockchains: Control roles individuals can play within the network. Code may or not be open source.

Private blockchains: Smaller, do not utilize a token. Membership closely controlled. Have trusted members and trade confidential information.

ONCE UPON A TIME…

- There were attempts for cryptocurrencies (with **centralized** transaction systems): Beenz, Flooz, E-Gold, DigiCash…
- Most fell victim to **double-spending:** Digital money transactions could be copied, resulting in spending the same money twice (if not verified)
- Then (2009) came *Bitcoin*: The king of cryptocurrencies
- White paper titled:

"Bitcoin: A Peer-to-Peer Electronic Cash System" by mysterious Satoshi Nakamoto

- *Described as "a system for electronic transactions without relying on trust"*

Image source: https://www.myblockchainblog.com/blog/a-brief-history-of-blockchain

Bitcoin Whitepaper – 2008.10.31

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

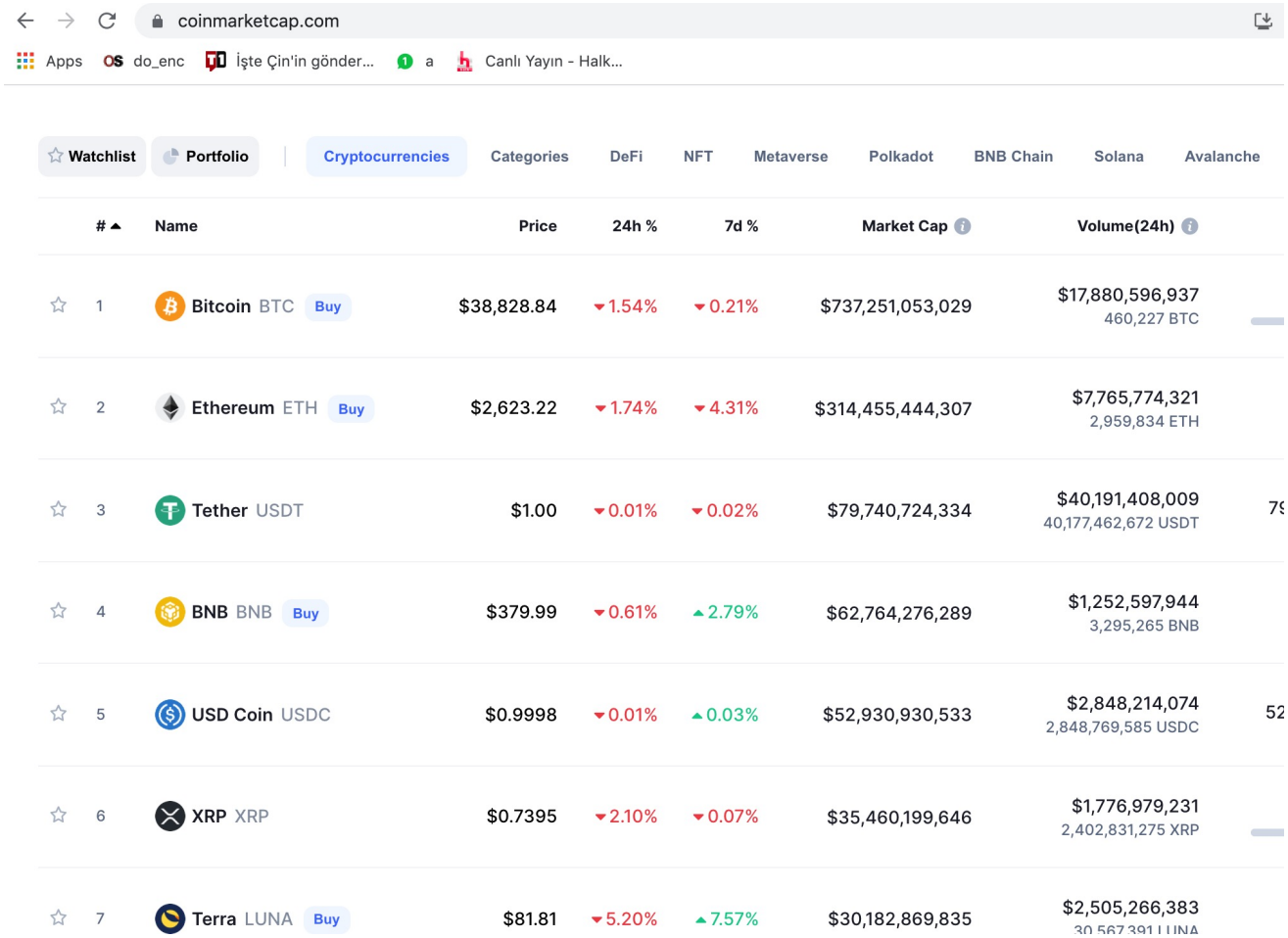
THE BTC ERA

- First open source Bitcoin client released in January 2009
- Satoshi Nakamoto amassed around 1 million BTC before disappearing from the scene around mid-2010
- BTC: First real-life application of blockchain technology
- April 2010: BitcoinMarket.com (first online marketplace for Bitcoin purchase and sales starts operating)
- May 2010: First **real-world transaction** using Bitcoin, purchasing two pizzas for 10,000 BTC.
- August 2010: First and only major **security flaw** in Bitcoin identified, protocol updated and all network computers updated to new version

THE BTC ERA CONTINUES…

- May 2011: BitPay, a global online Bitcoin payment service for merchants founded
- July 2011: The price of Bitcoin rises sharply, experiencing the first bubble ($31/BTC)
- Oct. 2011: Litecoin released as alternative (different mining algorithm and faster transactions)
- June 2012: Ripple released as alternative (focus on integration with current banking systems)
- Sept. 2012: Bitcoin Foundation launched
- Oct. 2012: > 1000 merchants accepting Bitcoin as payment
- August 2013: A Texas federal judge rules Bitcoin as “a form of money”
- Oct. 2013: FBI seizes 26,000 Bitcoins believed to have been involved in drug transaction on the infamous website “Silk Road”

CRYPTOCURRENCIES



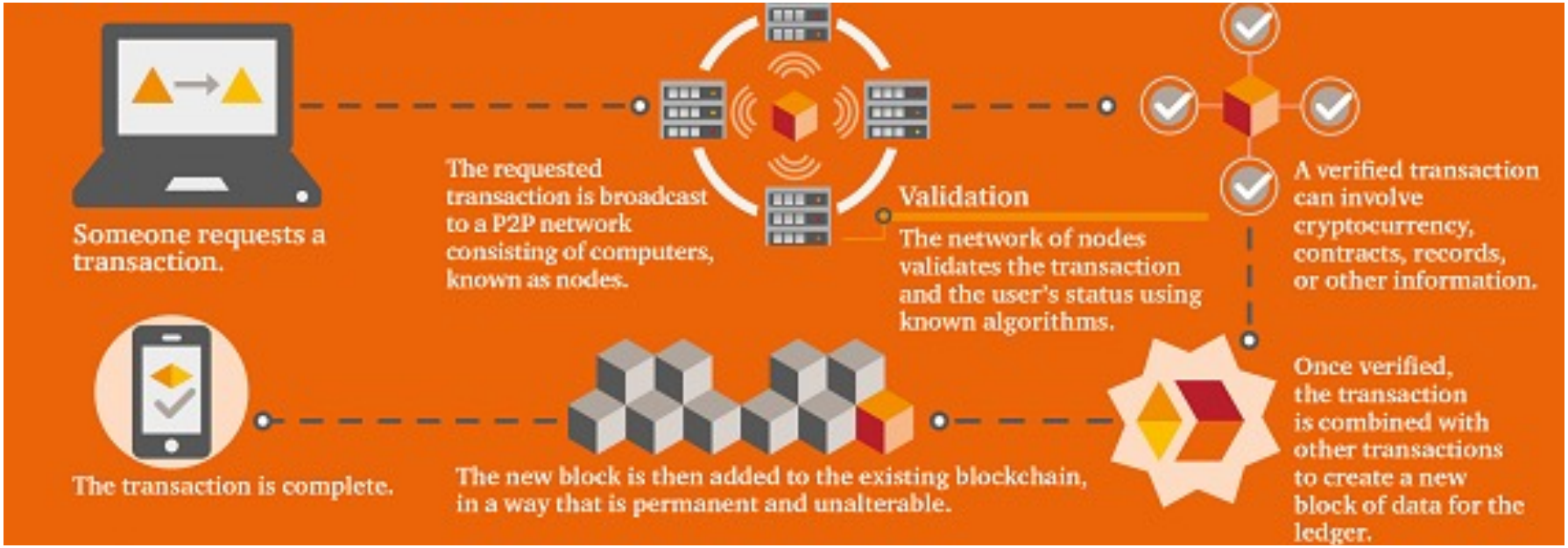
9542 of them!

Bitcoin Security Aspects

- Authentication
  - Am I paying the right person? Not some other impersonator?
- Integrity
  - Is the coin double-spent?
  - Can an attacker reverse or change transactions?
- Availability
  - Can I make a transaction anytime I want?
- Confidentiality
  - Are my transactions private? Anonymous?

Source: https://people.cs.umass.edu/~amir/courses/CMPSCI660-SP15/slides/15-Bitcoin.pptx

HOW DOES A BLOCKCHAIN WORK?



Source: https://www.pwc.com/us/en/financial-services/research-institute/blockchain.html

HOW DOES A BLOCKCHAIN WORK? (With a Bitcoin example)

THE LEDGER

Ali	12.5	
Ferit	323	
Ayse	1	
Merih	15.2	
Cagla	100	
Pelin	0.49985	- 0.00015
Hamdullah	45.00015	+ 0.00015
…	…	

Digital file of transactions

Hamdullah

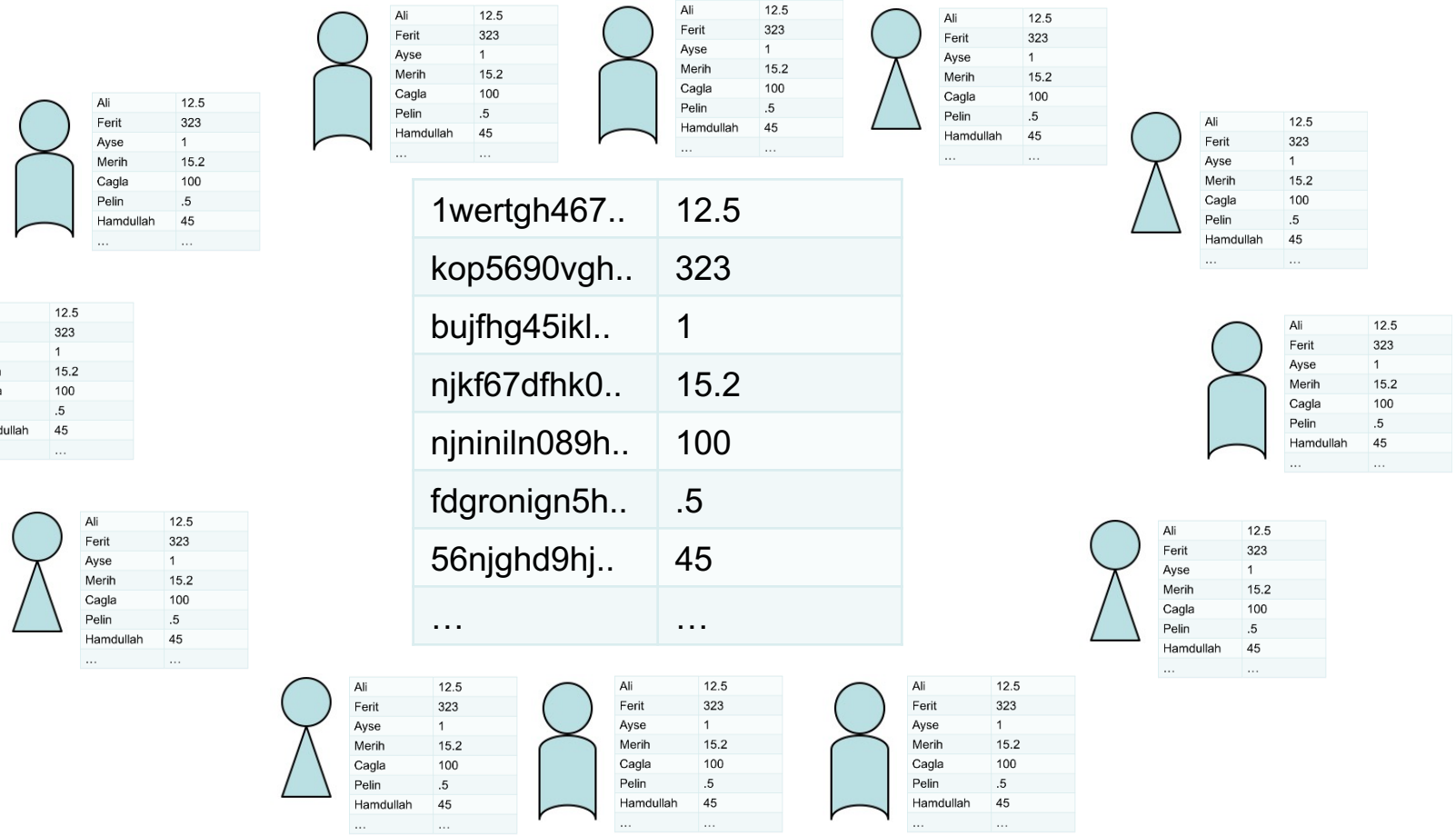
0.00015 BTC

Pelin

Image sources: https://www.pinterest.com/pin/157133474471824297/, http://knowyourmeme.com/photos/1293152-bitcoin

HOW DOES A BLOCKCHAIN WORK?

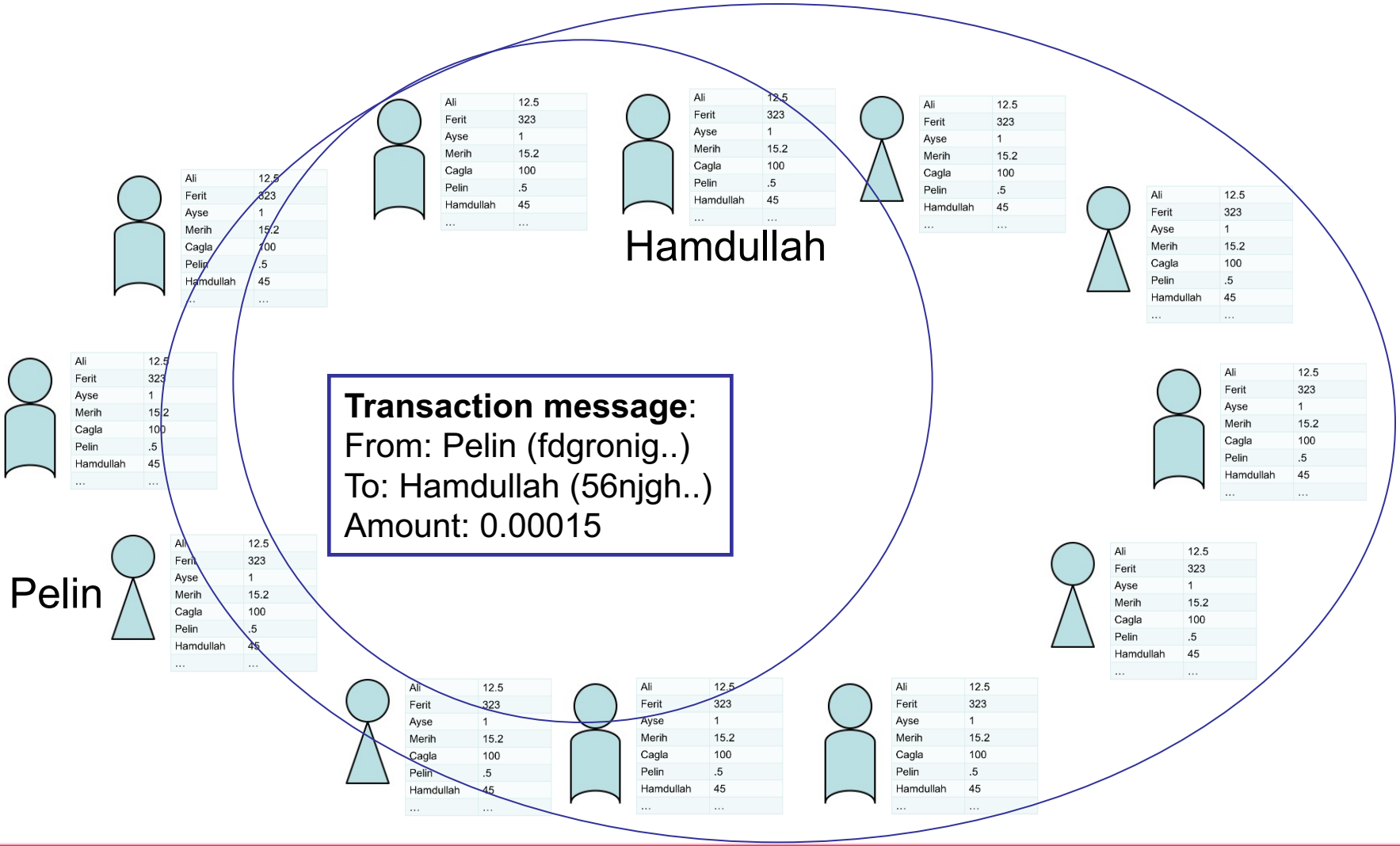
NO CENTRAL AUTHORITY, BANK, GOVERNMENT



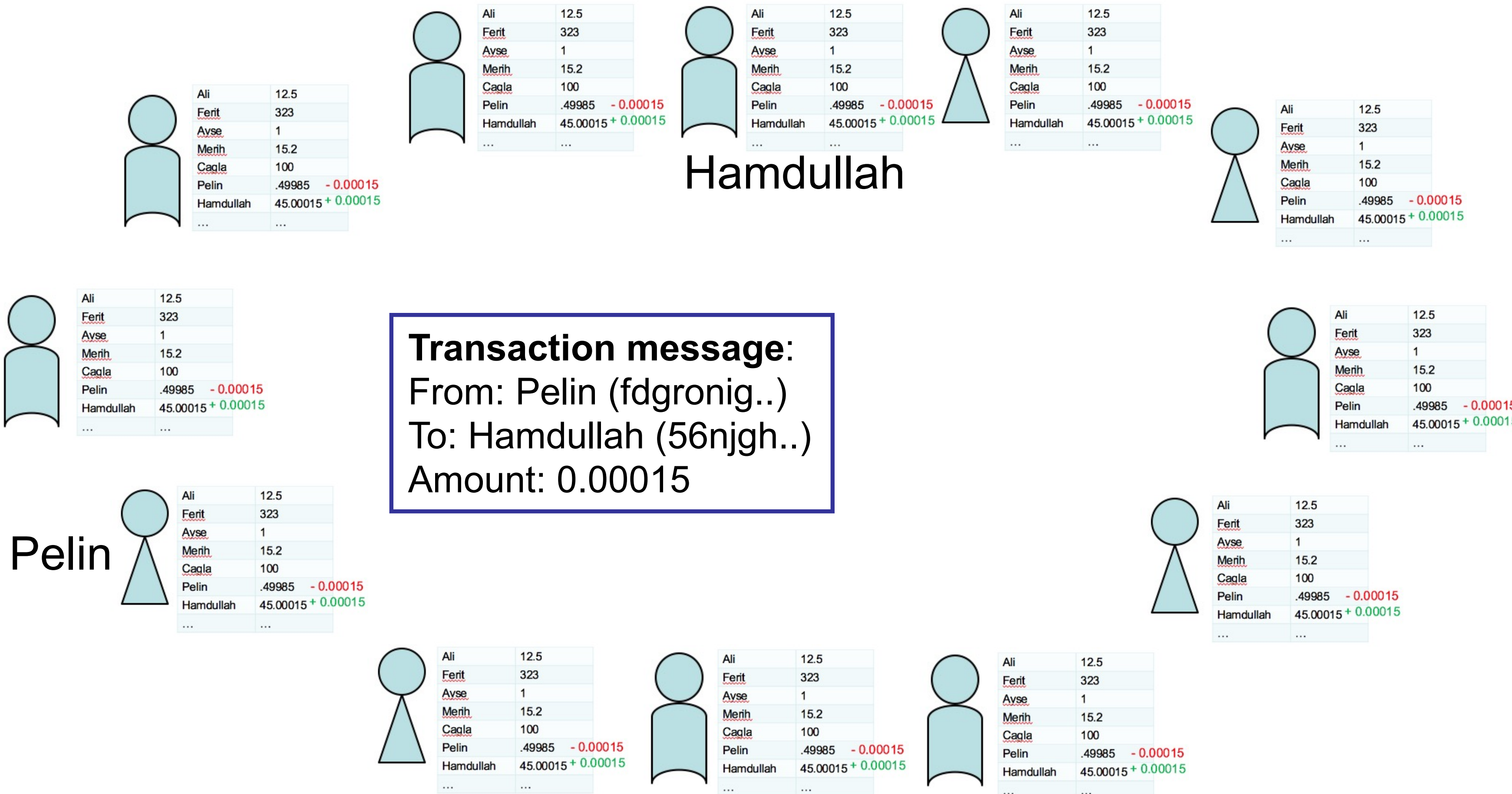
Ali	12.5
Ferit	323
Ayse	1
Merih	15.2
Cagla	100
Pelin	.5
Hamdullah	45
…	…

1wertgh467..	12.5
kop5690vgh..	323
bujfhg45ikl..	1
njkf67dfhk0..	15.2
njniniln089h..	100
fdgronign5h..	.5
56njghd9hj..	45
…	…

HOW DOES A BLOCKCHAIN WORK?



HOW DOES A BLOCKCHAIN WORK?



Decentralized

- The “digital wallet” operates in a peer-to-peer mode
- When it starts it bootstraps to find other wallets
  - Originally it used the Internet Relay Chat (IRC) network
  - Now based on DNS and “seed nodes”
- The wallet will synchronize with the network by downloading ALL of the transactions starting from the GENESIS block if necessary
  - **726,086** blocks at time of slide prep
- Using a “gossip protocol” the wallets share all transaction information with their peers http://en.wikipedia.org/wiki/Gossip_protocol

Security in Bitcoin

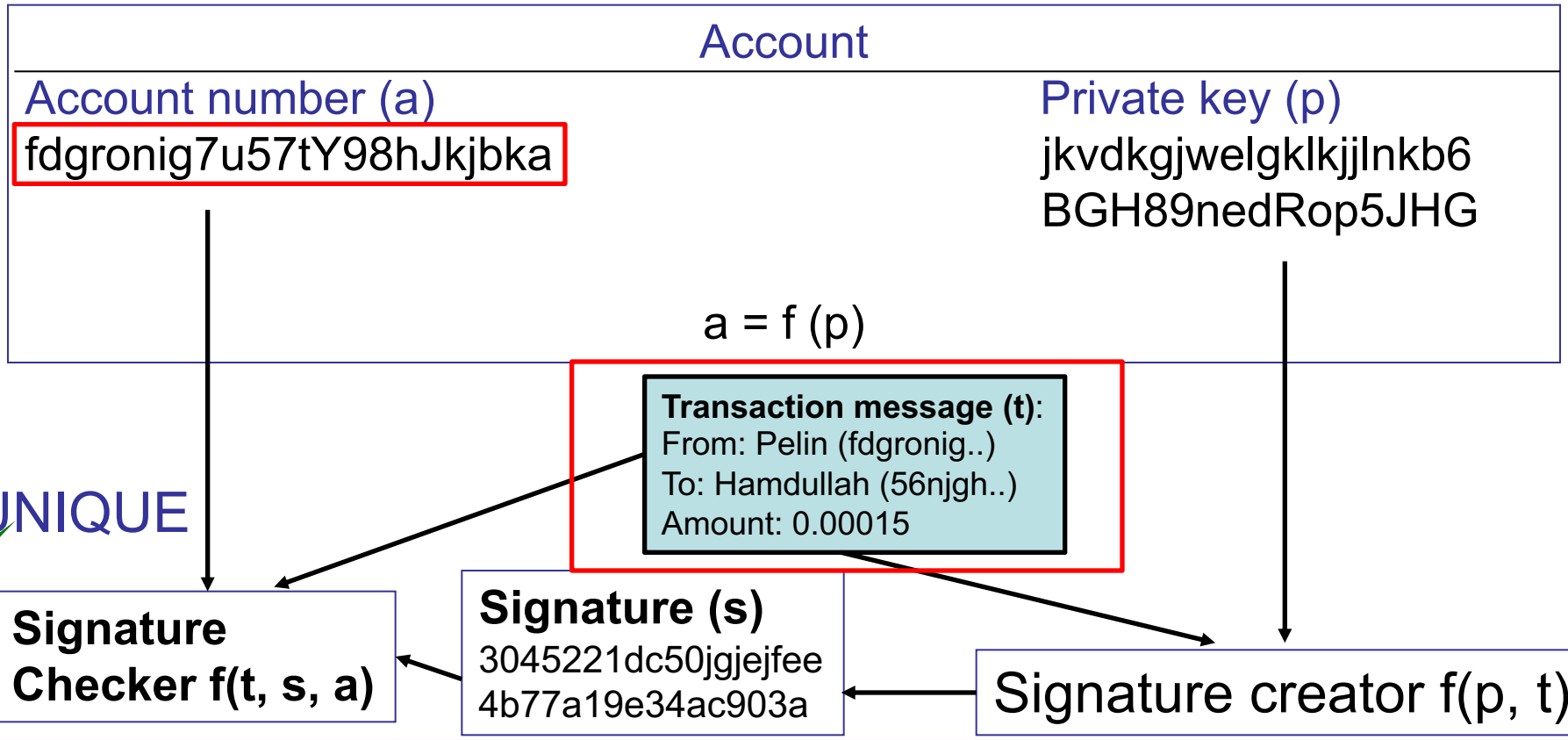
- Authentication → Public Key Crypto: Digital Signatures
  - Am I paying the right person? Not some other impersonator?
- Integrity → Digital Signatures and Cryptographic Hash
  - Is the coin double-spent?
  - Can an attacker reverse or change transactions?
- Availability→ Broadcast messages to the P2P network
  - Can I make a transaction anytime I want?
- Confidentiality→ Pseudonymity
  - Are my transactions private? Anonymous?

Source: https://people.cs.umass.edu/~amir/courses/CMPSCI660-SP15/slides/15-Bitcoin.pptx

HOW DOES A BLOCKCHAIN WORK?

What prevents someone from stealing Pelin's money (using Pelin's account number)?

DIGITAL SIGNATURE ON EACH TRANSACTION

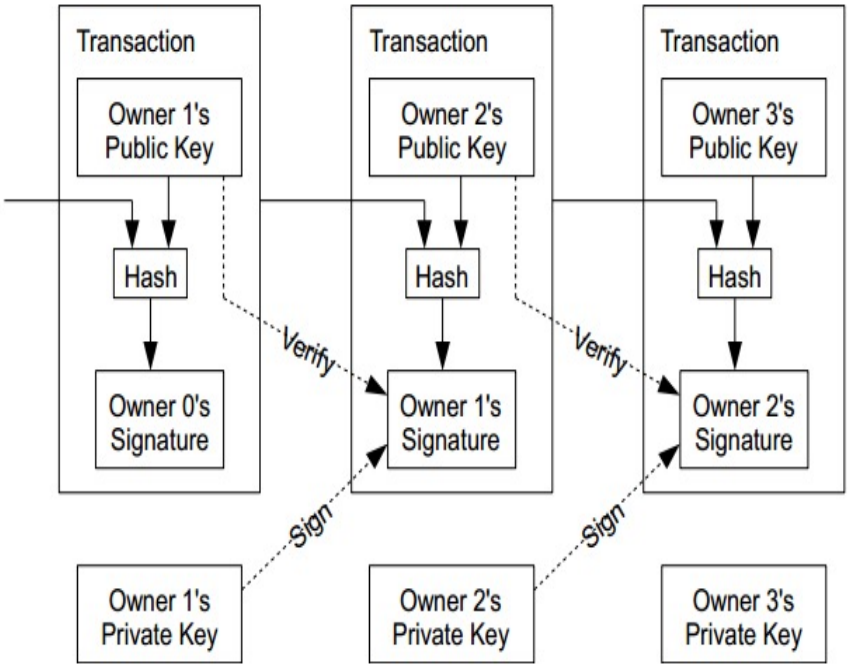


Transaction Structure in Bitcoin

- Electronic coin == chain of digital signatures
- Bitcoin transfer: Sign(Previous transaction + New owner's public key)
- Anyone can verify (n-1)th owner transferred this to the nth owner.
- Anyone can follow the history given a Bitcoin

- Using public key cryptography, specifically Elliptic Curve Cryptography due to its key strength and shorter keys

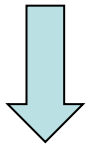
- Transactions are sent to public key "addresses"
  1AjYPi8qryPCJu6xgdJuQzVnWFXLmxq9s3
  1Give4dbry2pyJihnpqV6Urq2SGEhpz3K



Sources: https://www.umsec.umn.edu/sites/www.umsec.umn.edu/files/CodeFreeze2015-Blockchain%20Technology-Bitcoin%20and%20Beyond.pptx, https://people.cs.umass.edu/~amir/courses/CMPSCI660-SP15/slides/15-Bitcoin.pptx

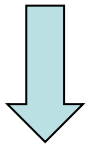
TRANSACTION ORDERING

Signatures prove who sent the transaction, not when



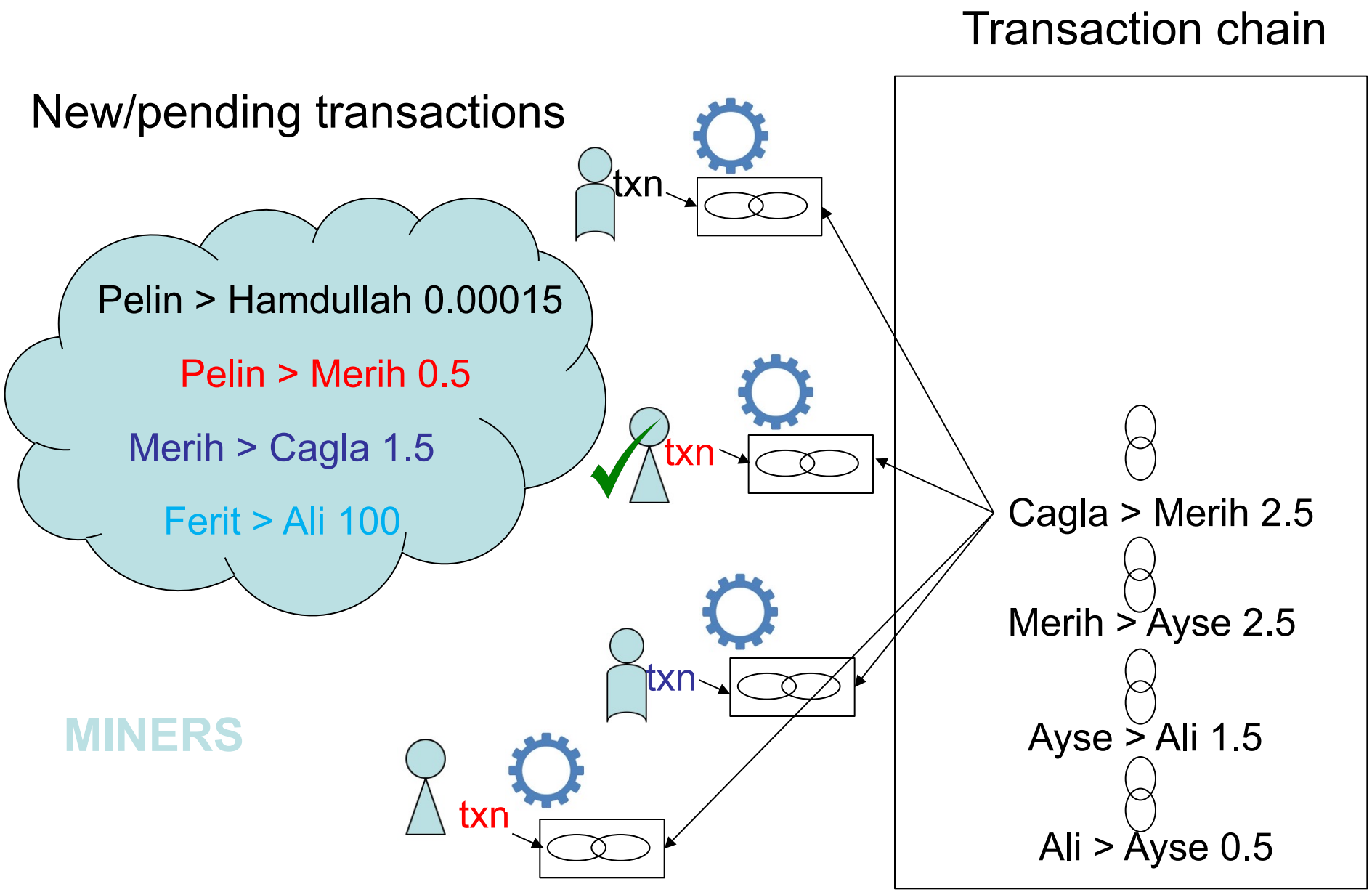
Need to establish transaction ordering
(determines who should get paid)

!!!Network delays might cause transactions to arrive in different order, users could lie about timestamps
→ Double spending problem

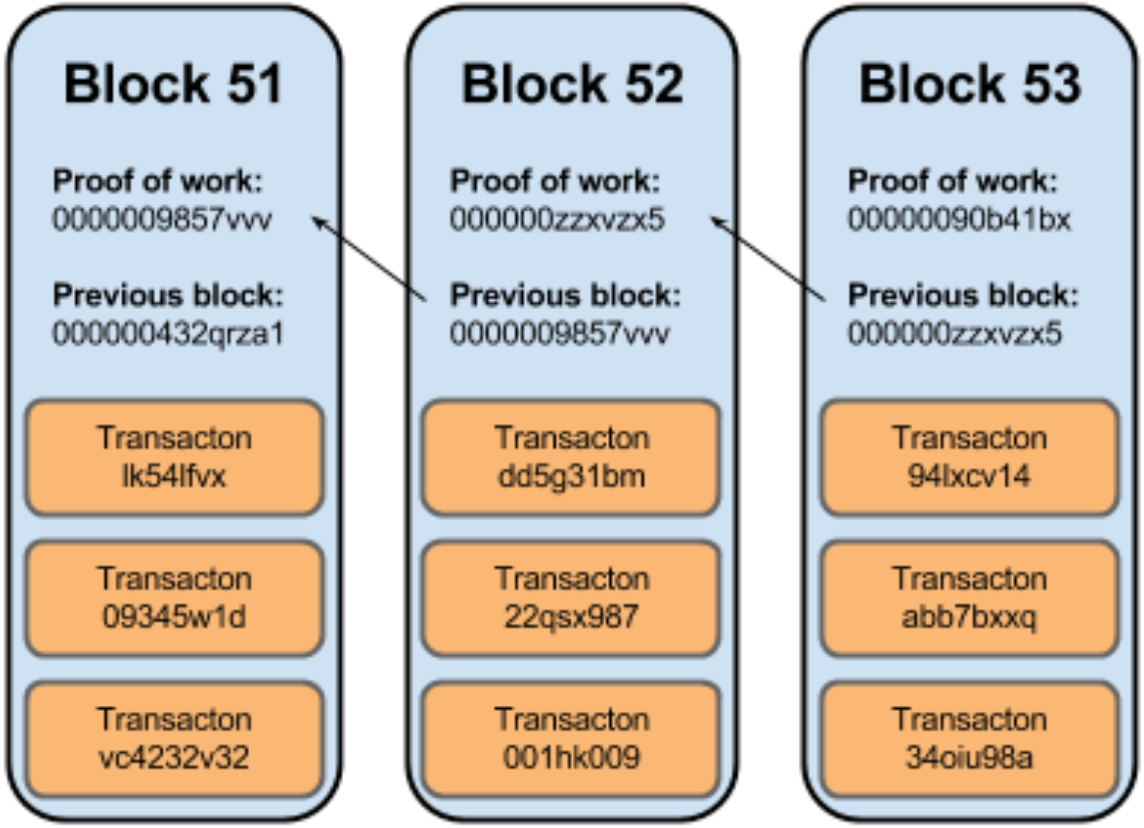


In blockchain, the whole network decides together

TRANSACTION ORDERING



BLOCKCHAIN STRUCTURE



Source: http://dataconomy.com/2015/10/wtf-is-the-blockchain-a-guide-for-total-beginners/

Anatomy of a Block

Block #404234

Summary	
Number Of Transactions	459
Output Total	3,812.78908631 BTC
Estimated Transaction Volume	815.7381711 BTC
Transaction Fees	0.1059914 BTC
Height	404234 (Main Chain)
Timestamp	2016-03-25 15:52:47
Received Time	2016-03-25 15:52:47
Relayed By	BitFury
Difficulty	165,496,835,118.23
Bits	403088579
Size	704.855 KB
Version	4
Nonce	311538175
Block Reward	25 BTC

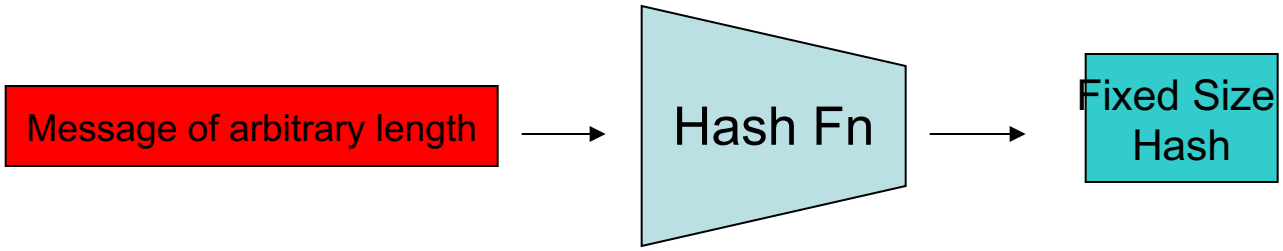
Hashes	
Hash	000000000000000000221e92ec5f42f4ccf8ba7ad71020e9dcbeed3f5e484b2f8
Previous Block	0000000000000000060e89871b8a2e9a769ec031ac3fc1da24d00886d5a8f256
Next Block(s)	0000000000000000005687e47a1fa3936b3c7eca894920b30d4904f42faa1df75
Merkle Root	3bef11b868b850a27ca176d8c4a5fb465f71771f9b46ba272dbf6f53d4e1550b

Network Propagation (Click To View)

(from blockchain.info)

Cryptographic Hash Functions

- Consistent: hash(X) always yields same result
- One-way: given Y, hard to find X s.t. hash(X) = Y
- Collision resistant: given hash(W) = Z, hard to find X such that hash(X) = Z



THE MINING PROBLEM

What linking problem do the miners solve?

Cryptographic hash

f (19342) = 56456

Irreversible: f(x) = 356 No easy way to find x!

Need to make lots of guesses:

f(5) = 43 not 356, try again

f(300) = 685 not 356, try again

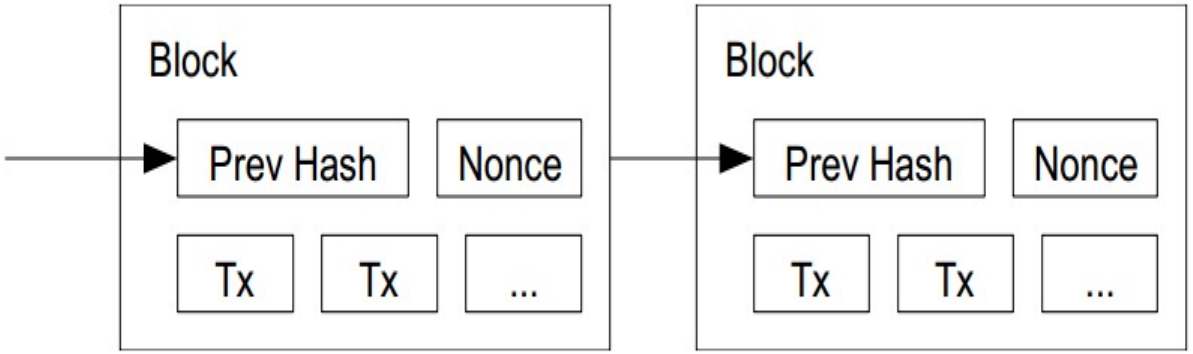
f(34) = 59 not 356, try again

Keep feeding random numbers until output meets certain criteria

https://steemit.com/bitcoin/@cryptovest/bitcoin-and-blockchain-what-math-puzzle-do-miners-actually-solve

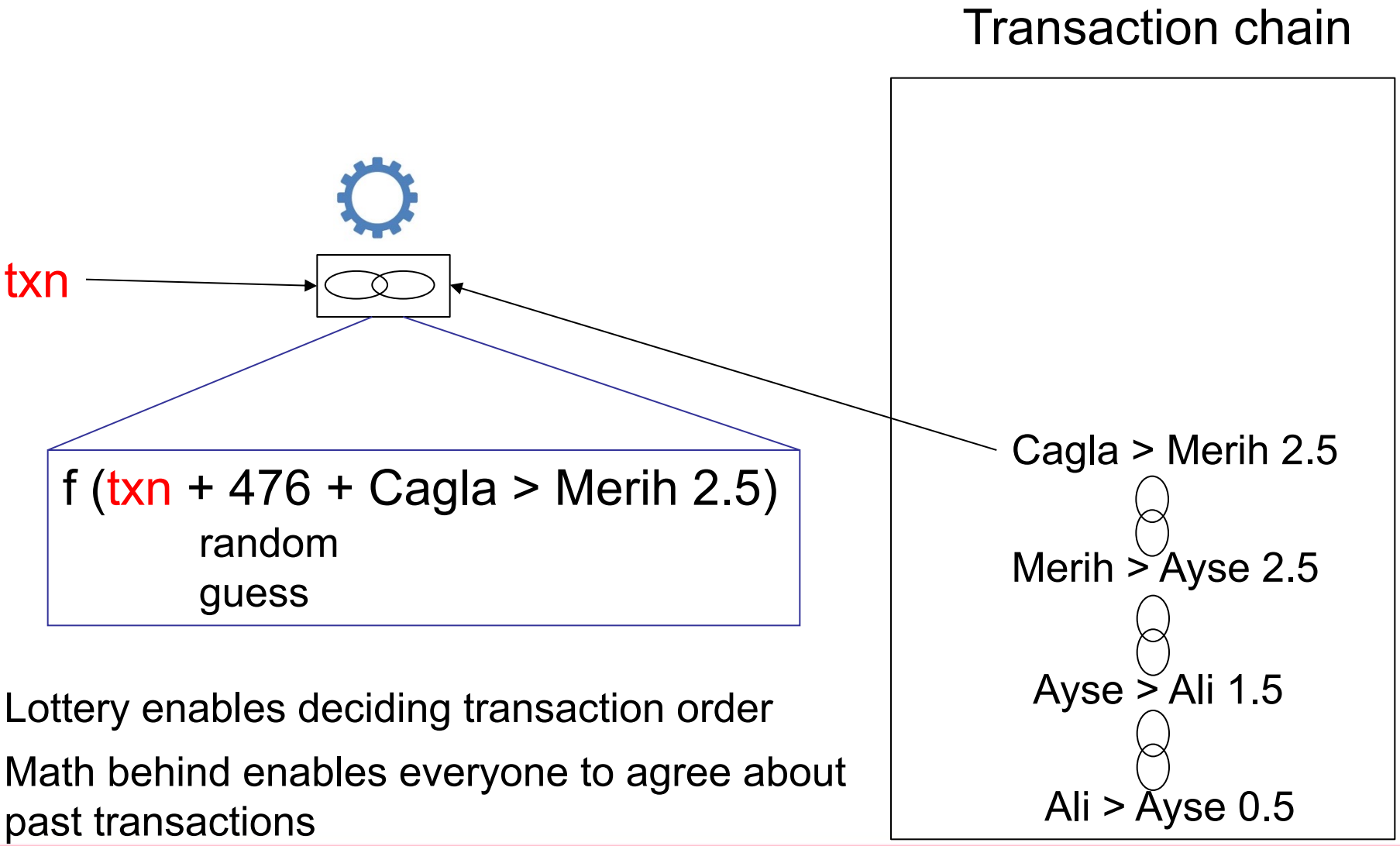
PoW (PROOF OF WORK)

- Block contains transactions to be validated and previous hash value.
- Pick a nonce such that **H(prev hash, nounce, Tx) < E**. E is a variable that the system specifies. Basically, this amounts to finding a hash value whose leading bits are zero. The work required is exponential in the number of zero bits required.
- Verification is easy. But proof-of-work is hard.



Source: https://people.cs.umass.edu/~amir/courses/CMPSCI660-SP15/slides/15-Bitcoin.pptx

CHAINING



Lottery enables deciding transaction order

Math behind enables everyone to agree about past transactions

BLOCKCHAIN SECURITY

- Decisions made by voting (50% + 1 wins!)
- What prevents one from voting many times?
- Voting requires solving difficult math problem → requires compute power → makes it unlikely that a single person/group will outvote majority of users
- Part of input to voting problem is end of chain transaction
- Due to well-defined statistical properties of cryptographic hash, possible to estimate how many guesses it took, given the answer
- Miners earn BTC when they win the transaction lottery

Preventing Double-spending

- The only way is to be aware of all transactions.
- Each node (miner) verifies that this is the first spending of the Bitcoin by the payer.
- Only when it is verified it generates the proof-of-work and attach it to the current chain.

Source: https://people.cs.umass.edu/~amir/courses/CMPSCI660-SP15/slides/15-Bitcoin.pptx

Bitcoin Network

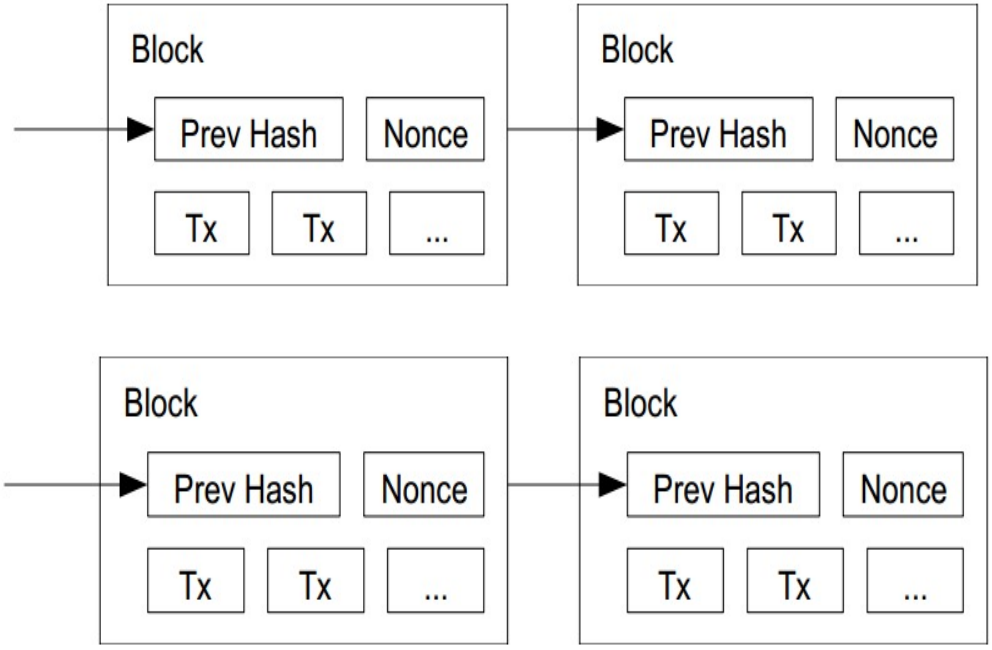
- Each P2P node runs the following algorithm:
  - New transactions are broadcast to all nodes.
  - Each node (miners) collects new transactions into a block.
  - Each node works on finding a proof-of-work for its block. (Hard to do. Probabilistic. The one to finish early will probably win.)
  - When a node finds a proof-of-work, it broadcasts the block to all nodes.
  - Nodes accept the block only if all transactions in it are valid (digital signature checking) and not already spent (check all the transactions).
  - Nodes express their acceptance by working on creating the next block in the chain, using the hash of the accepted block as the previous hash.

Source: https://people.cs.umass.edu/~amir/courses/CMPSCI660-SP15/slides/15-Bitcoin.pptx

Tie breaking

- Two nodes may find a correct block simultaneously.
  - Keep both and work on the first one
  - If one grows longer than the other, take the longer one

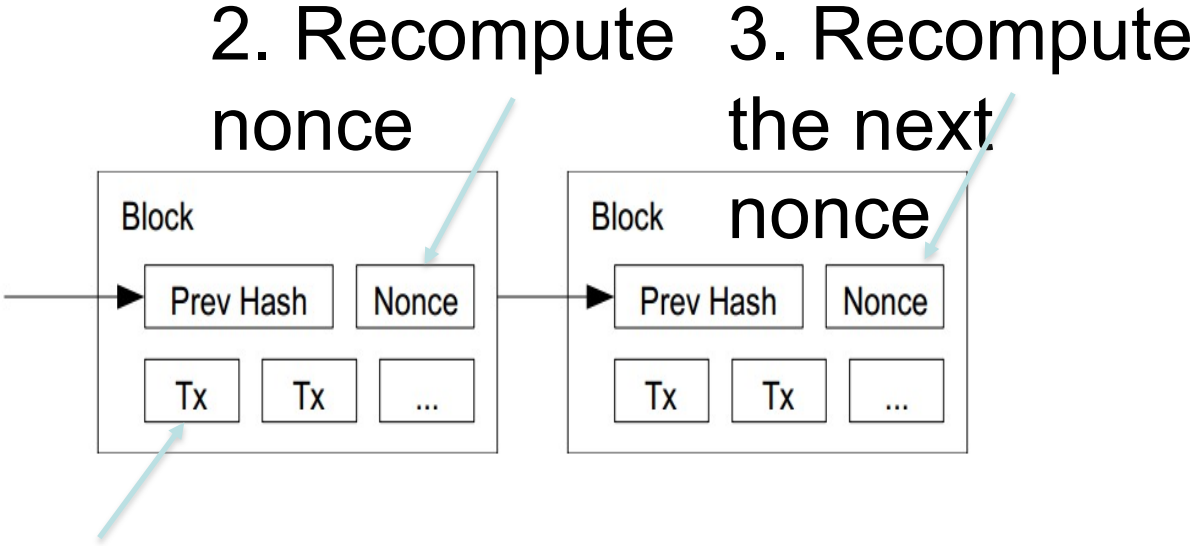
Two different block chains (or blocks) may satisfy the required proof-of-work.



Source: https://people.cs.umass.edu/~amir/courses/CMPSCI660-SP15/slides/15-Bitcoin.pptx

Reverting is Hard

- Reverting gets exponentially hard as the chain grows.



Transaction Confirmation

- Coins are not considered mature until there have been 6 confirmations (basically an hour assuming a 10 minute block cadence)
- New Coins created by the mining process are not valid until about 120 confirmations
- This is to assure that a node with more than 51% of the total hash-power does not pull off fraudulent transactions

Source: https://www.umsec.umn.edu/sites/www.umsec.umn.edu/files/CodeFreeze2015-Blockchain%20Technology-Bitcoin%20and%20Beyond.pptx

Practical Limitation

- At least 10 mins to verify a transaction.
  - Agree to pay
  - Wait for one block (10 mins) for the transaction to go through.
  - But, for a large transaction ($$$) wait longer. Because if you wait longer it becomes more secure. For large $$$, you wait for six blocks (1 hour).

Source: https://people.cs.umass.edu/~amir/courses/CMPSCI660-SP15/slides/15-Bitcoin.pptx

Privacy Implications

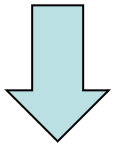
- No anonymity, only pseudonymity
- All transactions remain on the block chain– indefinitely!
- Retroactive data mining

Source: https://people.cs.umass.edu/~amir/courses/CMPSCI660-SP15/slides/15-Bitcoin.pptx

BACK TO HISTORY: BLOCKCHAIN GAINS MOMENTUM

- 2014: Blockchain technology goes beyond cryptocurrency with Vitalik Buterin (prominent Bitcoin enthusiast failing to gain agreement with Bitcoin community to update protocol)
- New blockchain protocol featuring **smart contracts:**
  - Allowing programmers to build scripts into blockchain, which act as contractual agreements executing when certain conditions met

Smart contract usage requires mini payments of **Ether (gas)**



ETHEREUM

Smart contracts allow automated transactions (money being invested/spent/saved on its own

AND THE STORY CONTINUES…

- Jan. 2014: Dash released as alternative (fast)
- Feb. 2014: Formal development of Ethereum protocol begins
- Feb 2014: Mt. Gox (one of the largest Bitcoin exchanges at the time) files for bankruptcy after 744,000 of their customers' Bitcoins stolen by hackers
- April 2014: Monero released as alternative (more focus on privacy)
- May 2015: First public version of Ethereum launched
- June 2015: Antshares (first Chinese public blockchain released)
- June 2016: Security flaws in DAO's (VC behind Ethereum) smart contracts allows hackers to access $50M worth of Ether. Blockchain split into Ethereum Classic and Ethereum
- August 2016: Bitfinex, large Bitcoin exchange hacked, 120,000 BTC stolen
- August 2016: Stratis (BaaS) platform released
- June 2017: Price of Ether reaches all-time high of $400
- …

CONSENSUS ALGORITHMS

- **Proof of stake** will make the entire mining process virtual and replace miners with validators.
- This is how the process will work:
- The validators will have to lock up some of their coins as stake.
- After that, they will start validating the blocks. Meaning, when they discover a block which they think can be added to the chain, they will validate it by placing a bet on it.
- If the block gets appended, then the validators will get a reward proportionate to their bets.

Slide: Courtesy of Prof. Ahmed Banafa

Why Ethereum wants to use PoS?

- In a distributed consensus-based on the proof of Work, miners need a lot of energy. One Bitcoin transaction required the same amount of electricity as powering 1.57 American households for one day.
- And these energy costs are paid with fiat currencies, leading to a constant downward pressure on the digital currency value.
- In recent research, experts argued that bitcoin transactions may consume as much electricity as Denmark.

Slide: Courtesy of Prof. Ahmed Banafa

A safer system?

- Using a Proof-of-Work system, bad actors are cut out thanks to technological and economic disincentives.
- In fact, programming an attack to a PoW network is very expensive, and you would need more money than you can be able to steal.
- Instead, the underlying PoS algorithm must be as bulletproof as possible because, without especially penalties, a proof of stake-based network could be cheaper to attack.

Slide: Courtesy of Prof. Ahmed Banafa

CASPER

- To solve this issue, Vitalik Buterin created the Casper protocol, designing an algorithm that can use the set some circumstances under which a bad validator might lose their deposit.
- He explained: “Economic finality is accomplished in Casper by requiring validators to submit deposits to participate, and taking away their deposits if the protocol determines that they acted in some way that violates some set of rules (‘slashing conditions’).”
- Slashing conditions refer to the circumstances above or laws that a user is not supposed to break.

Slide: Courtesy of Prof. Ahmed Banafa

Delegated Proof-of-Stake (DPoS)

- DPoS is similar to PoS in regard to staking but has a different and a more democratic system that is said to be fair. Like PoS, token holders stake their tokens in this consensus protocol.
- Instead of the probabilistic algorithm in PoS, token holders within a DPoS network are able to **cast votes proportional to their stake to appoint delegates to serve on a panel of witnesses—these witnesses secure the Blockchain network**.
- In DPoS, delegates do not need to have a large stake, but they must compete to gain the most votes from users.
- It provides better scalability compared to PoW and PoS as there are fully dedicated nodes who are voted to power the Blockchain.
- Block producers can be voted **in or out** at any time, and hence the threat of tarnishing their reputation and loss of income plays a major role against bad actors.

Slide: Courtesy of Prof. Ahmed Banafa

Proof-of-Authority (PoA)

- PoA is known to bear many similarities to PoS and DPoS, where only a group of pre-selected authorities (called validators) secure the Blockchain and are able to produce new blocks.
- New blocks on the Blockchain are created only when a **super majority** is reached by the validators.
- The **identities** of all validators are **public** and verifiable by any **third party**—resulting in the validator's public identity performing the role of proof of stake.
- As these validators identity are at stake, the threat of their identity being ruined incentivizes them to act in the best interest of the network.
- Due to the fact that PoA's trust system is predetermined, concerns has been raised that there might be a centralized element with this consensus algorithm.

Slide: Courtesy of Prof. Ahmed Banafa

Proof-of-assignment (PoA)

- Similar to DPoS, the proof-of-assignment model establishes **several trusted nodes** within the network, but only those nodes store the entire ledger.
- By allowing other network contributors to participate without **ledger storage**

Byzantine Fault Tolerance (BFT)

- BFT is the **most popular permissioned Blockchain platform protocol** and is currently used by **Hyperledger Fabric etc**.
- Imagine a group of Byzantine generals and their armies have surrounded a castle and preparing to attack.
- To win, they must attack **simultaneously**.
- But they know that there is at least one **traitor** among them.
- So, how do they launch a successful attack with at least one, unknown, bad actor in their midst?

Slide: Courtesy of Prof. Ahmed Banafa

BFT

- A consensus decision is determined based on the total **decisions submitted by all the generals**.

BLOCKCHAIN PROJECTS

- Major platforms: Ethereum, Hyperledger Fabric, Corda, Ripple, Quorum, IBM, Stellar…

- Business contracts (both public and private)
- Manufacturing supply chain (tracking back each part of the product to original producer, telling authenticity of each part)
- Exchange of assets
- TenneT: Europe's first decentralized distributed system to securely and intelligently manage flows of electricity across various regions

*https://thenextweb.com/hardfork/2017/11/09/deloitte-blockchain-26000-projects/

BLOCKCHAIN PROJECTS (CONT.)

- Singapore's Smart Nation Project:
  - Share information between networks in a smart city securely
  - Alleviate traffic jams
  - Satellite cities in India to provide low-energy housing, intelligent grids, planned transportation…
- China's big data problem:
  - Enforce reliability of big data
  - Solve trust issue in sharing data between parties without aligned incentives
  - Tracking ownership, origin and authenticity
- Securing borders (UK, USA)
- Estonia's e-residency (Hybrid cloud enhancing security of tax reporting, online healthcare advice)
- Biographical identities

ANTICIPATED APPLICATION AREAS

- Government-backed land record systems
- International travel security applications (blockchain-enabled passports)
- UK, Singapore, UAE see it as a way to cut cost, create new financial instruments, and keep clean records
- Moving money across borders
- Real estate (transparent mortgage-backed securities
- Smart cities (IoT-enabled)
- Digital rights management
- Smart homes, wearables
- Collaborative software development

INTERNET OF THINGS (IOT)

Image source: https://www.jigsawacademy.com/iot/

IOT SECURITY PROBLEMS

- Confidentiality
- Device authentication
- Enlarged attack surface
- Data integrity
- Distributed denial of service (DDoS)
- Repudiation
- Device capacity constraints

IOT INCIDENTS

1

2

3

4

5

Sources:

1. https://ahmedbanafa.blogspot.com.tr/2016/10/a-wake-up-call-for-iot.html
2. https://thehacktoday.com/hackers-can-easily-hijack-popular-baby-monitors-to-watch-your-kids
3. https://thehackernews.com/2015/02/smart-tv-spying.html
4. https://www.thedailybeast.com/the-terrifying-us-israeli-computer-worm-that-could-cause-world-war-iii
5. https://www.wired.com/2015/07/hackers-remotely-kill-jeep-highway/

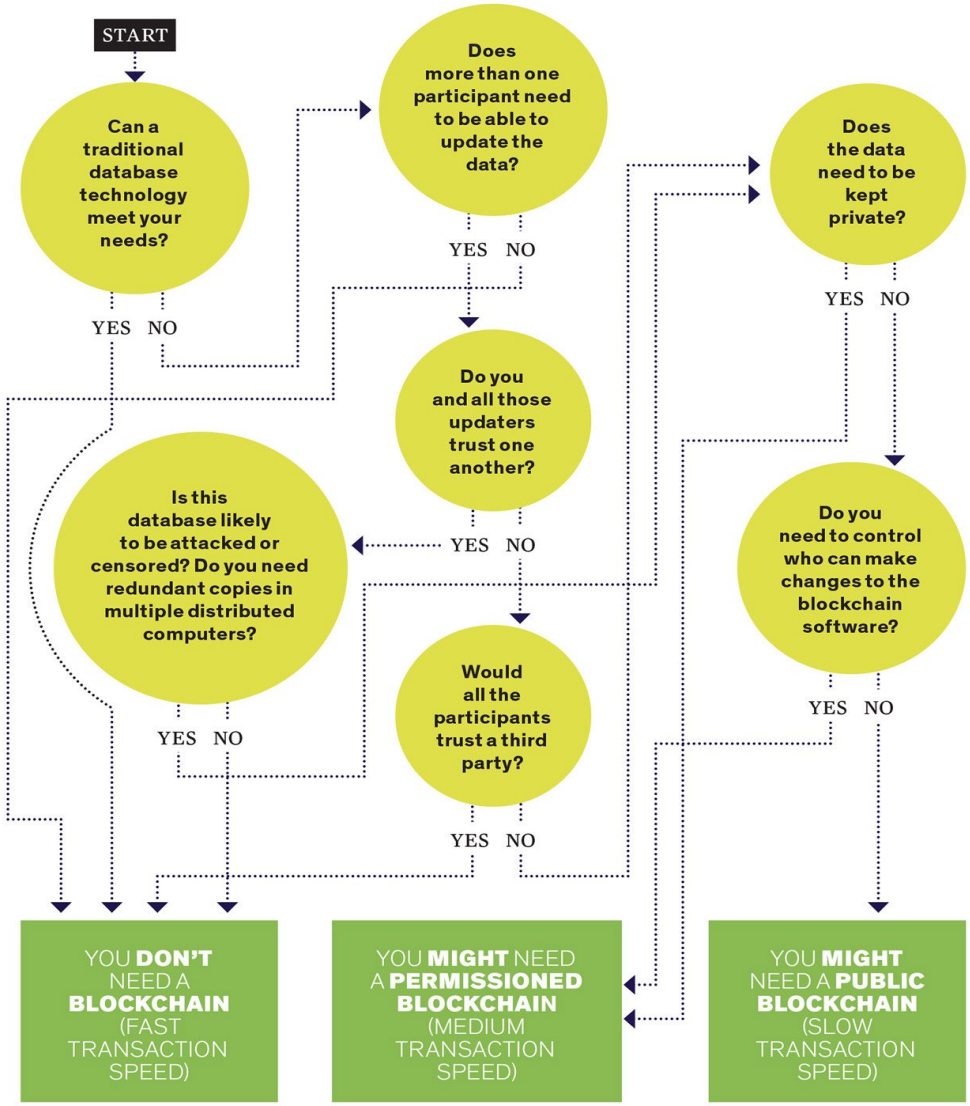
HOW CAN BLOCKCHAIN HELP IOT?

- Decentralized device authentication
- Data integrity verification
- Assignment of responsility
- Royalty for shared resource usage (IOTA)

BLOCKCHAIN LIMITATIONS

- No real distributed transaction processing (replication instead)
- Ever-growing size
- Speed in some (Bitcoin network capable of processing 7 transactions/sec, transactions recorded once every 10 mins)
- Energy consumption in PoW (Electricity consumed equivalent to the amount a city with population of 100,000 would consume)
- If 51% of network is malicious, alternative history can be written
- Not complete anonymity, pseudonymity rather (everyone sees all transactions)
- Regulatory issues and integration

DO YOU NEED BLOCKCHAIN?



https://medium.com/@sbmeunier/when-do-you-need-blockchain-decision-models-a5c40e7c9ba1

THANK YOU ☺

REFERENCES

- Tiana Laurence, “Blockchain for dummies”, John Wiley & Sons, 2017.
- https://www.kaspersky.com/blog/bitcoin-blockchain-issues/18019/
- https://hbr.org/2017/02/a-brief-history-of-blockchain
- https://www.myblockchainblog.com/blog/a-brief-history-of-blockchain
- https://www.myblockchainblog.com/blog/the-argument-against-blockchain
- https://www.techbullion.com/blockchain-definition-origin-history/
- https://thenextweb.com/hardfork/2017/11/09/deloitte-blockchain-26000-projects/
- https://www.evry.com/globalassets/insight/bank2020/bank-2020---blockchain-powering-the-internet-of-value---whitepaper.pdf
- https://coinsutra.com/bitcoin-double-spending/
- http://www.wikizero.org/index.php?q=aHR0cHM6Ly9lbi53aWtpcGVkaWEub3JnL3dpa2kvSGlzdG9yeV9vZl9iaXRjb2luI2NpdGVfbm90ZS1XaXJlZDpSRkItMTI
- https://www.luno.com/blog/en/post/how-bitcoin-price-determined
- https://www.youtube.com/watch?v=l9jOJk30eQs