Cryptocurrencies summary

D. Papaioannou, Prof. Ioannis Pitas
Aristotle University of Thessaloniki
pitas@csd.auth.gr
www.aiia.csd.auth.gr

Version 1.0

Artificial Intelligence &
Information Analysis Lab

Cryptocurrencies

- **Introduction to Cryptography**
- Introduction to Blockchain
- Introduction to Blockchain Consensus Algorithms
- Blockchain and Cryptocurrency

Introduction to Cryptography

- ***Four pillars of Cryptography:***
  - ***Encryption:*** Method for converting normal texts (plaintext) into a sequence of random bits (ciphertext).
  - ***Decryption:*** Defined as the inverse task of encryption, transformation of ciphertext to plaintext.
  - ***Cipher:*** An algorithm for modifying plaintext to chiphertext or the inverse.
  - ***Key:*** A set of information which is fed as input in the encryption/ decryption operation in order to produce the desired output, the ciphertext or the plaintext respectively.

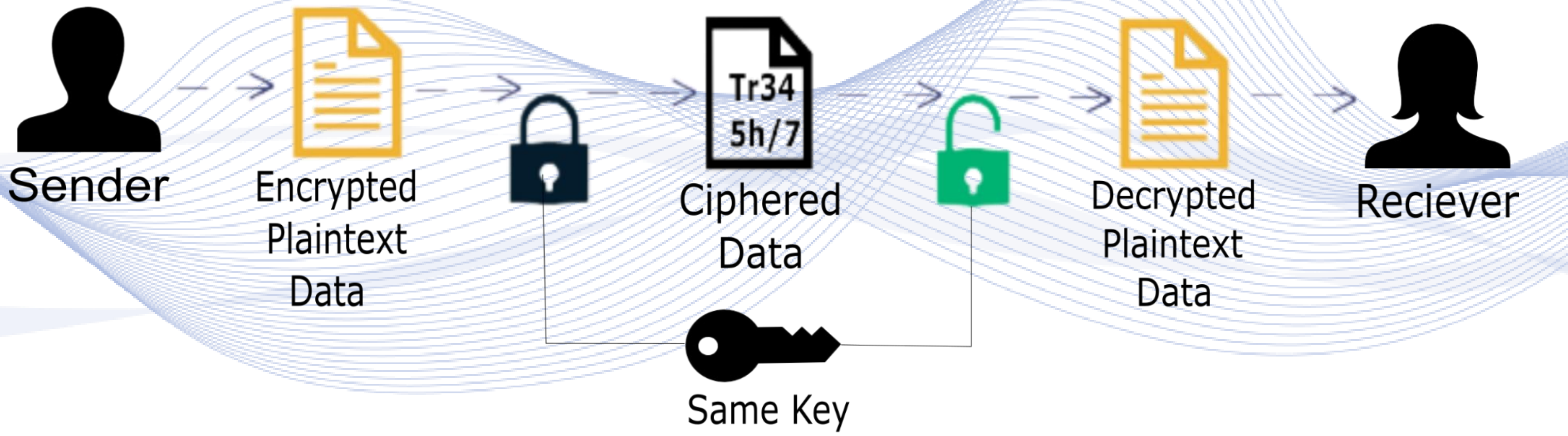
Introduction to Cryptography

- ***Types of Cryptography:***
  - ***Symmetric Key Cryptography***: Achieving encryption and decryption using a single-key, also known as Private key Cryptography.
  - ***Asymmetric Cryptography:*** Achieving encrypt and decrypt by using a public key for the first operation and a private key for the second operation, also called Public key Cryptography.
  - ***Hash Functions:*** Irreversibly “encrypt” information achieved by using mathematical transformations.

Introduction to Cryptography

Symmetric Key Cryptography

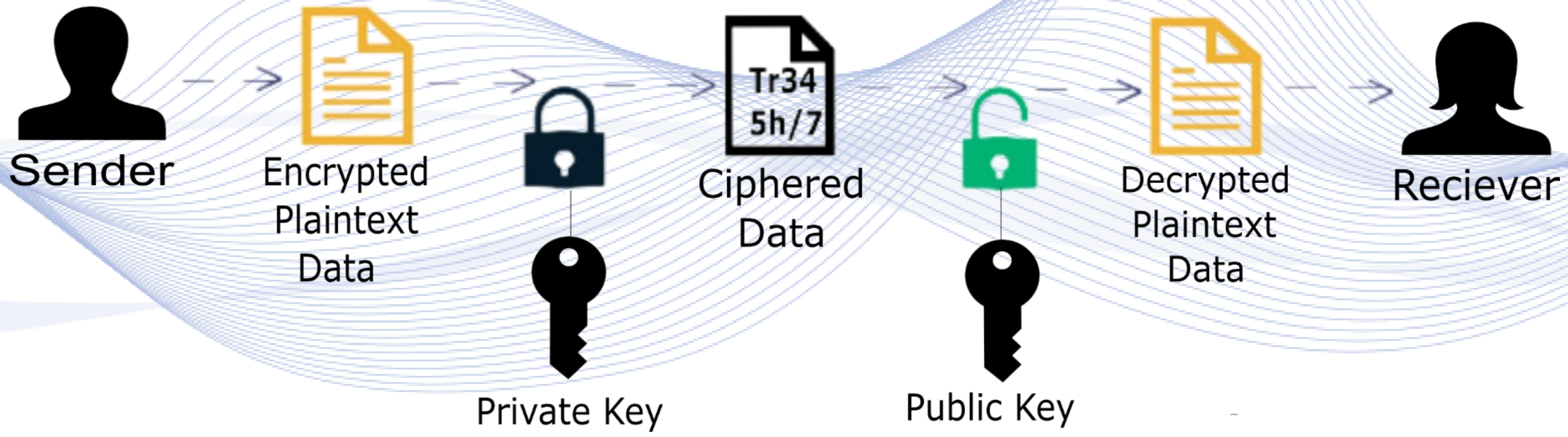
- ***Encryption*** and ***decryption*** achieved by ***one single key.***
- Both, sender and receiver, have knowledge about the ***shared key***.
- Fast Symmetric encryption achieved.
- Less secure for sensitive data since key size is smaller.



Introduction to Cryptography

Asymmetric Key Cryptography

- ***Public key*** is shared by ***everyone*** on the cryptographic scheme while ***Private key*** is known only by the ***authenticated user***.
- Private key is a result by a randomly generated number and the public key is the result of the irreversible algorithm
- Less processing speed and encryption power.



Introduction to Cryptography

- ***Hash Function:*** Can be defined as a " ***digital fingerprint"*** (unique identifier) for every given piece of data.

- A process that receives as ***input*** a plaintext data $\boldsymbol{X}$ of any size and maps it into a ***unique output*** (chipertext) of a fixed size.

- The ***Secure Hash Algorithm SHA***, developed by NIST and NSA, is one of the most efficient and well-known hash function families.

Cryptocurrencies

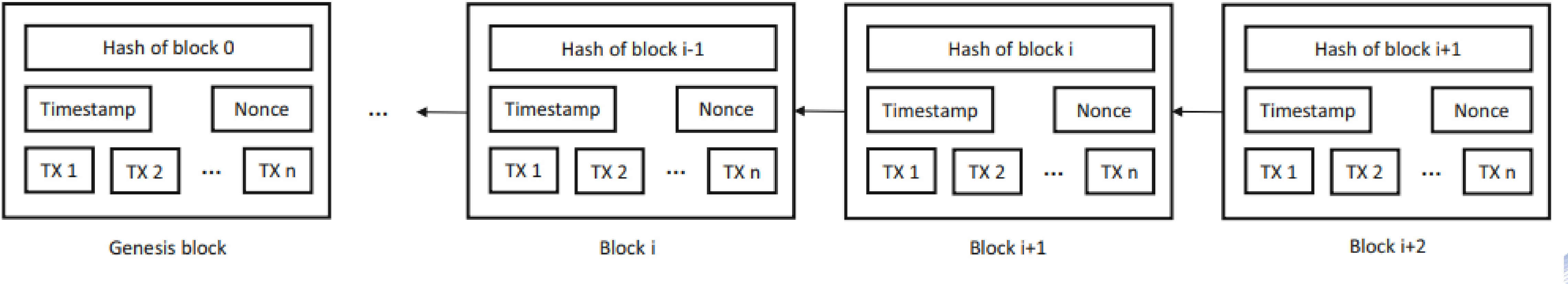
- Introduction to Cryptography
- **Introduction to Blockchain**
- Introduction to Blockchain Consensus Algorithms
- Blockchain and Cryptocurrency

Introduction to Blockchain

Blockchain essentially consists of a ***sequence of blocks*** each one of them holding a complete list of transactions records.

Can be defined as a database system which holds data sets secured and bounded to each other in a ***chain***, using crypto-graphic principles, in form of packages (blocks) where each one of the blocks consist of various transactions (TX-n).

Introduction to Blockchain



The blocks structure.

Source: [NOF2017]

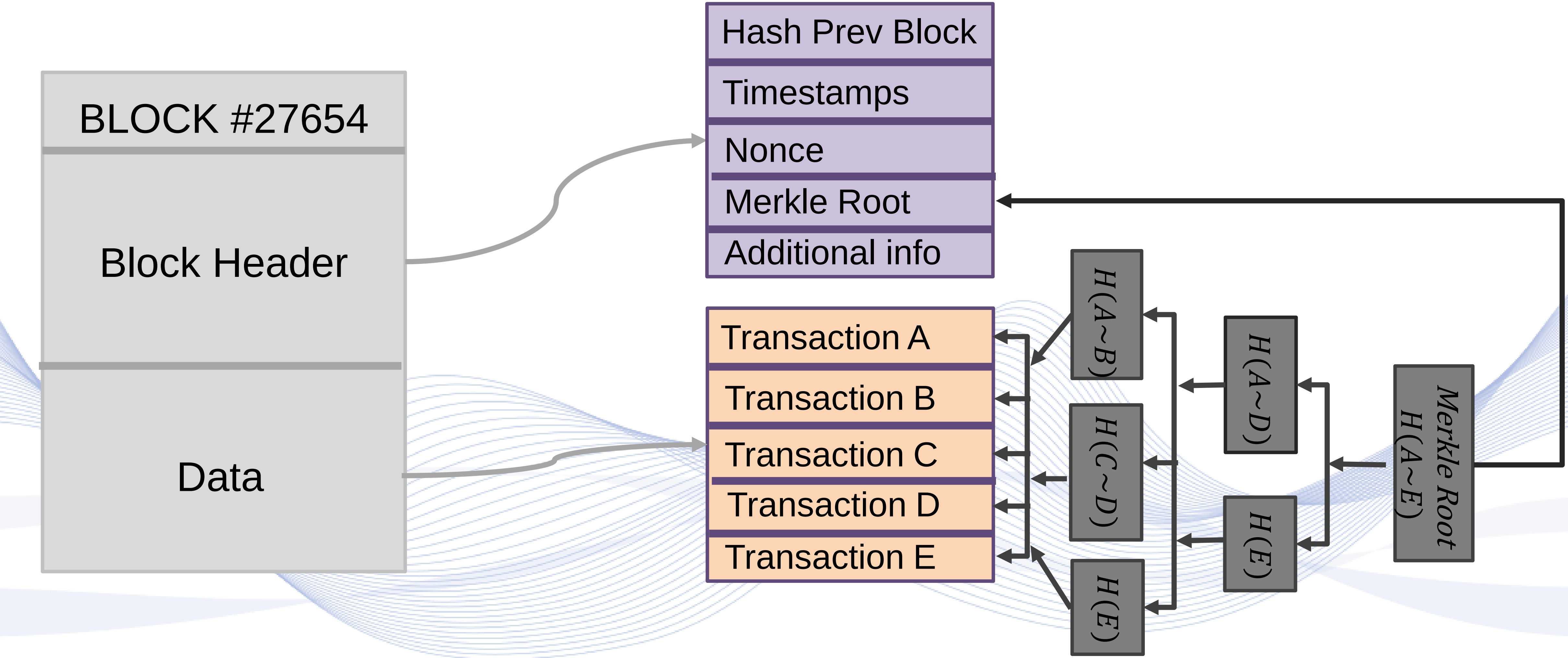
Introduction to Blockchain

Each block contains the header where ***timestamp, hash for the past block, hash for the block itself*** and a ***nonce*** are stored inside. The above structure can ensure the integrity of the chain from the first to the last block.

First block is known as “***Genesis block***” and does not contain hash value for the previous block.

Nonce is a $32-bit$ random integer number used in order to validate the hash value produced for the specific block.

Introduction to Blockchain



BLOCK #27654

Block Header

Data

Hash Prev Block

Timestamps

Nonce

Merkle Root

Additional info

Transaction A

Transaction B

Transaction C

Transaction D

Transaction E

Introduction to Blockchain

Blockchain technology is a ***peer-to-peer***, distributed network ledger which is secured by cryptography methods, immutable, append-only and updated only via consensus or agreement between nodes.

- ***Peer-to-peer:*** No central authority governs this network, but instead all participants (peers) must communicate directly with each other. In case of transaction cash, this feature allows exchanges to be achieved directly between peers without third-party interaction.

Introduction to Blockchain

- ***Distributed Ledger:*** Ledger is spread all over the network and between all the nodes (peers), and each node keeps a copy of the entire ledger.

- ***Cryptographically-secure:*** Cryptography assures the security, making in that way the ledger safe in terms of misuse and tampering. Data origin authentication and integrity is necessary for that step.

Introduction to Blockchain

- ***Append-Only:*** Data enter in the chain only via time-ordered sequential order. Once data enter the chain is almost impossible to change them (immutability).

- ***Updated via consensus:*** The last critical aspect, no central authority upgrades the ledger but instead, the upgrades that are being made in the blockchain are invoked through various guidelines determined by the chain protocol and are entered only when a consensus has been made between the nodes (participants) in the chain.

Cryptocurrencies

- Introduction to Cryptography
- Introduction to Blockchain
- **Introduction to Blockchain Consensus Algorithms**
- Blockchain and Cryptocurrency

Blockchain Consensus

- In synchronous communication models a clock consistency frequency is being used, allowing for a limited time the presence of errors.

- The consensus protocols relying on:
  - Synchronous communication models.
  - Weak synchronous communication models, where a timeout method is used for the transition of messages.

Blockchain Consensus

- Blockchain is using weak synchronization communication models, where a message even if delayed, it would eventually reach the recipient within a certain time limit.

- A solution to Byzantine Generals’ Problem through a consensus protocol where each individual node of the chain could reach an agreement about the state of the chain.

Blockchain Consensus

- Those consensus algorithms must guarantee:
  - ***Consistency:*** If a message (transaction) is verified for a loyal node then it will be verified for the remaining loyal nodes too. So, if honest nodes is the majority then the double-spending attacks will never be a success in a blockchain system.
  - ***Liveness:*** All valid messages (transactions) between loyal nodes must and eventually will be confirmed, ensuring in that way the system's sustainability.

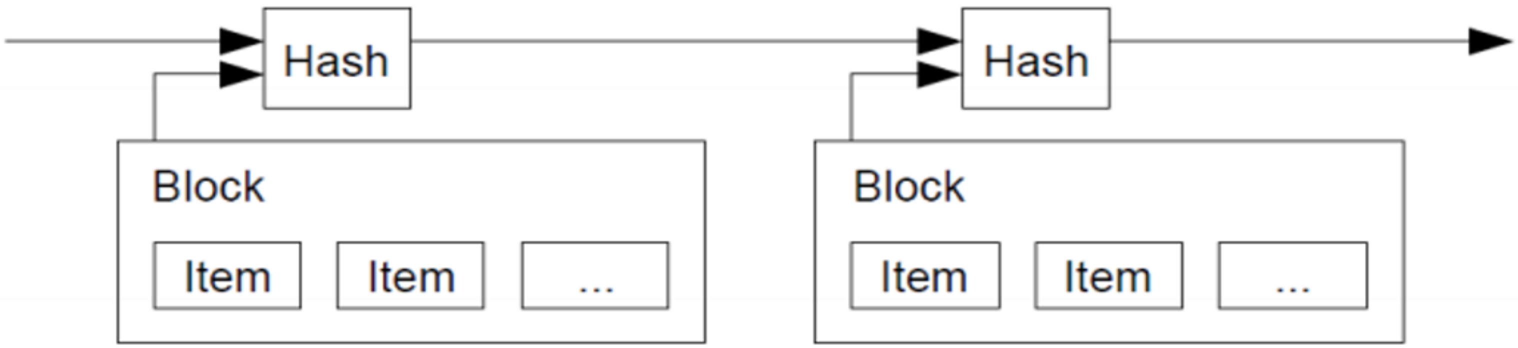
Proof of Work

- ***Proof of Work (PoW):*** Is an algorithm (protocol) formed around a cryptographic zero-knowledge proof where it involves two independent ***nodes, the prover*** (requestors) and ***the verifier*** (provider).

- The prover also called ***miner*** executes a time consuming hard computational task (cryptographic task or mathematical problem) trying to reach a specific goal and present it to verifier or in group of them in order to validate the task.

Proof of Work

- PoW consensus protocol is also used for adding new blocks in the chain.
- As we know blocks in the chain are append-only in a sequence of timestamped blocks using hash values for verifying their existence.



Timestamps.

Source: [CHA2019]

Proof of Work

- Miners via the requested computational task are actually trying to produce a new hash for the candidate block, which is supposed to be less than a dynamically varying target value (consensus rule).

- Mining the hash performed using three known values:
  - Hash for the previous block.
  - Hashes of the transactions inside the block.
  - And the blocks creating time.

- Goal is to create the “nonce” value which fits better in the pattern.

Proof of Work

- When a miner generate such value then it needs to be verified from at least 51% of the nodes in order to be accepted ***(winning value)***.
- The verification is considered as a low computational procedure which can last almost a few seconds, if the process indicates that the block is valid then the node is add it in his version of the chain.
- Once a winning value is detected then the miner is being rewarded with the amount of Bitcoins, that correspond to the effort he provided to the chain as well as the sum of all fees.

Cryptocurrencies

- Introduction to Cryptography
- Introduction to Blockchain
- Introduction to Blockchain Consensus Algorithms
- **Blockchain and Cryptocurrency**

Cryptocurrency

Blockchain is a decentralized mechanism that can have huge impact in economy by creating ***electronic currencies*** which attempts to be more ***trustworthy*** and ***secure*** than the physical money:

- There is no central authority controlling the money flow.
- Customers no longer need to put their “faith” in centralized systems (e.g., their bank). Instead, they must trust the technology.
- Blockchain technology is transparent.

Cryptocurrency Institution

Technology	Blockchain			
Protocol - Coins	Bitcoin	Ethereum	Ripple	Neo
Tokens	No Tokens	- TRX - SNT - AE - PPT	No Tokens	- ACAT - DBC - TNC - IAM

Cryptocurrency

- ***Cryptocurrency*** is as an electronic or digital currency that is ***secured*** via a ***cryptographically mechanism***. Many cryptocurrencies are using decentralized networks like the blockchain technology.

Cryptocurrency

- A cryptocurrency ***is not*** just a ***currency***
- It is actually a protocol with a set of specific rules that specify how the participants of the network communicate with each other, using protocols, such as IP/HTTP/TCP/SMTP.

- Each of those protocols contains an important feature called ***coin***.
- There is only one coin attached to each protocol.

- The coin is an innate asset of the protocol which facilitates the interaction of participants by rewarding the miners for their mining or for transactions.

Cryptocurrency

Tokens basically rely on smart contracts, which are built on top of the different protocols.

- They constitute a form of funding a new idea, e.g., how to use blockchain in healthcare, IoT or for supply chain.
- Thus, basically, when someone invests in tokens, he actually invests on new ideas, in order to create ***Decentralized Applications*** (***Dapps***).

Initial Coin Offering (ICO)

Initial Coin Offering (***ICO***) can be achieved on token layer or even in protocol layer (e.g., a new protocol for chain).

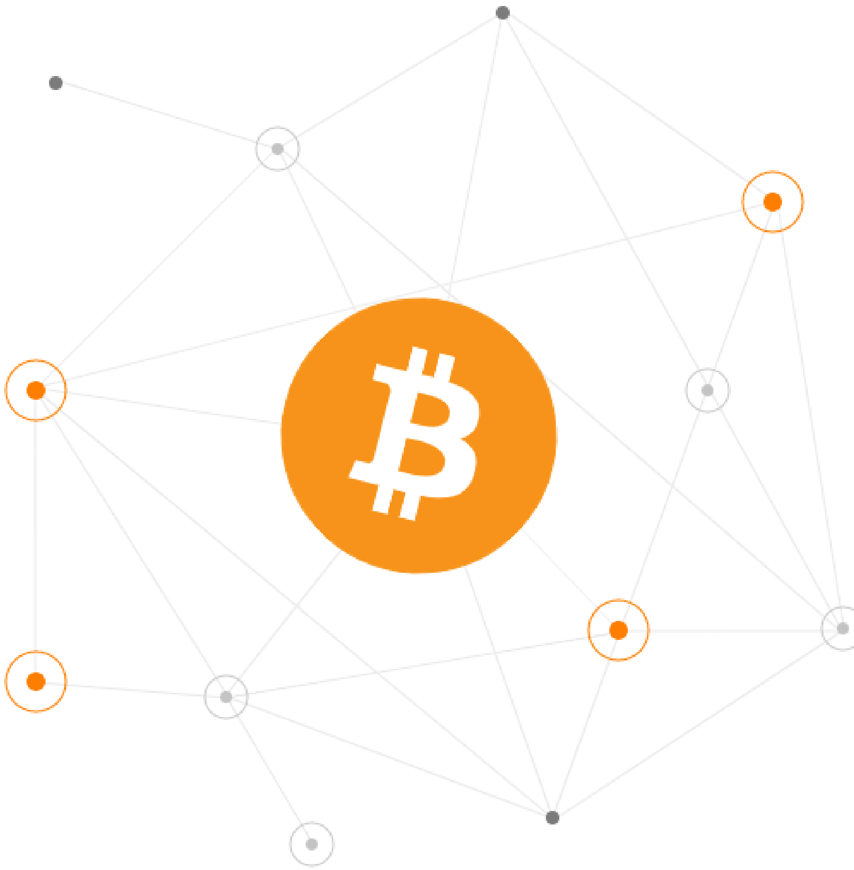
- ICO can be related to the ***Initial Public Offering*** (***IPO***), a way that companies used to raising money from the stock market.

- In IPOs, the public gives cash to the company in exchange with shares in that company, a way for them to raise their cash in order to fund further their operations.

Bitcoin

- ***Bitcoin*** is an **open-source** software that applies a **decentralized**, **peer-to-peer** e-cash payment system that does **not need** any trusted authorities to operate.

- Published by Satoshi Nakamoto in 2009 and was the first huge application on blockchain technology.



Source: bitcoin.org

Bitcoin Ecosystem

- The Bitcoin ecosystem include the following participants:
  - ***Nodes:*** The devices who participating in the network, but they do not participate in the mining process, they store, update, validate the chain.
  - ***Miners:*** Participants who are involved in the growing of the chain itself by mining, adding transactions into the blocks etc.
  - ***Large miners:*** Miners with a lot computational power and therefore big contribution to the growth of the chain (e.g., mining farms).
  - ***Mining Pools***: Combination of miners.

Transactions and UTXOs

- In cryptocurrency world the transactions are named as Unspent Transaction Outputs (UTXOs).

$$\left.\begin{array}{ll}\text{Alice} & \rightarrow \text{Me } 0.1 \text{ BTC}\\ \text{Jack} & \rightarrow \text{Me } 0.3 \text{ BTC}\\ \text{Nicol} & \rightarrow \text{Me } 0.6 \text{ BTC}\\ Carl & \rightarrow Me\ 0.5\ BTC\end{array}\right\} \text{UTXOs}$$

- The difference with the existing bank system’s transactions is that in Bitcoin transactions are live on after is been executed until another transactions builds off of the UTXOs.

Transactions Fees

- The rule is that anything that you do not account for becomes the fee for this transaction in order to be included in a block in the chain.

- This scheme come in contrast with the philosophy of blockchain, but since there are lot of transactions to be processed fee is working as motive for the miners to procced this transaction.

- Fees are calculated automatically with the rule of:

$$Fee = Input - Output$$

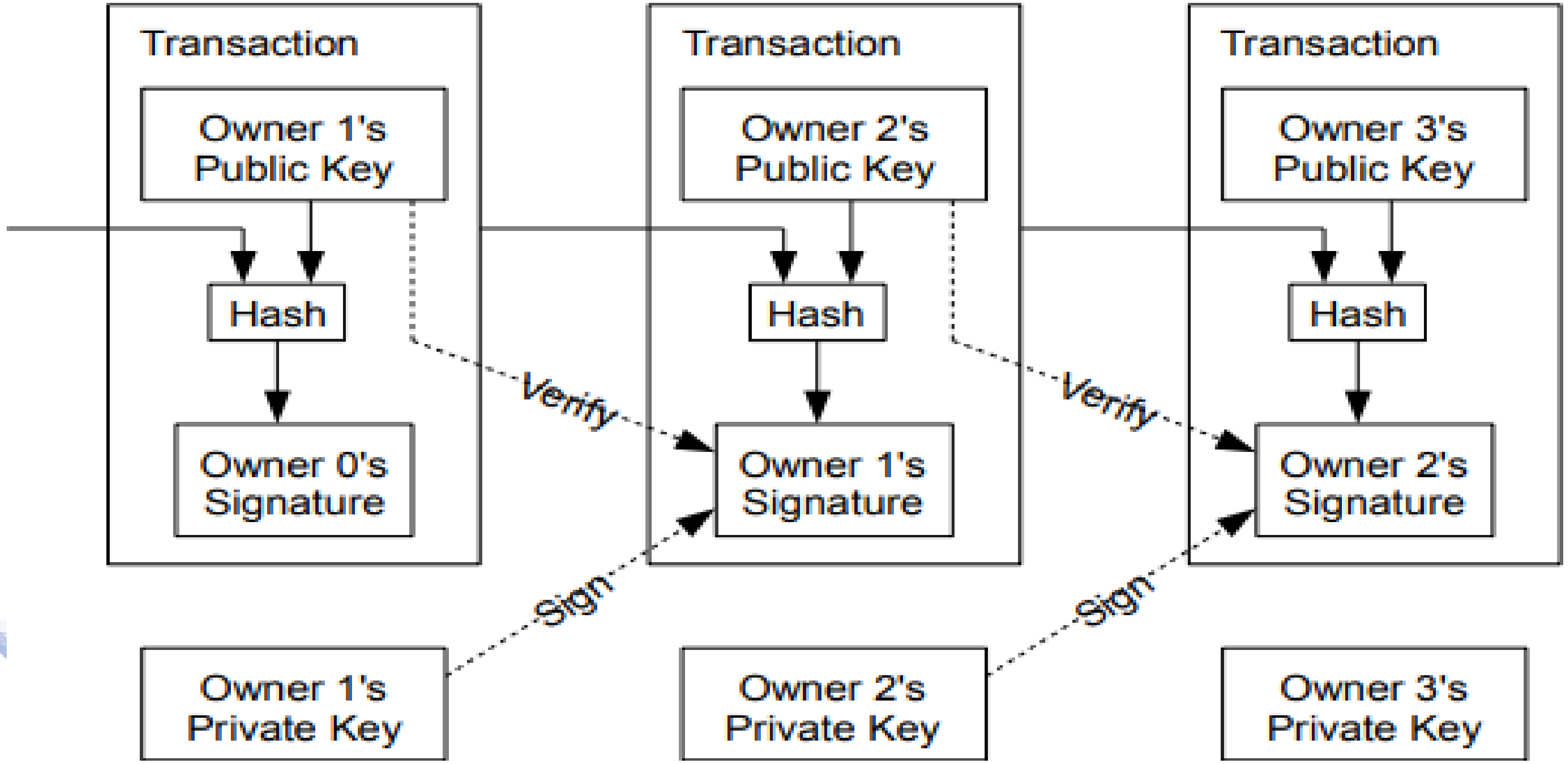
Digital Wallets

- As we see there is not exist an amount in blockchain but instead we have a list of UTXO transactions.

- Digital wallets is basically a type of account which is calculate the total UTXO that are available and name it as “balance”.

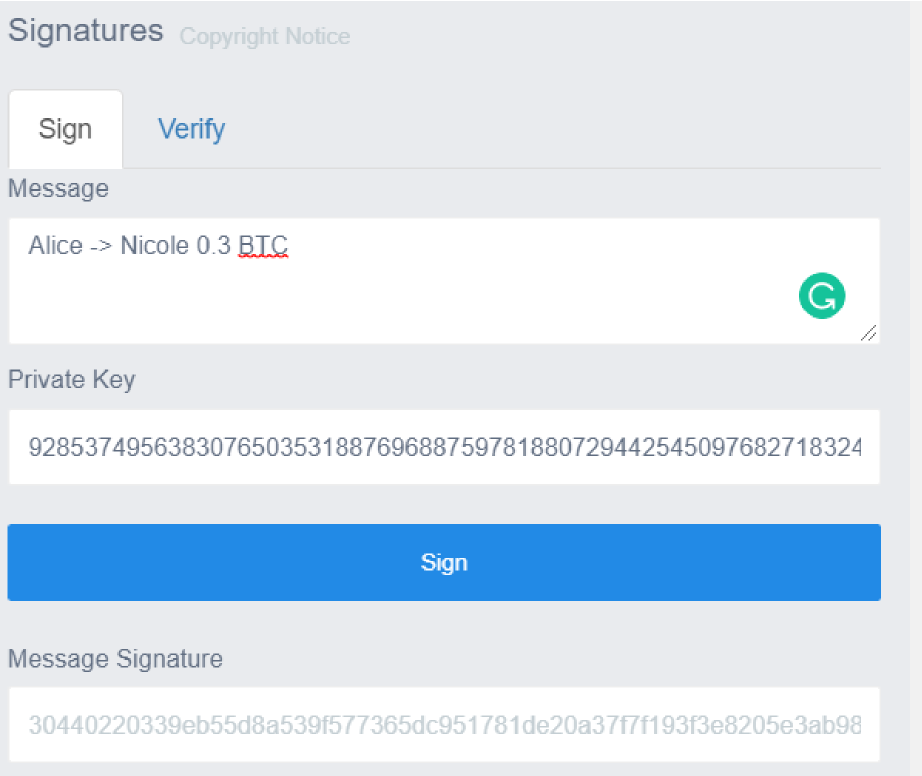
- What actually do is to scan across the blockchain and detect the transactions that is linked to the user and have the UTXO property and sum them up.

Bitcoin Signatures



Source: [NAK2008]

Bitcoin Signatures



Message

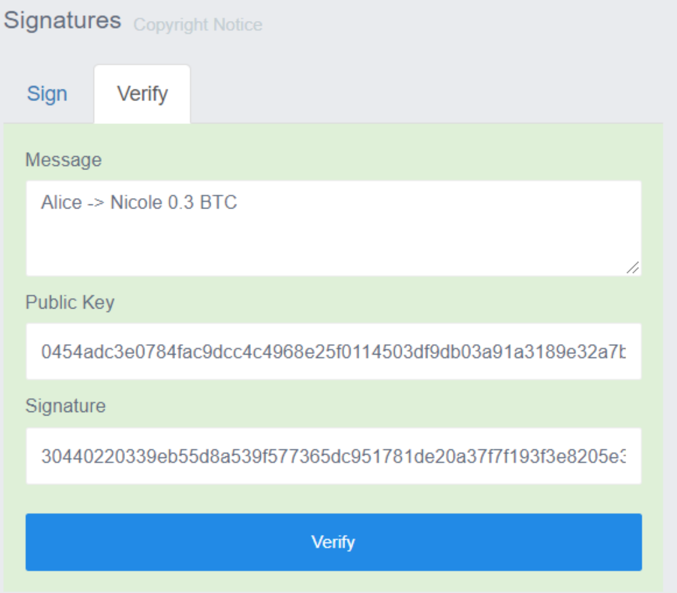
Alice -> Nicole 0.3 BTC

Private Key

928537495638307650353188769688759781880729442545097682718324

Message Signature

30440220339eb55d8a539f577365dc951781de20a37f7f193f3e8205e3ab98



Message

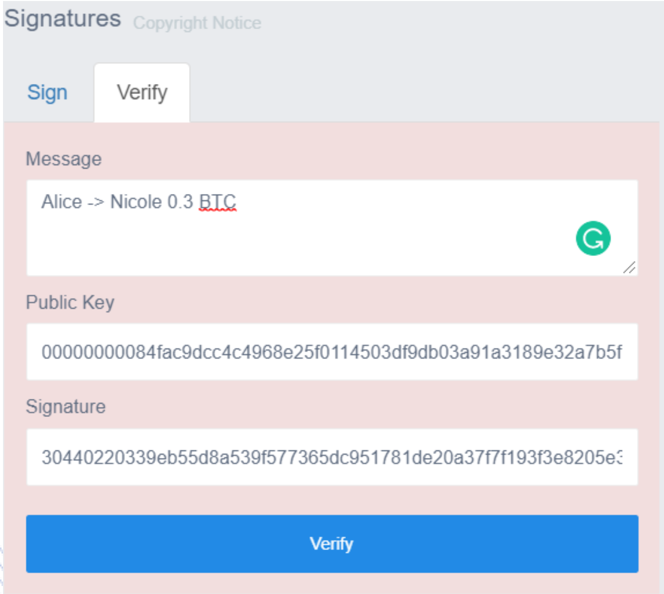
Alice -> Nicole 0.3 BTC

Public Key

0454adc3e0784fac9dcc4c4968e25f0114503df9db03a91a3189e32a7b

Signature

30440220339eb55d8a539f577365dc951781de20a37f7f193f3e8205e3



Message

Alice -> Nicole 0.3 BTC

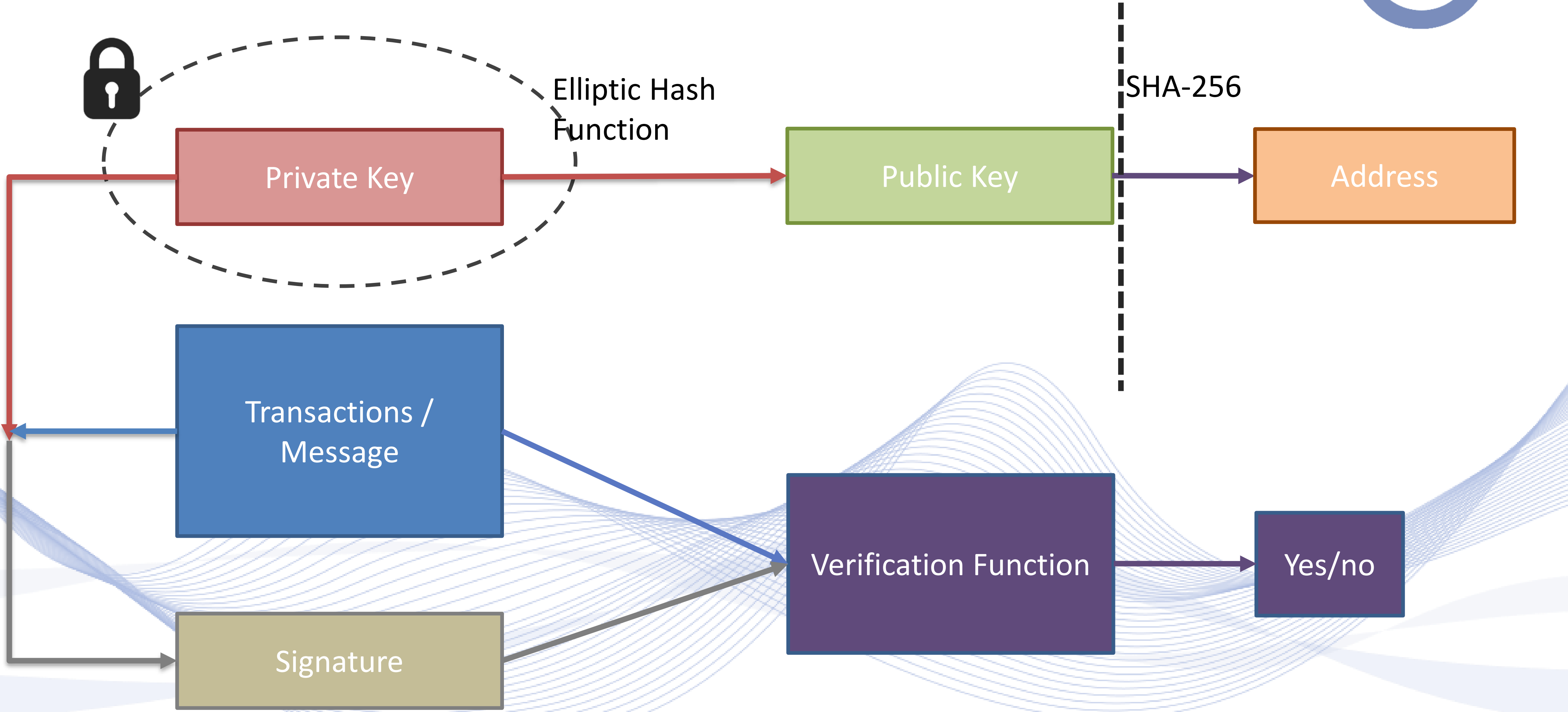
Public Key

00000000084fac9dcc4c4968e25f0114503df9db03a91a3189e32a7b5f

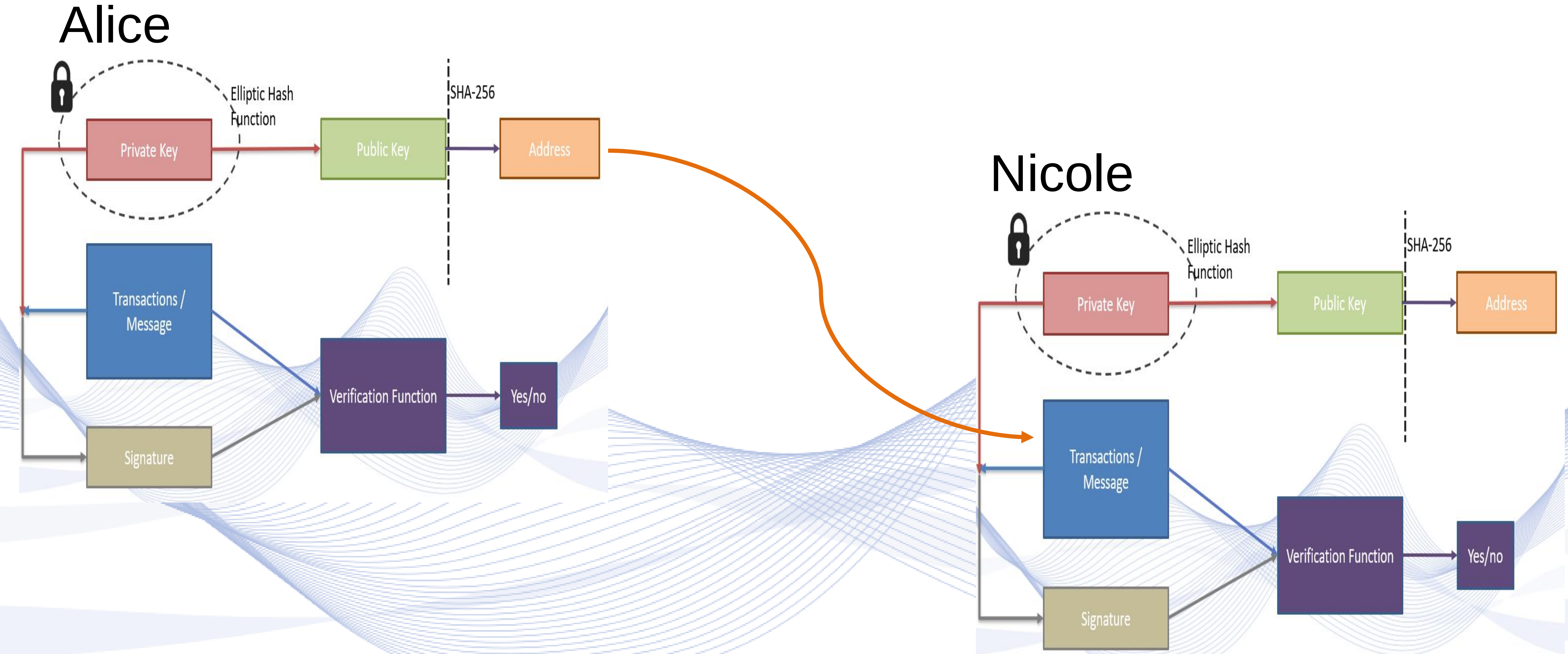
Signature

30440220339eb55d8a539f577365dc951781de20a37f7f193f3e8205e3

Bitcoin Address



Bitcoin Address

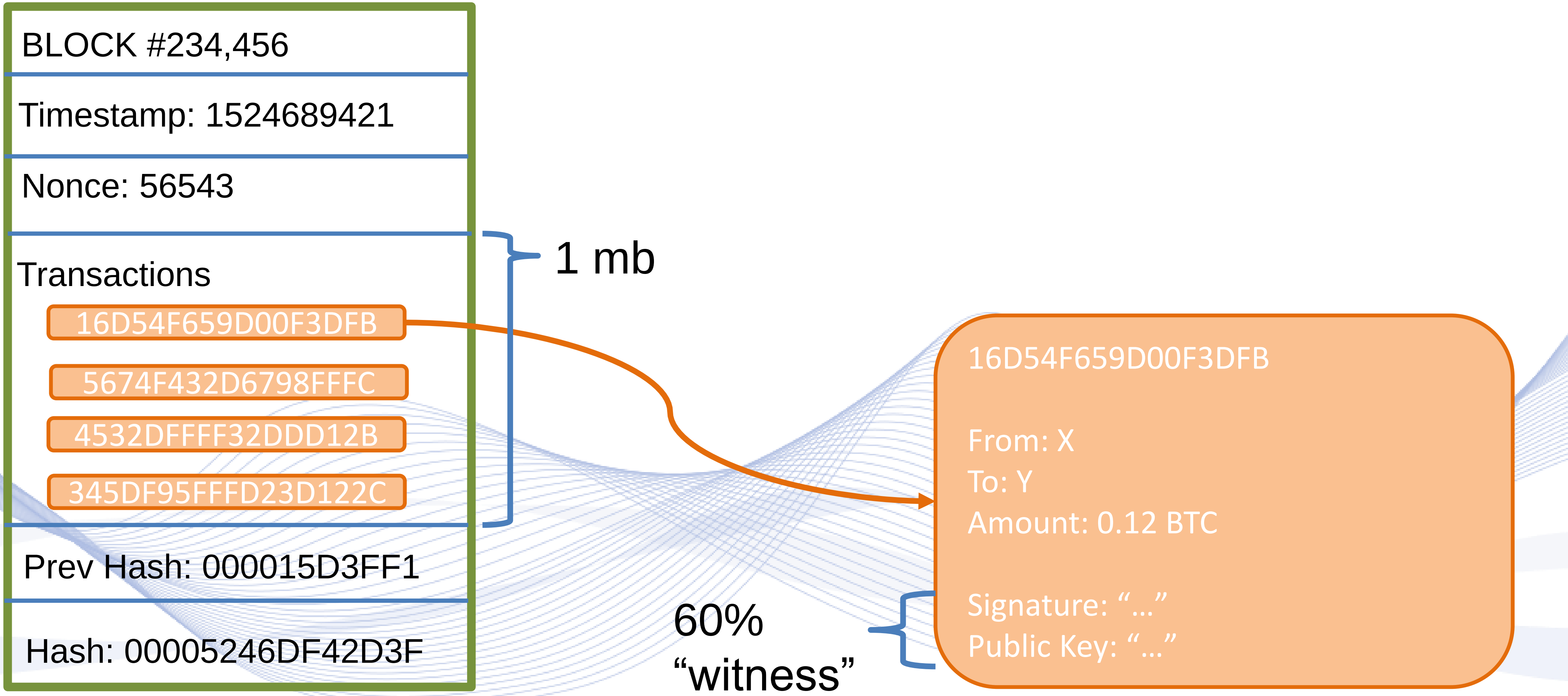


Segregate Witness

- Initial, a block in bitcoin network had a limit of $1mb$ transactions to be able to stored inside a block.

- One of the reason for that restriction is that:
  - If a block accept small number of transactions, then the network will occur with bandwidth problems since lot of participants will must wait long in order their transactions to be accepted.
  - On the other hand, if the block accept huge number of transactions that will slow down the network, since each block is shared with the whole network it will take long time a new information to propagate across all peers and this may result consensus issues.

Segregate Witness



BLOCK #234,456

Timestamp: 1524689421

Nonce: 56543

Transactions

- 16D54F659D00F3DFB
- 5674F432D6798FFFC
- 4532DFFFF32DDD12B
- 345DF95FFFD23D122C

Prev Hash: 000015D3FF1

Hash: 00005246DF42D3F

1 mb

16D54F659D00F3DFB

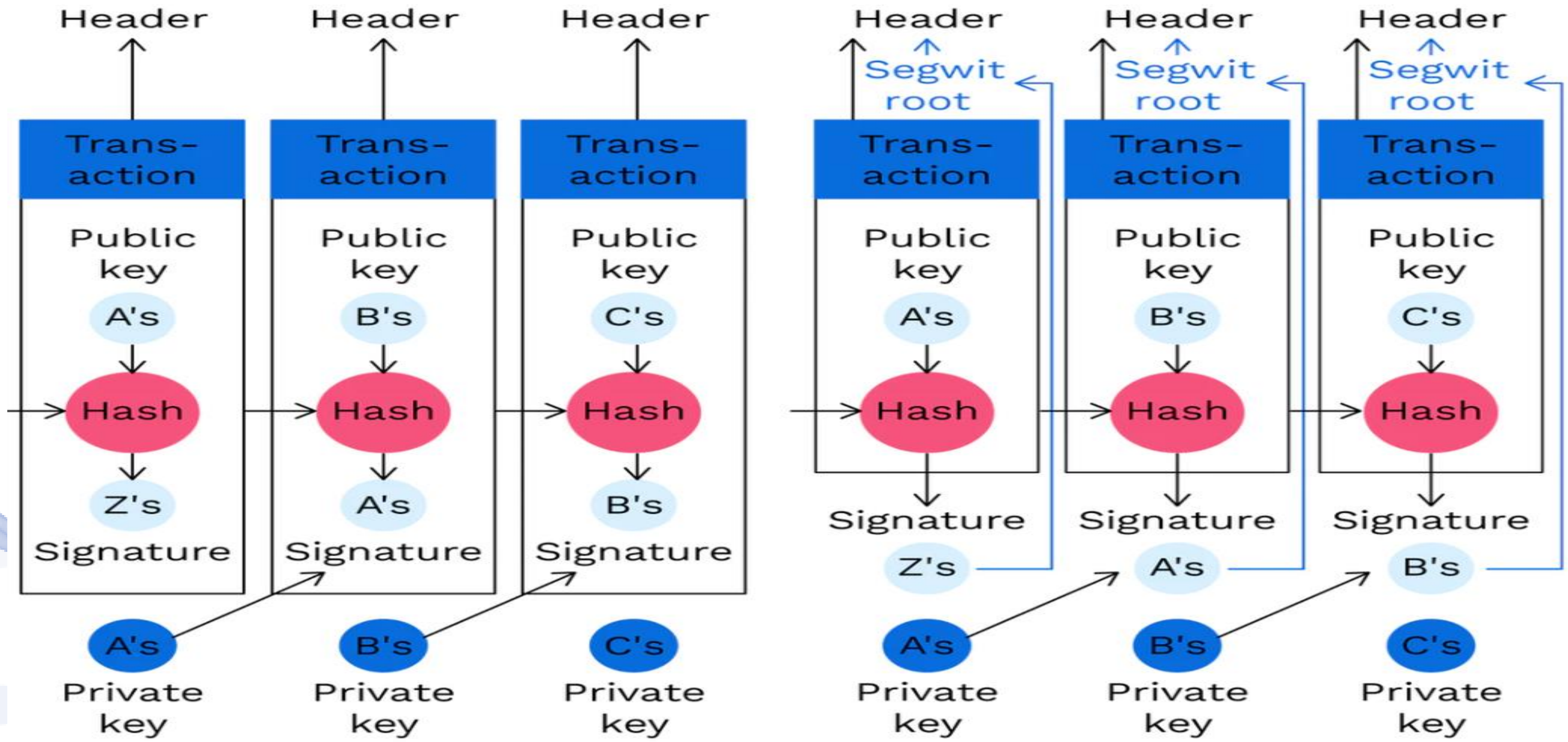
From: X
To: Y
Amount: 0.12 BTC

Signature: "…"
Public Key: "…"

60%
"witness"

Segregate Witness

Blocks (non SegWit) **Blocks (SegWit)**



Artificial Intelligence & Information Analysis Lab

Mining Pools

- Large Miners usually consist of huge facilities with thousand of ASIC rings so in order a normal user to be competitive and able to mine a nonce before those facilities the mining pools is invented.

- Here the miners can combine their processing power in the mining pool in order to solve the puzzle. What actually provide is a service where the cryptographic puzzle is distributed among the miners without doing a double work.

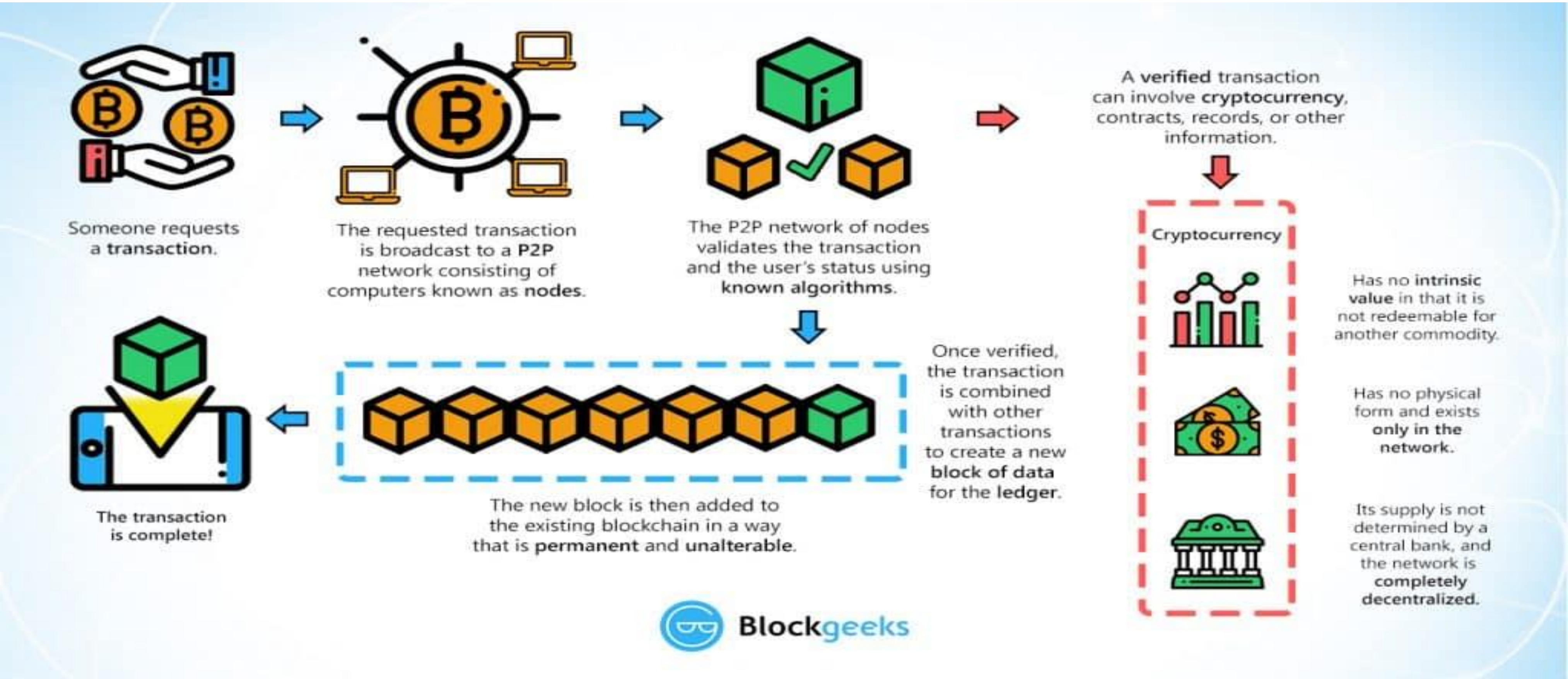
- It achieved distributing the nonce values between them until they find the winning one.

Bitcoin Proof of Work

- **Mining procedure:** Users perform a heavy computational task to prove that they are valid users. And as soon as the total computational power of the loyal users (nodes) is greater than (by 51%) the attackers, the network will maintain its consistency and the legal transactions will be performed.

- In bitcoin chain a mining procedure completes every 10 minutes. When the generation of a new block occurs then the miners are rewarded for their resource spent (electricity and power) with an amount of bitcoins.

Bitcoin



Someone requests a **transaction**.

The requested transaction is broadcast to a **P2P** network consisting of computers known as **nodes**.

The P2P network of nodes validates the transaction and the user's status using **known algorithms**.

A **verified** transaction can involve **cryptocurrency**, contracts, records, or other information.

Has no **intrinsic value** in that it is not redeemable for another commodity.

Has no physical form and exists **only in the network**.

Its supply is not determined by a central bank, and the network is **completely decentralized**.

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

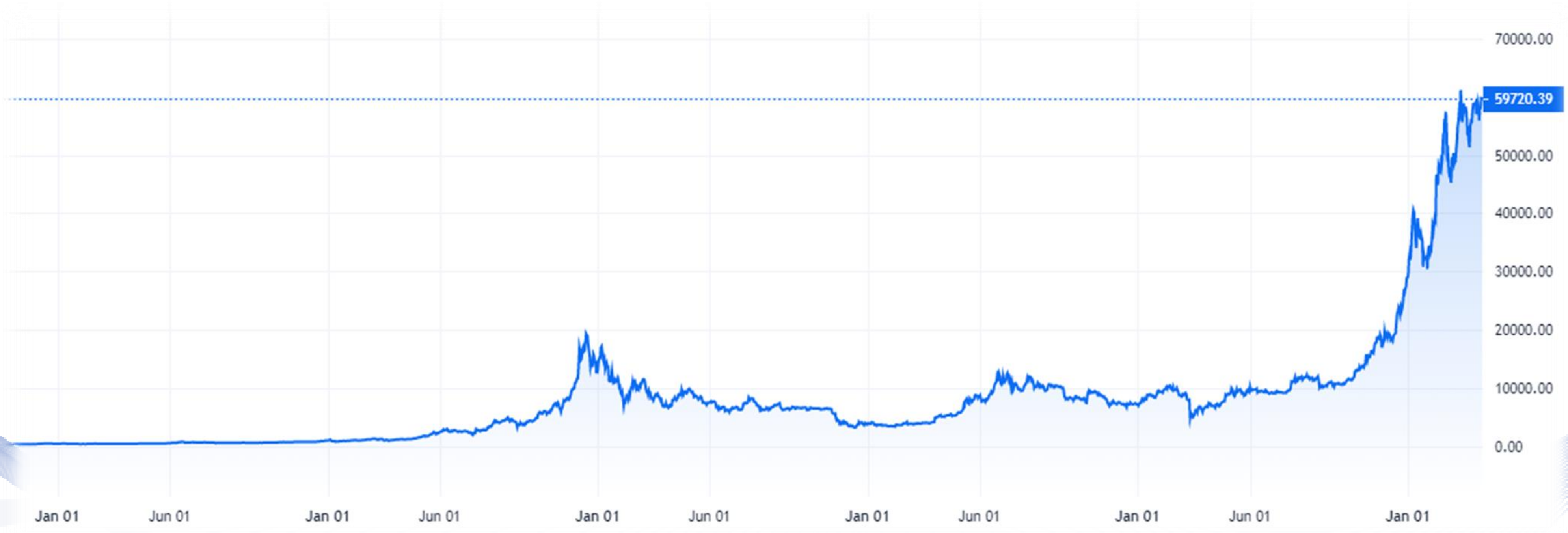
The new block is then added to the existing blockchain in a way that is **permanent** and **unalterable**.

The transaction is complete!

Bitcoin Transaction Process.

Source: [ROS2018]

Bitcoin



Bitcoin rising of value from 2016 till 2021.

Source: blockchain.com

Ethereum

- ***Ethereum*** is a type of chain that uses a ***built-in*** programming language, where everyone has the permission to write decentralized apps and smart contracts. In this way participants design their own rules for ***ownership***, ***state transition functions*** and ***transaction formats***. Smart contract is essentially for that structure.

- ***Ether*** is the cryptocurrency which is designed to be rewarded in the honest nodes of the chain.

Source: Wikipedia.org

Ethereum Accounts

- State of Ethereum is made upon “accounts” which consist of $20-byte$ address and informations can be directly transferred between accounts using the state of transitions. Such account contains:
  - **Nonce**, involved to ensure that transactions are executed only once.
  - **The balance** of the ether’s account.
  - **Contract code** for this account.
  - **Storage** of the account.

Artificial Intelligence & Information Analysis Lab

Ethereum Accounts

- ***Account types:***
  - ***Externally owned accounts:*** One can send message via transactions, no code available, and it use private keys.

  - ***Contract Accounts:*** Once it receives a message the code is activated, permission is given in order to read or send to others or to design contracts in turn, control achieved by their contract code.

Smart Contracts Limitations

- Ethereum Blockchain is designed not as a cryptocurrency but as a platform where everyone can build on top of others, decentralized applications through the execution of smart contracts.

- But since smart contracts are tuning-complete we have the follow security threats:
  - Virus and privacy issue
  - Infinite loops.

Artificial Intelligence & Information Analysis Lab

GAS and Ether

- GAS is not Ether but since the currency of the Ethereum network is Ether there is a conversion rate that converts the GAS to Ether.

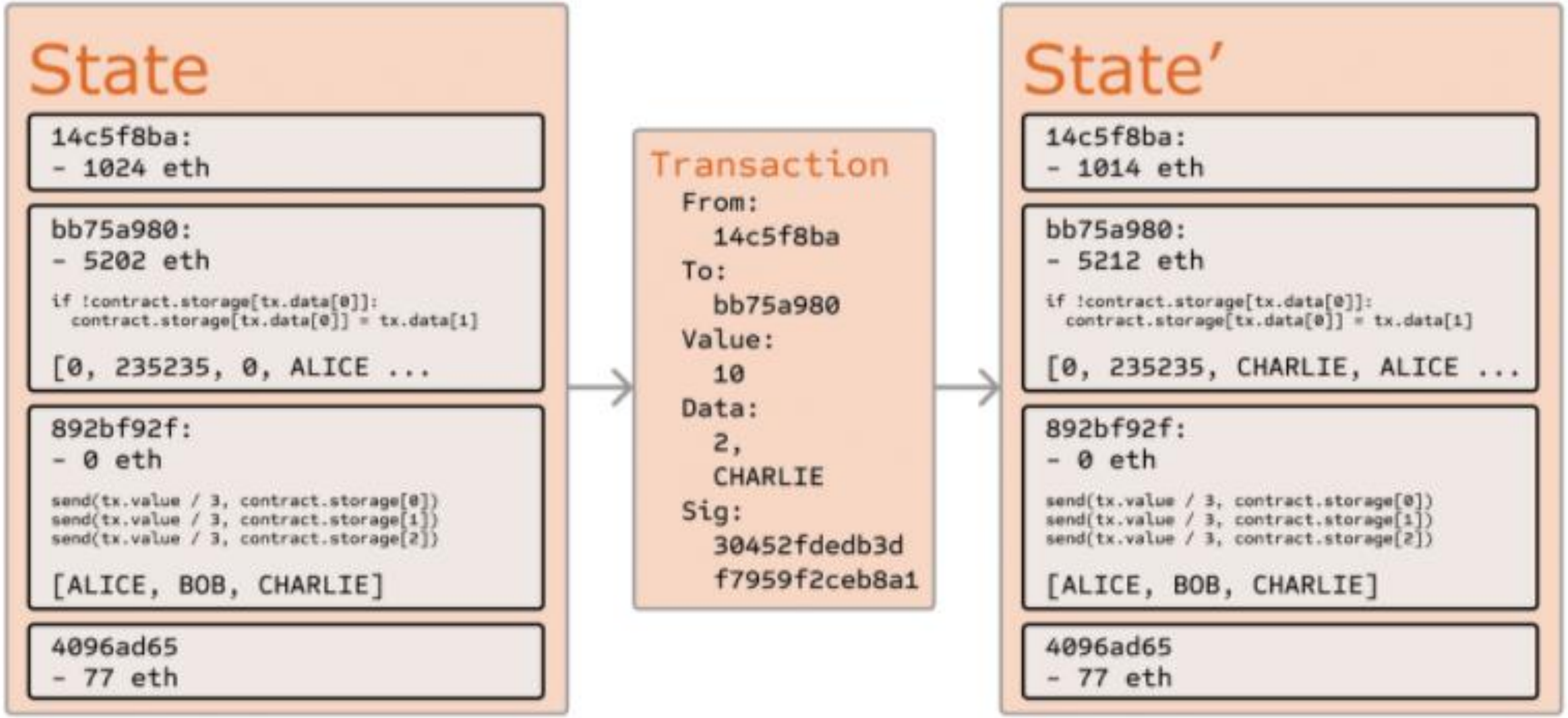
- This conversion rate is decided by a community consensus in the network, since the whole system is decentralized.

- And that’s the core difference with Bitcoin. Ethereum is not just a chain for cryptocurrency like bitcoin, but essentially is a network where participants can run code in blockchain by paying in Ether and therefore to create applications that will run on the blockchain.

Message and Transactions

- **Transactions implements:**
  - The recipient of the message.
  - Sender’s identification signature.
  - Amount of ethers need to be transferred among sender and receiver.
  - An optimal data field.
  - ***STARTGAS*** value, which contains the maximum computational steps allowed by the transaction to execute.
  - ***GASPRICE*** value, containing the fee which must pay the sender for each computational step.

Message and Transactions



State

```
14c5f8ba:
- 1024 eth
```

```
bb75a980:
- 5202 eth

if !contract.storage[tx.data[0]]:
  contract.storage[tx.data[0]] = tx.data[1]

[0, 235235, 0, ALICE ...
```

```
892bf92f:
- 0 eth

send(tx.value / 3, contract.storage[0])
send(tx.value / 3, contract.storage[1])
send(tx.value / 3, contract.storage[2])

[ALICE, BOB, CHARLIE]
```

```
4096ad65
- 77 eth
```

Transaction

```
From:
  14c5f8ba
To:
  bb75a980
Value:
  10
Data:
  2,
  CHARLIE
Sig:
  30452fdedb3d
  f7959f2ceb8a1
```

State'

```
14c5f8ba:
- 1014 eth
```

```
bb75a980:
- 5212 eth

if !contract.storage[tx.data[0]]:
  contract.storage[tx.data[0]] = tx.data[1]

[0, 235235, CHARLIE, ALICE ...
```

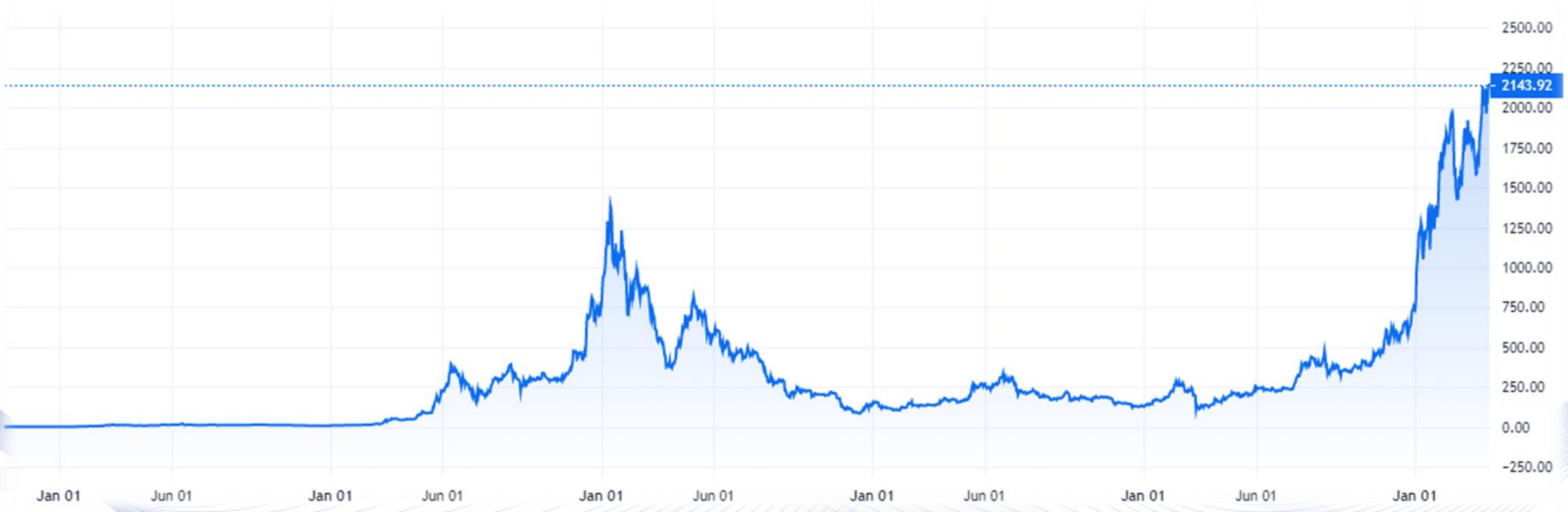
```
892bf92f:
- 0 eth

send(tx.value / 3, contract.storage[0])
send(tx.value / 3, contract.storage[1])
send(tx.value / 3, contract.storage[2])

[ALICE, BOB, CHARLIE]
```

```
4096ad65
- 77 eth
```

Example of transaction process.

Source: [BUT2013]

Ethereum Blockchain



Ether value from 2016 till 2021.

Source: Blockchain.com

Bibliography

[MAS2017] Maqsood, Faiqa, et al. "Cryptography: a comparative analysis for modern techniques." International Journal of Advanced Computer Science and Applications 8.6 (2017): 442-448.

[RAI2019] M. Raikwar, D.Gligoroski and K. Kralevska, "SoK of Used Cryptography in Blockchain,“ in IEEE Access, vol. 7, pp. 148550-148575, 2019, doi: 10.1109/ACCESS.2019.2946983.

[ZHA2019] S.Zhai, Yang, Yuanyuan, Li, Jing, Qiu, Cheng, Zhao, Jiangming, “Research on the Application of Cryptography on the Blockchain”, Journal of Physics: Conference Series, Feb 2019.

[ZHE2018] Zheng, Zibin & Xie, Shaoan & Dai, Hong-Ning & Chen, Xiangping & Wang, Huaimin. (2018). Blockchain challenges and opportunities: A survey. International Journal of Web and Grid Services. 14. 352. 10.1504/IJWGS.2018.095647.

[NOF2017] Nofer, M., Gomber, P., Hinz, O. et al. Blockchain. Bus Inf Syst Eng 59, 183–187 (2017).

[ACH2019] V. Acharya, A.Eswararao Yerrapati, N. Prakash, “Oracle Blockchain Quick Start Guide”, September 2019.

[REJ2021] Rejeb, Abderahman & Rejeb, Karim & Keogh, John. (2021). Centralized vs. decentralized ledgers in the money supply process: a SWOT analysis. Quantitative Finance and Economics.

Bibliography

[BAS2018] I. Bashir, (2018). ”Mastering Blockchain: Distributed ledger technology”, decentralization, and smart contracts explained, 2nd Edition.

[YAN2019] Yang Lu, “The blockchain: State-of-the-art and research challenges”, Journal of Industrial Information Integration, Volume 15, 2019, Pages 80-90,ISSN 2452-414X.

[CUR2019] B.Curran, “What is Practical Byzantine Fault Tolerance? Complete Beginner’s Guide”, April 18, 2020.

[CAS1999] M.Castro, B.Liskov, 1999, “Practical Byzantine fault tolerance”. In Proceedings of the third symposium on Operating systems design and implementation (OSDI '99). USENIX Association, USA, 173–186.

[FER2020] Ferdous, Md. Sadek & Chowdhury, Mohammad & Hoque, Mohammad & Colman, Alan. (2020). Blockchain Consensus Algorithms: A Survey.

[BAC2018] L. M. Bach, B. Mihaljevic and M. Zagar, "Comparative analysis of blockchain consensus algorithms," 2018 41st International Convention on Information and Communication Technology, Electronics and Microelectronics (MIPRO), Opatija, Croatia, 2018, pp. 1545-1550.

Bibliography

[FU2021] Fu, X., Wang, H. & Shi, P. A survey of Blockchain consensus algorithms: mechanism, design and applications. Sci. China Inf. Sci. 64, 121101 (2021).

[VUJ2018] D. Vujičić, D. Jagodić and S. Ranđić, "Blockchain technology, bitcoin, and Ethereum: A brief overview," 2018 17th International Symposium INFOTEH-JAHORINA (INFOTEH), East Sarajevo, Bosnia and Herzegovina, 2018, pp. 1-6.

[NAK2008] S. Nakamoto, 'Bitcoin: A peer-to-peer electronic cash system', Decentralized Business Review, 2008.

[BUT2013] V. Buterin, "Ethereum white paper: a next generation smart contract & decentralized application platform," 2013.

[DUN2018] P. Dunphy and F. A. P. Petitcolas, "A First Look at Identity Management Schemes on the Blockchain," in IEEE Security & Privacy, vol. 16, no. 4, pp. 20-29, July/August 2018.

[GAR2018]P. Dunphy, L. Garratt and F. Petitcolas, "Decentralizing Digital Identity: Open Challenges for Distributed Ledgers," 2018 IEEE European Symposium on Security and Privacy Workshops (EuroS&PW), London, UK, 2018, pp. 75-78.

Bibliography

[DEL2020] Delgado Mohatar, Oscar & Fierrez, Julian & Tolosana, Ruben & Vera-Rodriguez, Ruben. (2020). Blockchain meets Biometrics: Concepts, Application to Template Protection, and Trends.

[COS2020] Cos, “Bitcoin’s Proof of Work: The problem of the Byzantine Generals’”, medium,(2020).

[CHA2019] C. Rizos, “Blockchain Consensus Algorithms”, 2019.

[ROS2018] A. Rosic, “What is Blockchain Technology?”, Blockgeeks, 2016, 2018.

[LI2020] W. Li, H. Guo, M. Nejad and C. -C. Shen, "Privacy-Preserving Traffic Management: A Blockchain and Zero-Knowledge Proof Inspired Approach," in *IEEE Access*, vol. 8, pp. 181733-181743, 2020, doi: 10.1109/ACCESS.2020.3028189.

Q & A

Thank you very much for your attention!

More material in
http://icarus.csd.auth.gr/cvml-web-lecture-series/

Contact: Prof. I. Pitas
pitas@csd.auth.gr