CRYPTOGRAPHIC TOOLS FOR BLOCKCHAIN

"Nothing is lost,
nothing is created,
everything is transformed"

By:

Corina Dimitriu

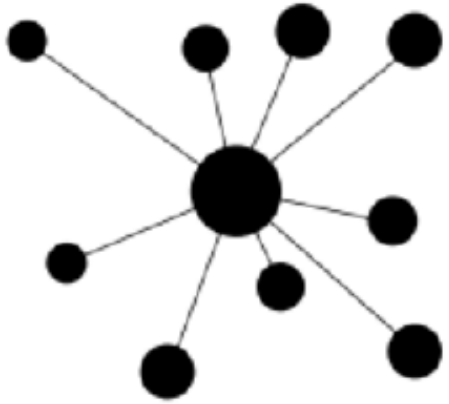
Bianca Buzila

Leonard Rumeghea

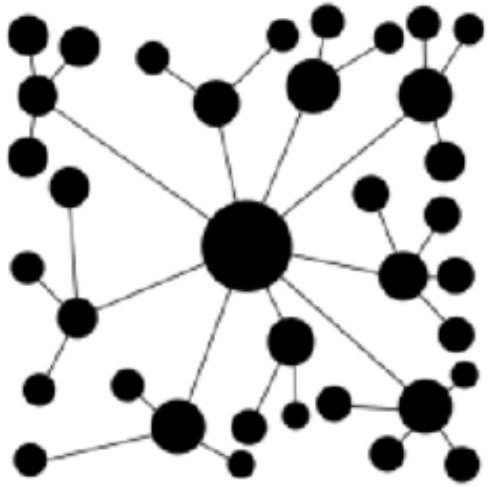
- Blockchain technology came into being through the financial domain as a means to transfer digital resources between two endpoints without intervention from a central unit.

- Blockchain does not have an almighty owner or controller, which makes all the nodes in the network both activity monitors and activity executors.

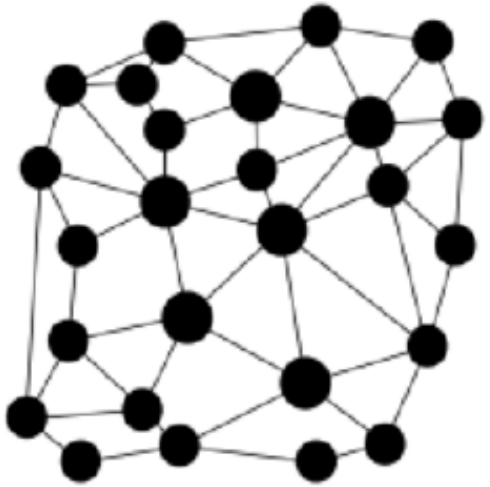
- The blockchain architecture requires powerful computers, with large storage capacity.



A centralized network.



A decentralized network.



A distributed network.

❖ Most well-known example: Bitcoin

- According to the Bitcoin mining policy, users (associated to computers) posses private keys in order to identify themselves when announcing in the network the exact amount of BTC they aim to send.

- The process of sharing transaction details with the other endpoints may be perceived as an integrity guarantee.

- The confidence of participants guarantee is given by the unchangeable and irreversible nature of transactions

1

- The blockchain architecture comprises many layers. Having the next 4 of them is usually considered common practice:

Application layer
Consensus layer
Network layer
Data layer: hash functions, Merkle trees

- https://app.diagrams.net/#G1m7h72e6QbiisaeSWorC3bu9-odf0gxKN
- There are 6 security-oriented elements which form the foundation of blockchain, namely:

Decentralization

Immutability

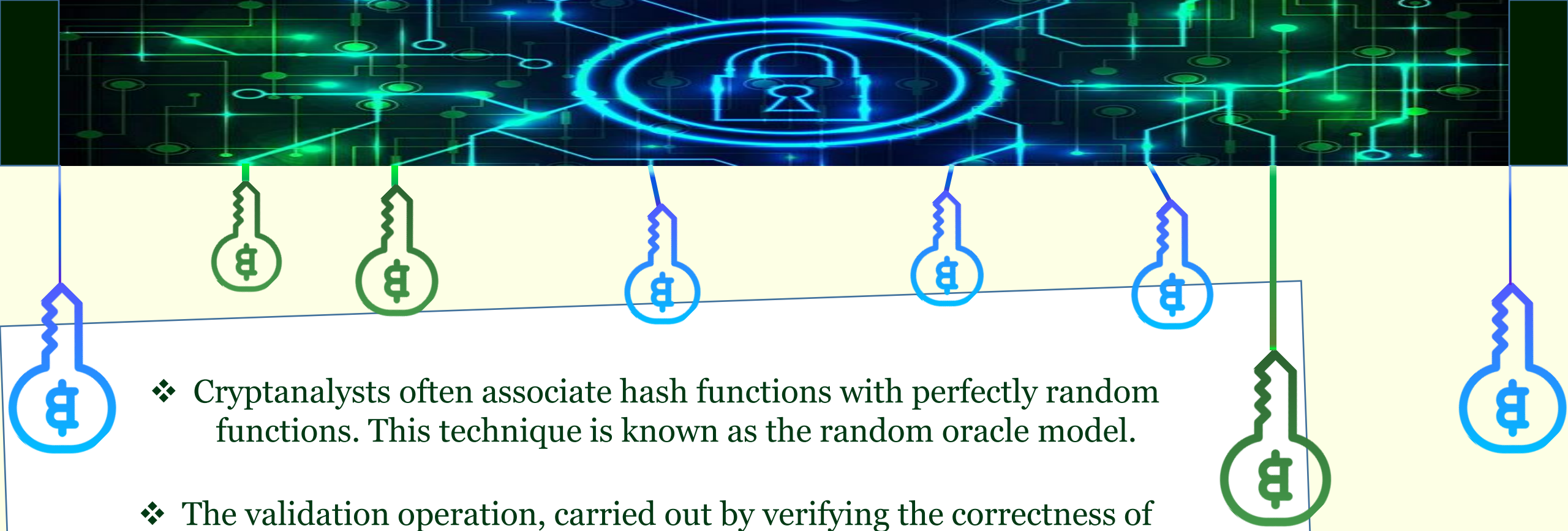
Transparency

Anonymity

Distributed ledgers

Consensus

- Blockchain system's security is usually discussed with respect to the CIA (Confidentiality, Integrity, Availability) triad

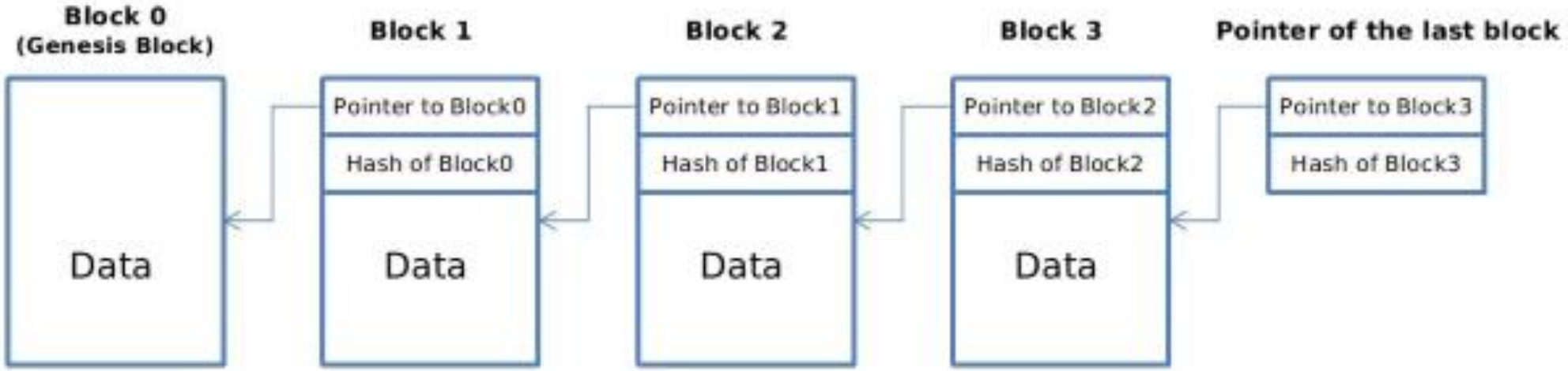


- Cryptanalysts often associate hash functions with perfectly random functions. This technique is known as the random oracle model.

- The validation operation, carried out by verifying the correctness of block sequences, gives an insight into the reason why blocks are actually chained.

- Bitcoin and other cryptocurrencies uniquely identify coin transfer participants through hashes of their public keys, which are conceptually transformed into endpoint addresses.

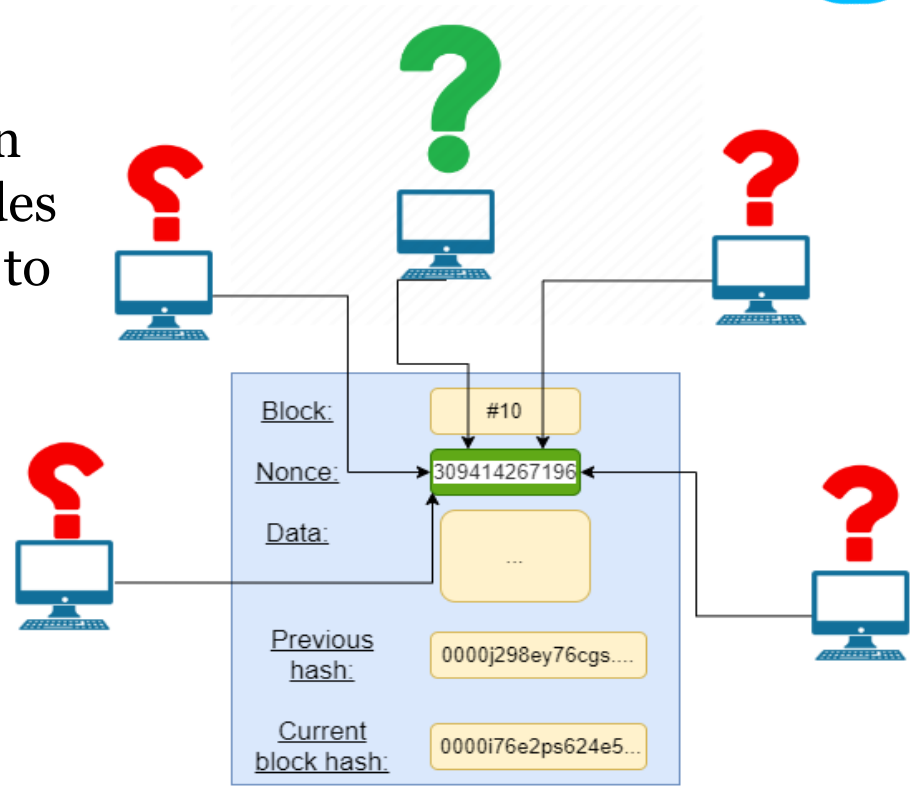
- Filling a transaction block is immediately followed by chaining it into the ledger of the targeted system.
- The validation step results in participants indirectly validating the entire chain.



2

- The nonce serves as a decision instrument to the unbiased selection of the ”validators” from the other nodes in the network: miners are supposed to make a ”collective effort” to guess the nonce.

- It is computationally impossible to edit a previous block without reversing the chained hashing process. (one-wayness property)



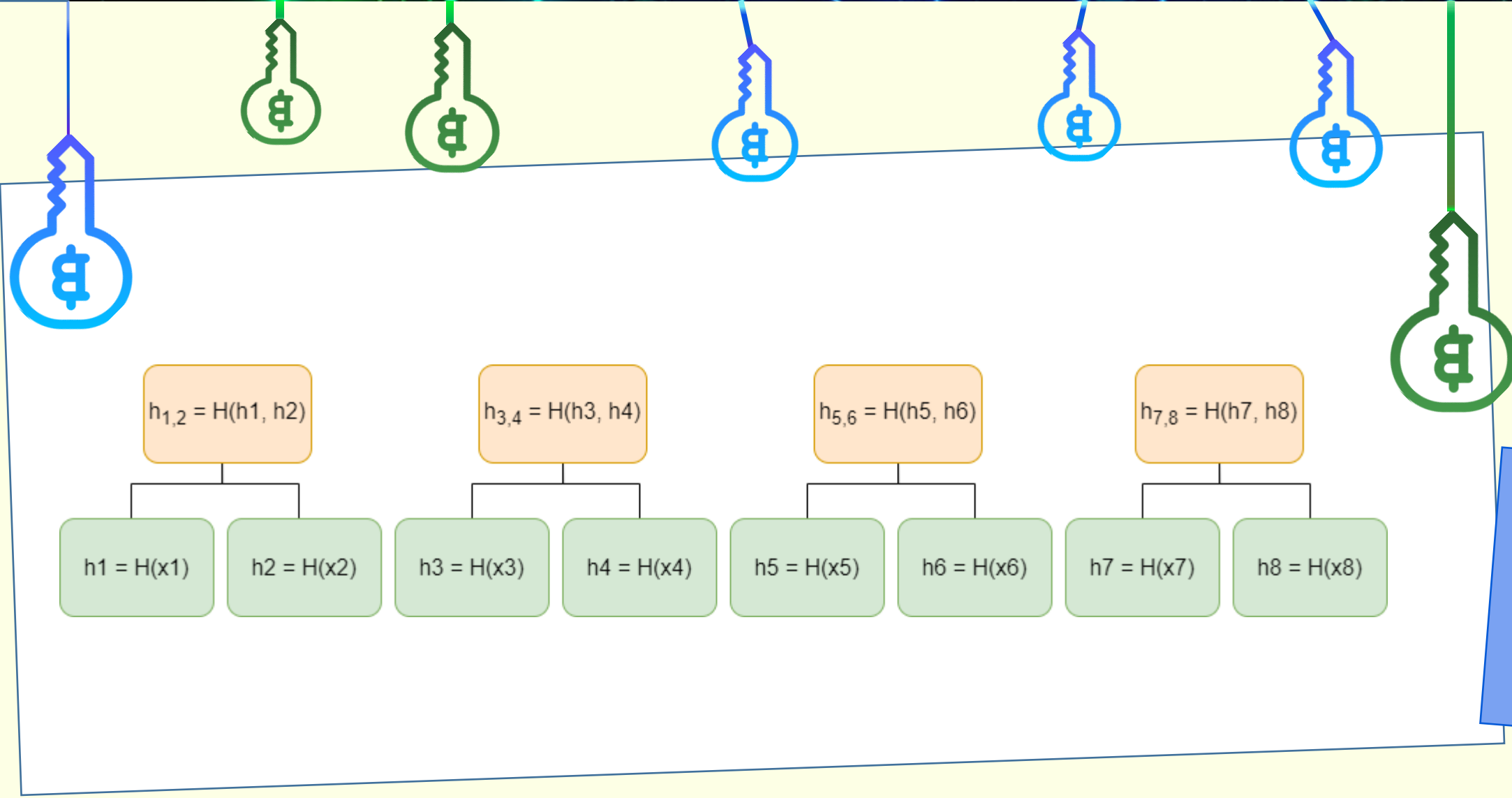
- A Merkle tree might be seen as a (hash) function that requires n parameters as input and outputs a Merkle tree root hash. The tree is usually denoted by MHT.

- The example below represents the way a Merkle tree which takes 8 files/data containers as input is built.

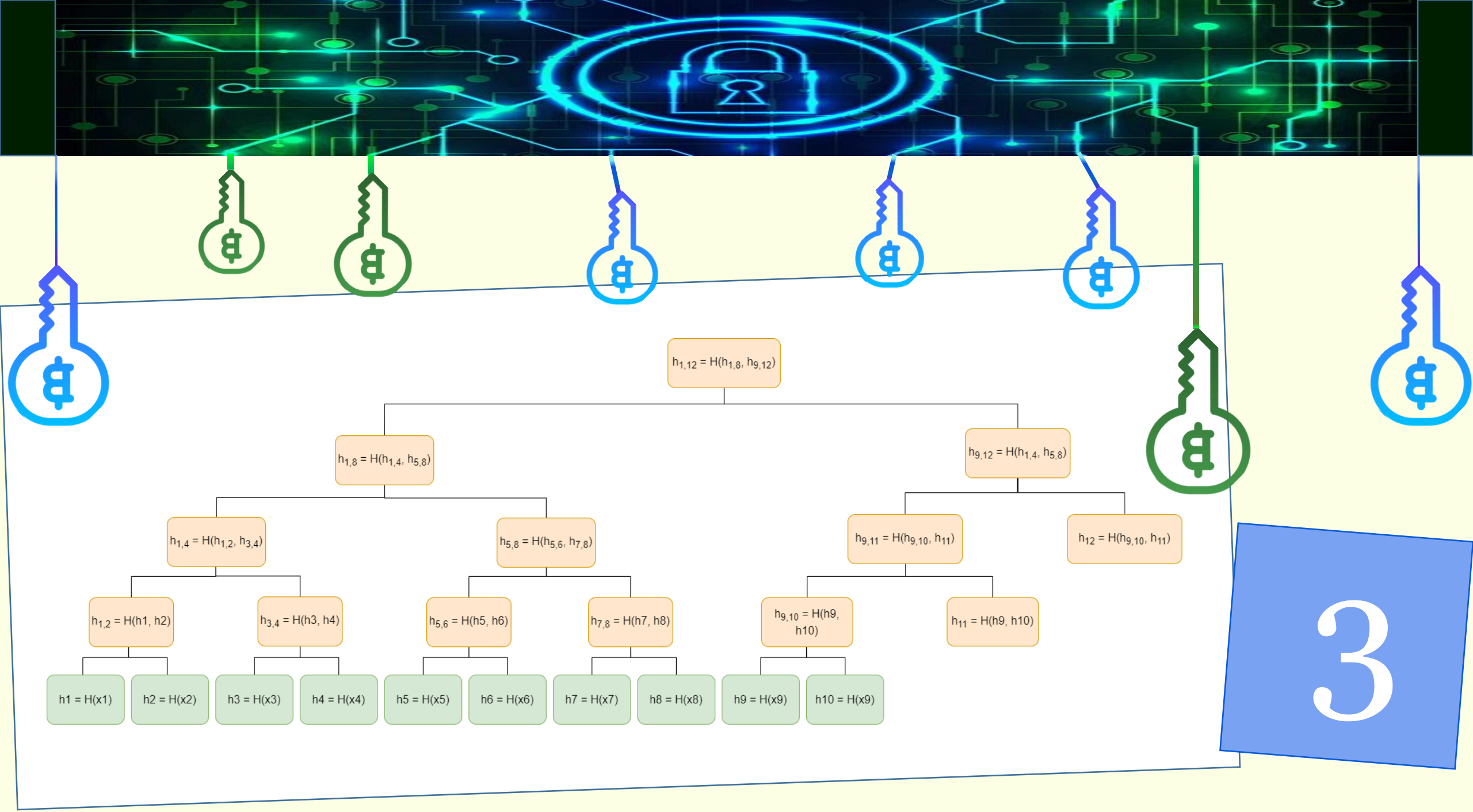
- If there is an odd number of hashes on the previous level (on any level of the tree except the root), the rightmost previously obtained hash is duplicated.

h1 = H(x1) | h2 = H(x2) | h3 = H(x3) | h4 = H(x4) | h5 = H(x5) | h6 = H(x6) | h7 = H(x7) | h8 = H(x8)

3


$h_{1,2}$ = H(h1, h2)
$h_{3,4}$ = H(h3, h4)
$h_{5,6}$ = H(h5, h6)
$h_{7,8}$ = H(h7, h8)
h1 = H(x1)
h2 = H(x2)
h3 = H(x3)
h4 = H(x4)
h5 = H(x5)
h6 = H(x6)
h7 = H(x7)
h8 = H(x8)

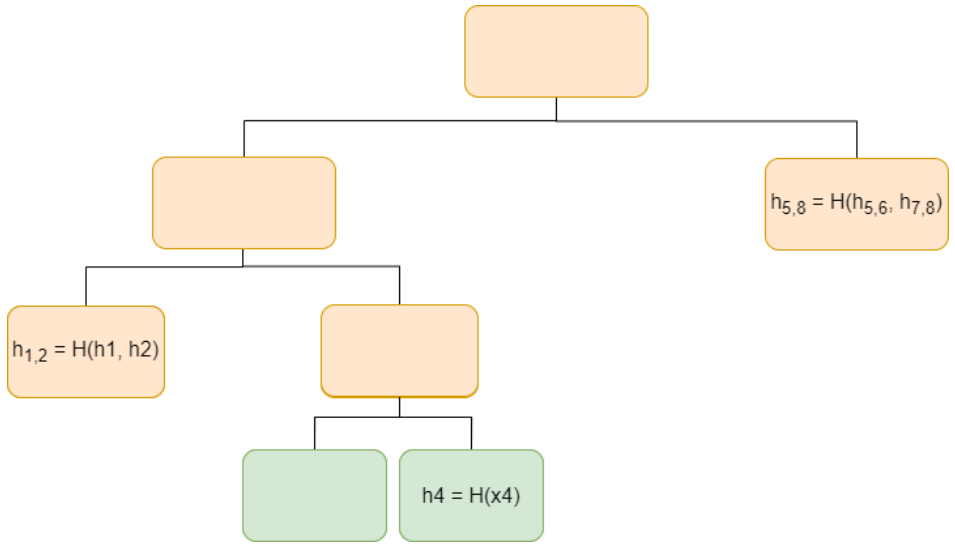
3

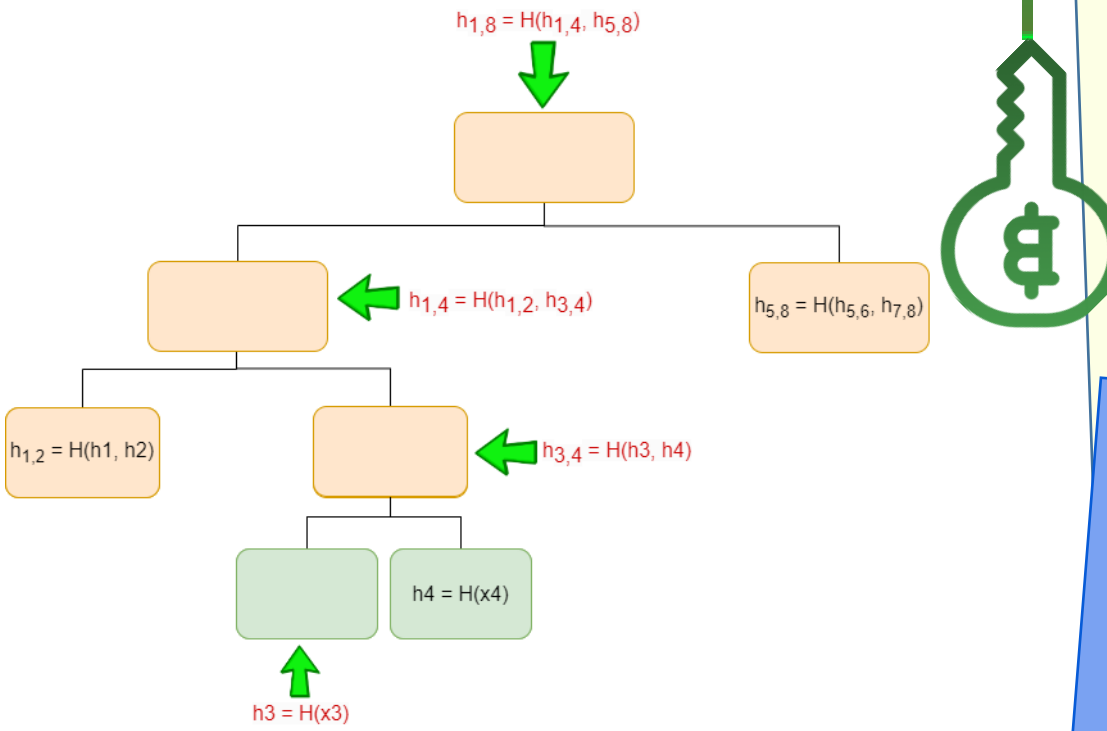

$h_{1,12} = H(h_{1,8}, h_{9,12})$
$h_{1,8} = H(h_{1,4}, h_{5,8})$
$h_{9,12} = H(h_{1,4}, h_{5,8})$
$h_{1,4} = H(h_{1,2}, h_{3,4})$
$h_{5,8} = H(h_{5,6}, h_{7,8})$
$h_{9,11} = H(h_{9,10}, h_{11})$
$h_{12} = H(h_{9,10}, h_{11})$
$h_{1,2} = H(h1, h2)$
$h_{3,4} = H(h3, h4)$
$h_{5,6} = H(h5, h6)$
$h_{7,8} = H(h7, h8)$
$h_{9,10} = H(h9, h10)$
$h_{11} = H(h9, h10)$
h1 = H(x1)
h2 = H(x2)
h3 = H(x3)
h4 = H(x4)
h5 = H(x5)
h6 = H(x6)
h7 = H(x7)
h8 = H(x8)
h9 = H(x9)
h10 = H(x9)
3

- The basic and most significant use of Merkle trees refers to the file integrity problem, but also to the storage problem.

- Eventually, it all boils down to searching in a Merkle tree.
The root hash is somehow made public so as it is known by both the personal computer and the platform.

- After download, the receiver (the computer) asks for a Merkle proof.
h4, $h_{1,2}$, $h_{5,8}$ forms the Merkle path for the leaf x3.


$h_{5,8} = H(h_{5,6}, h_{7,8})$
$h_{1,2} = H(h1, h2)$
h4 = H(x4)

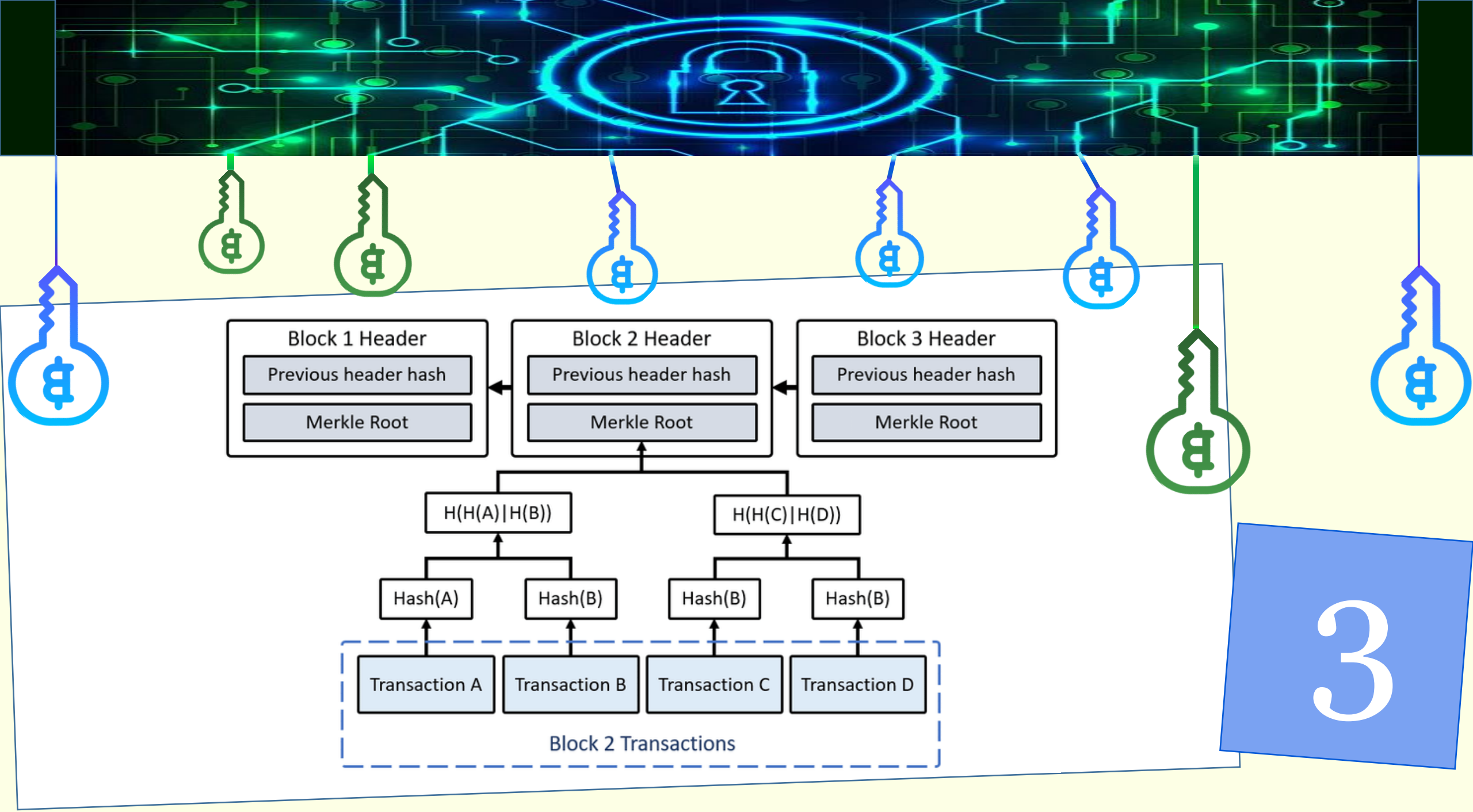

$h_{1,8} = H(h_{1,4}, h_{5,8})$
$h_{1,4} = H(h_{1,2}, h_{3,4})$
$h_{5,8} = H(h_{5,6}, h_{7,8})$
$h_{1,2} = H(h1, h2)$
$h_{3,4} = H(h3, h4)$
h4 = H(x4)
h3 = H(x3)

3

- The key in the Merkle proof's structure is given by the fact that the information they provide suffices to re-compute all the missing hashes, all the way up to the root hash, which is therefore compared to the pre-existing Merkle root.

- Proving that a transaction belongs to the Merkle root in its header is achieved through the use of Merkle proofs.

- Merkle trees succeed in creating a digital fingerprint for the entire collection of transactions, so that all the nodes (as endpoints/miners) in the network, both full and lightweight, stay up-to-date with consistent information.


Block 1 Header
Previous header hash
Merkle Root
Block 2 Header
Previous header hash
Merkle Root
Block 3 Header
Previous header hash
Merkle Root
H(H(A)|H(B))
H(H(C)|H(D))
Hash(A)
Hash(B)
Hash(B)
Hash(B)
Transaction A
Transaction B
Transaction C
Transaction D
Block 2 Transactions

3

- Immutability is preserved: A change in one transaction in the record (and, thus, in that transaction's hash) would trigger changes in all the hashes of the above tree nodes

- Applying Merkle proofs reduces the amount of memory space and computing power needed.

- Double-spending as forgery attempt cannot pass unnoticed through the network.

- Digital signatures play the role of an authenticity ticket for the transmitted data that ”travels” from the sender to the receiver.

- The hash of the message is signed before being sent into the network, from where the signature acts as a digital fingerprint for that particular transaction filled with data.

- The sender cannot deny having sent the document (non-repudiation).

- Digital signatures fulfill their desired role through the interaction of three algorithms, namely:

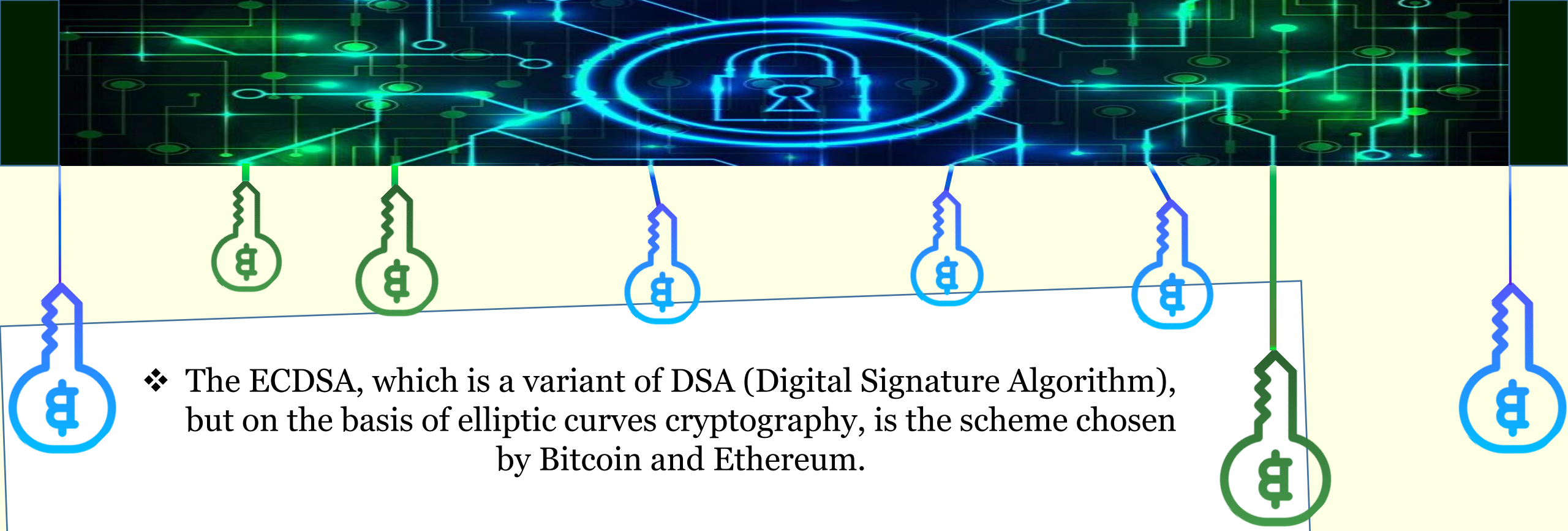
Key generation

Signature generation

Signature verification

EUF-CMA

SUF-CMA



- The ECDSA, which is a variant of DSA (Digital Signature Algorithm), but on the basis of elliptic curves cryptography, is the scheme chosen by Bitcoin and Ethereum.

- The Computational Diffie-Hellman problem: the problem of computing g^{xy} given only g^x and g^y

- The co-Gap Diffie-Hellman assumption: the contrast between the hardness of computing h^a given $h \in \langle g1 \rangle$, g_2 and ${g_2}^a \in \langle g2 \rangle$ and the ease of deciding whether $h^a = h^b$ given the co-Diffie-Hellman triple

- The BLS scheme takes $x \in Z_q$, where q is the groups' order (the groups are $\langle g1 \rangle$ and $\langle g2 \rangle$), as the private key and g_2^x as the public key.

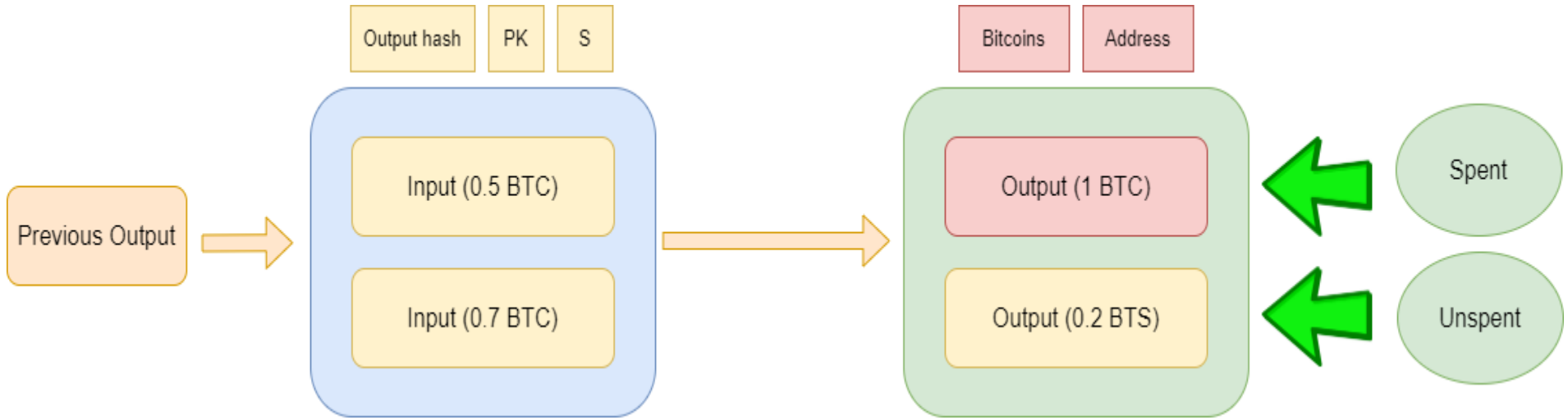
- The hash of the message is signed by raising it to the power of x.

- The secure character of the scheme comes from the fact that g_2^x and the signed hash can be used for signature verification, but re-computing the signature is difficult due to the co-Diffie-Hellman assumption.

- The Bitcoin UTXO model (unspent transaction output) explains its name by each transaction being depicted as an input-output pair, in which the input represents the spent amount of coins and the output covers the target sum and the BTC that will be spent in future transactions, yet unspent.

- The input which traverses the transaction and exceeds the target sum turns into unspent output until entering other transactions in the system.

- Bitcoin gives its users the flexibility to decide the future of the remaining coins from the current transaction



- Aggregate signatures enforce the combination of multiple signatures, on multiple messages, signed by different users, into a single representation.

- Bilinear map: a bilinear map e : ⟨g1⟩x⟨g2⟩ → G, where G is a newly formed group

- When it comes to data saved in multiple copies, aggregate signatures lead to significant storage space savings, mainly generated by the aggregation of all transaction signatures from each block into a compact signature.

- Considering n users, each one has a signing (secret) key s_i and a verification (public) key $v_i = g_2^{s_i}$. The aggregation step consists of computing the previously mentioned single representation as the product of the individual signatures.
- According to mathematical notation, $S \leftarrow \prod_{i=1}^{n} s_i$

- If order constraints are enforced over the aggregation of the individual signing keys, then the signature specialises into a so-called ***sequential aggregate signature***.

- Verification is carried out by checking the equality:

$$e(S,g2) = e(\prod_{i=1}^{n} H((m_i)^{x_i}, g_2) = \prod_{i=1}^{n} e(H(m_i)^{x_i}, g_2) = \prod_{i=1}^{n} e(H(m_i), g_2^{x_i})$$

- All messages must be different from each other, since the existence of equal messages might result in one user computing his public key at the expense of the other user having the same message and inducing attack risks.

THANK YOU FOR PAYING ATTENTION!

"Nothing is lost,
nothing is created,
everything is transformed"

Multi-signatures

Two or more users sign documents as a group.

- 2012 for Bitcoin
- multi-sig wallets
- two-factor authentication

The scheme of Boneh et al. uses the key aggregation technique:

The scheme combines multiple unique signatures into a final signature.

Key generation algorithm:
$sk \leftarrow \mathbb{Z}_q$ and outputs (pk, sk),
where $pk \leftarrow g_2^{sk}$

Each share:
$s_i = H_0(m)^{a_i sk_i}$

Aggregated key:

$$apk \leftarrow \sum_{i=1}^{n} pk_i^{a_i}$$

where
$a_i = H_1(pk_i, \{pk_1, \ldots, pk_n\})$

Final signature:

$$\sigma = \prod_{i=1}^{n} s_i$$

Threshold signatures

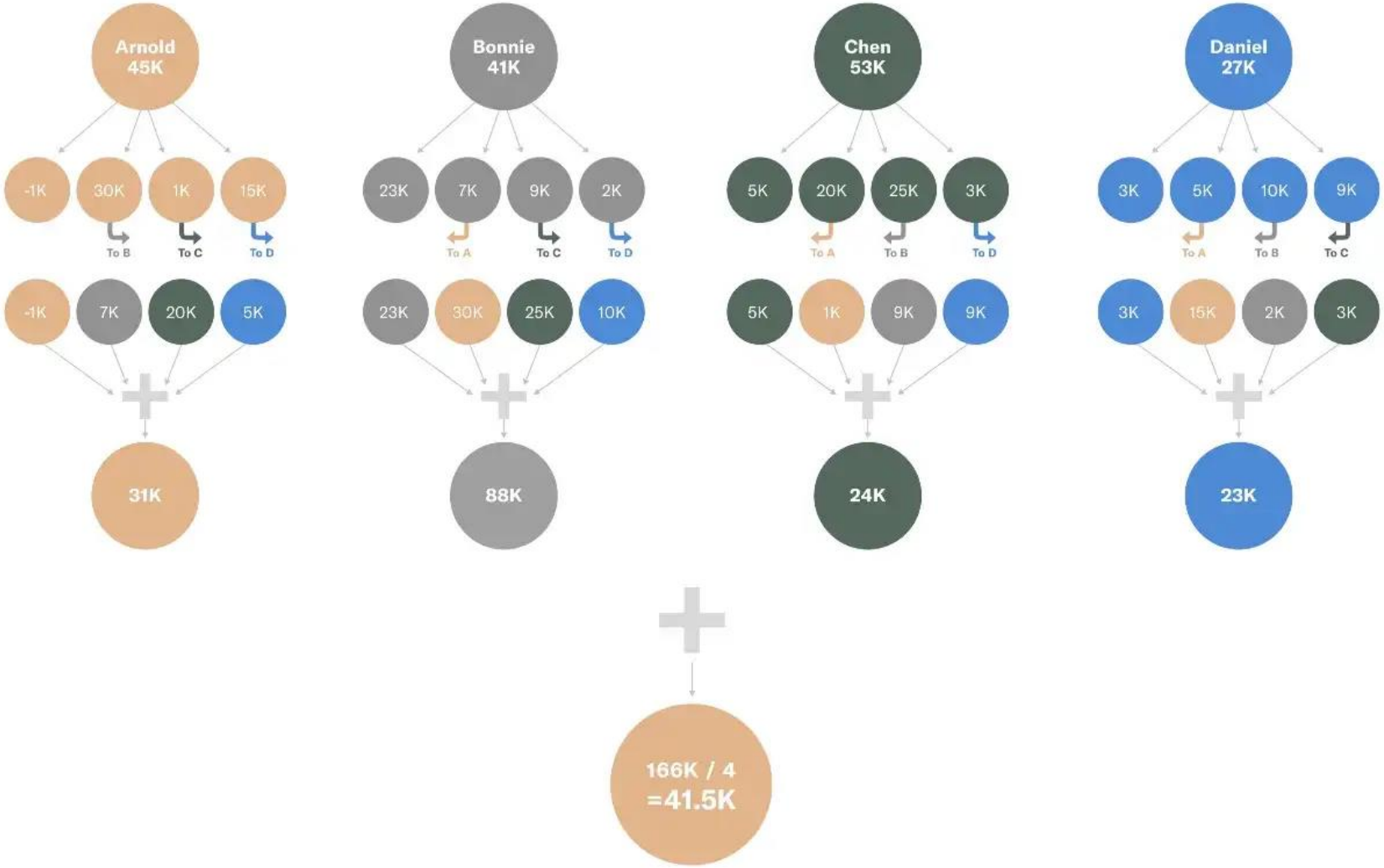
Single digital signature from multiple signers, each having a private key share.

In a TSS (n,t) n is the total number of participants t is a previously decided upon threshold.

Advantages:

- The private key is no longer held by a single point of failure.
- TSS transactions are faster and cheaper to verify with lower transaction fees.
- Many different distributed key share combinations an be easily generated.
- The private key can be extended to new members.

Arnold + Bonnie + Chen + Daniel = 166K



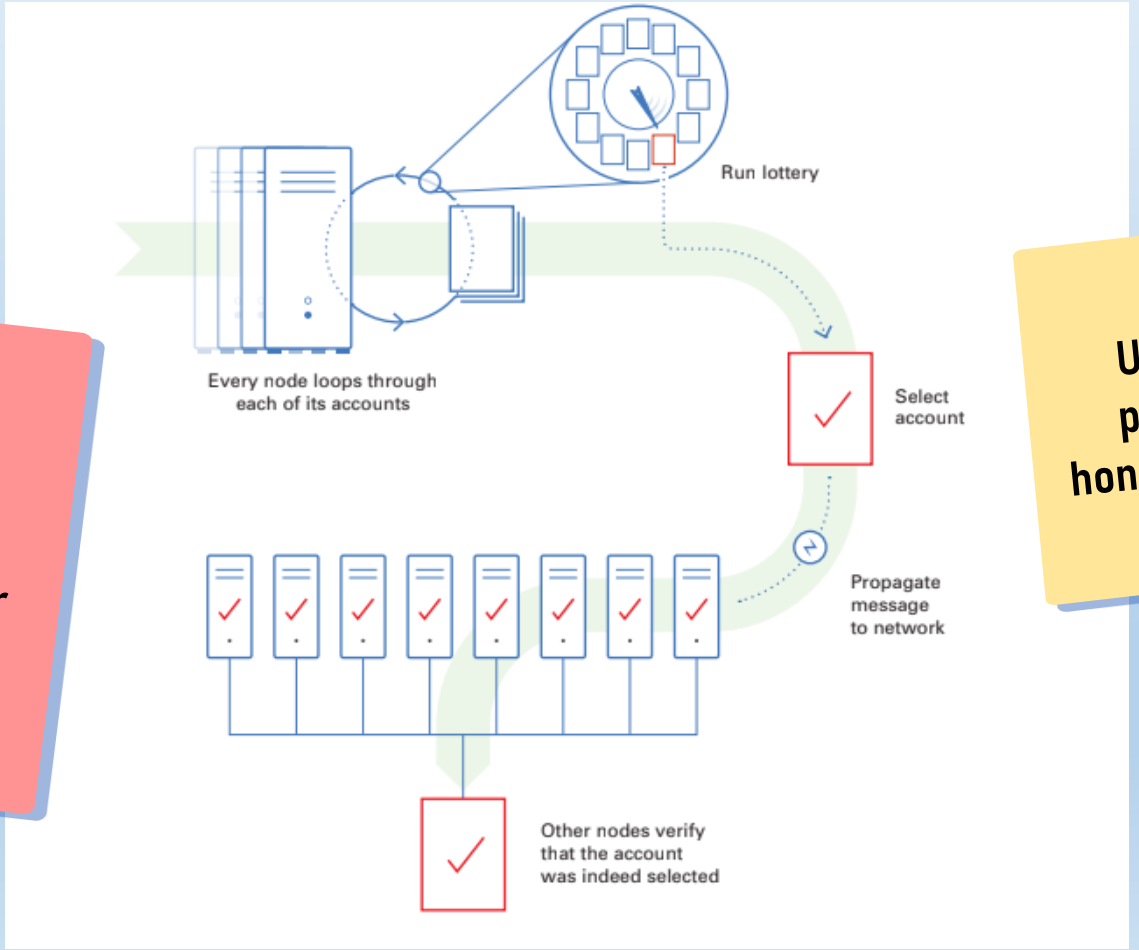
Forward-secure signatures

Past signatures remain valid even if the current signing key has been compromised.

- *T periods of time during which the public key is valid.*
- *Different secret key in each time period .*

- Used in Algorand or the Ouroboros protocols that build the foundation of the Cardano blockchain.
- The attacker is not able to create messages related to any consensus round.

Verifiable random functions



Input: string
Generates: (pk,sk)
Output: (r,π)
r = pseudo-random number
π = a string, also known as the proof

Used in consensus protocols based on honest majority of stake.

Commitment schemes

- encode a message
- keep it hidden
- reveal the committed message at a certain desired time in the future

Non-interactive proofs

Interactive zero-knowledge proofs:

- the prover manages to convince the verifier that some theorems are true
- side information are not revealed
- are not publicly verifiable

Non-interactive zero-knowledge proofs:

- the prover manages to convince more verifiers
- are publicly verifiable

SNARGs and SNARKs:

- the proof computed by the prover is short in length and fast to verify
- Zerocash is known as one of the first blockchain protocols to design a zk-SNARK

Cryptographic tools for blockchain

- Privacy-Enhancing Signatures
- Secure Multi-Party Computation
- Conclusions

Privacy-Enhancing Signatures

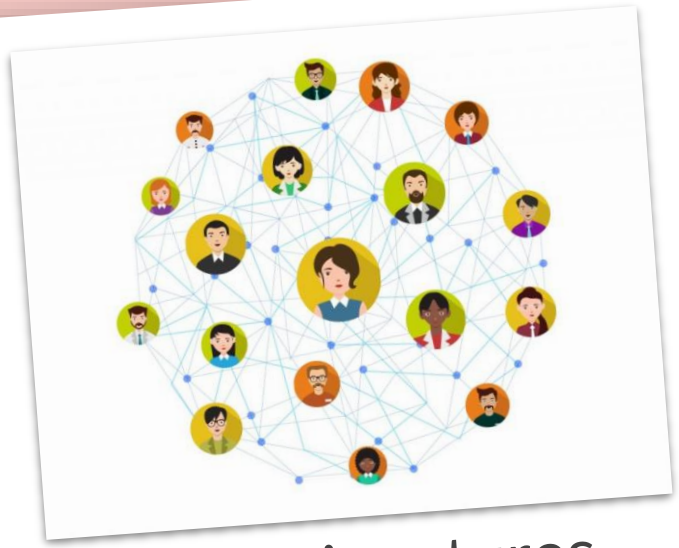
- Privacy Enhancement Techniques
- Ring signatures
- Threshold Ring Signature Schemes
- Accountable Ring Signatures

Privacy Enhancement Techniques

- Protect user’s online:
  - Transactions
  - Data
  - Identity

- Privacy technologies:
  - Soft
  - Hard

- Aggregate signature
- Group signature



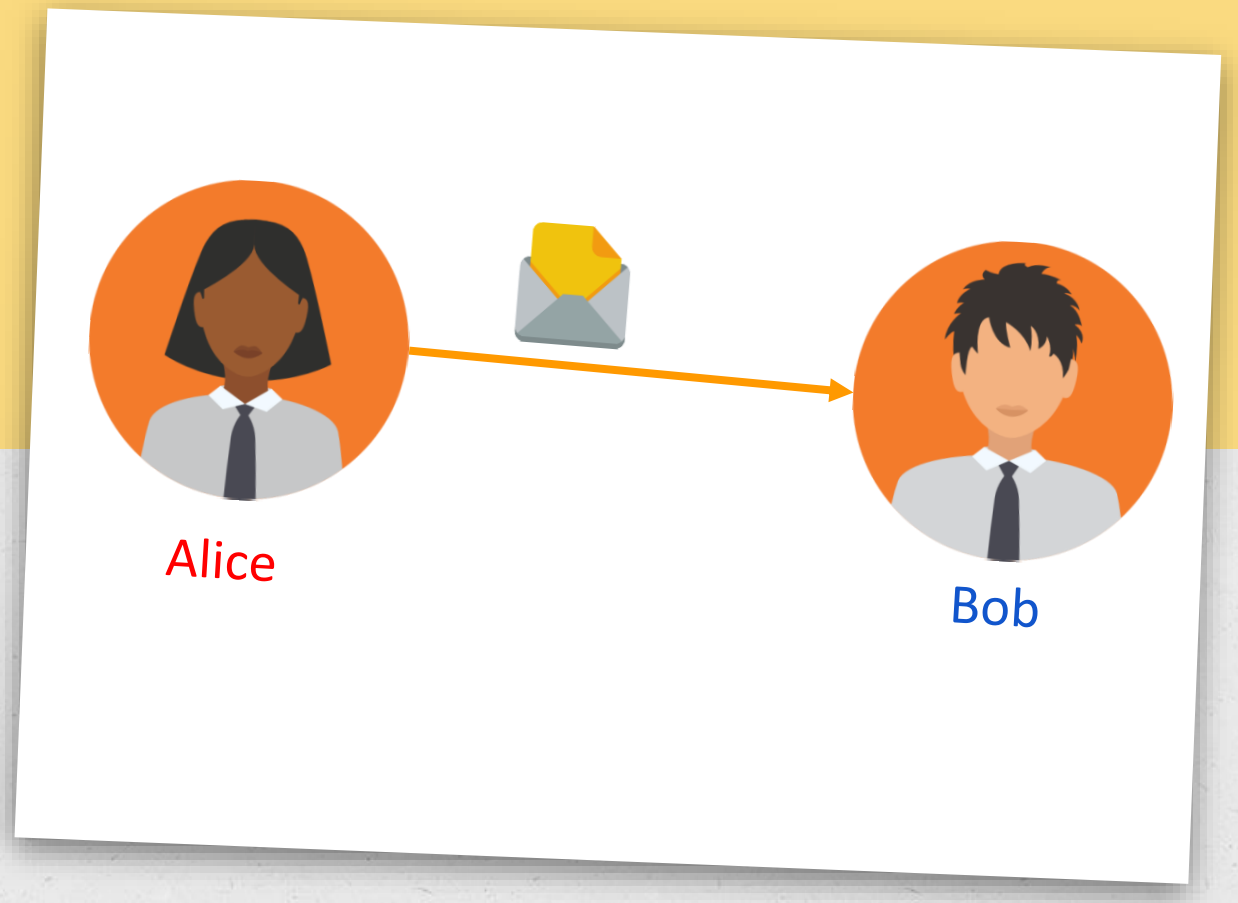
Ring signatures

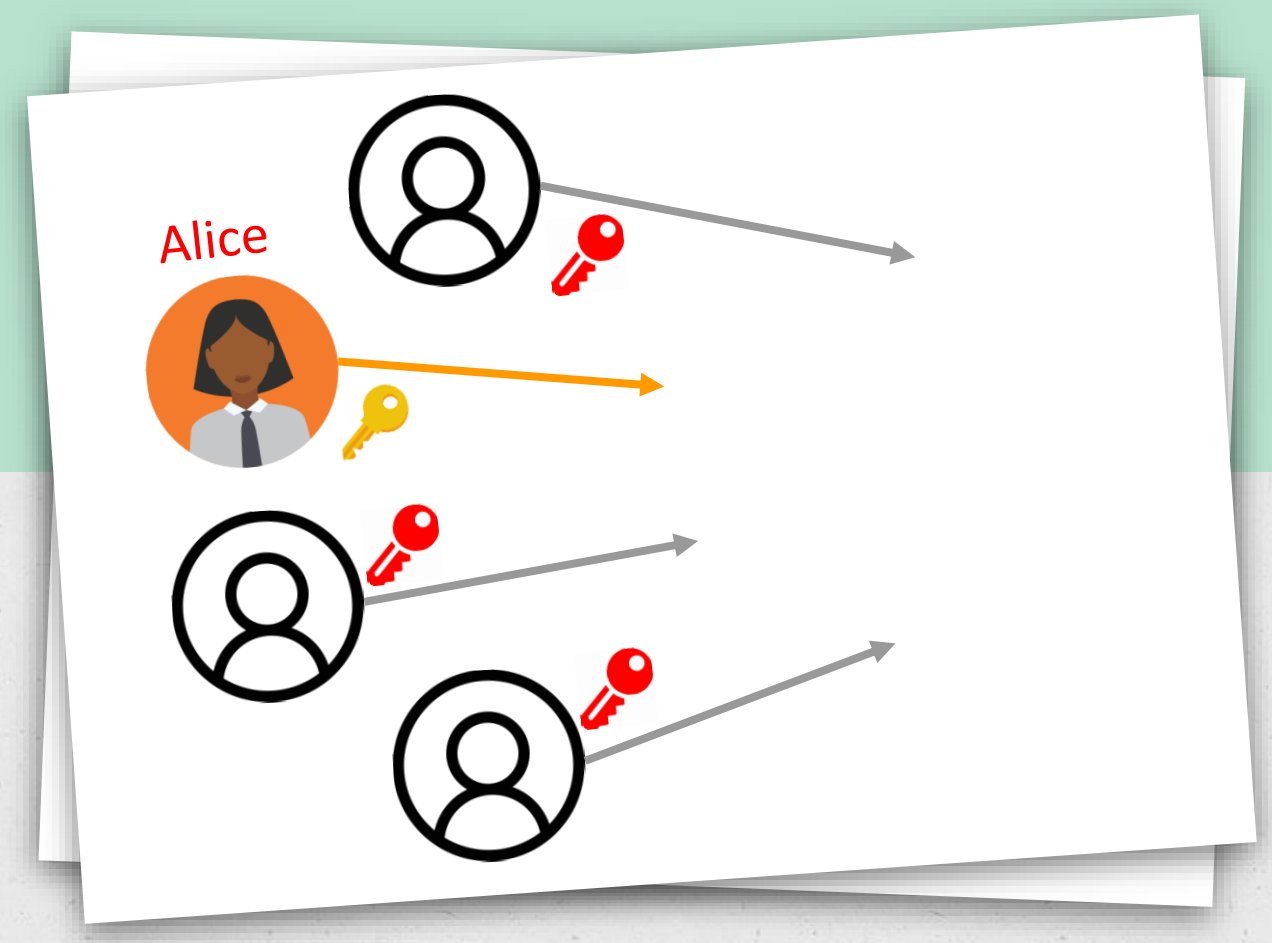
- multiple parties come together and form a group and anyone from that group can sign the message using the key
- only reveal to the verifier that the signer is one of the members of the ring and not which specific user signed

Introduced by:

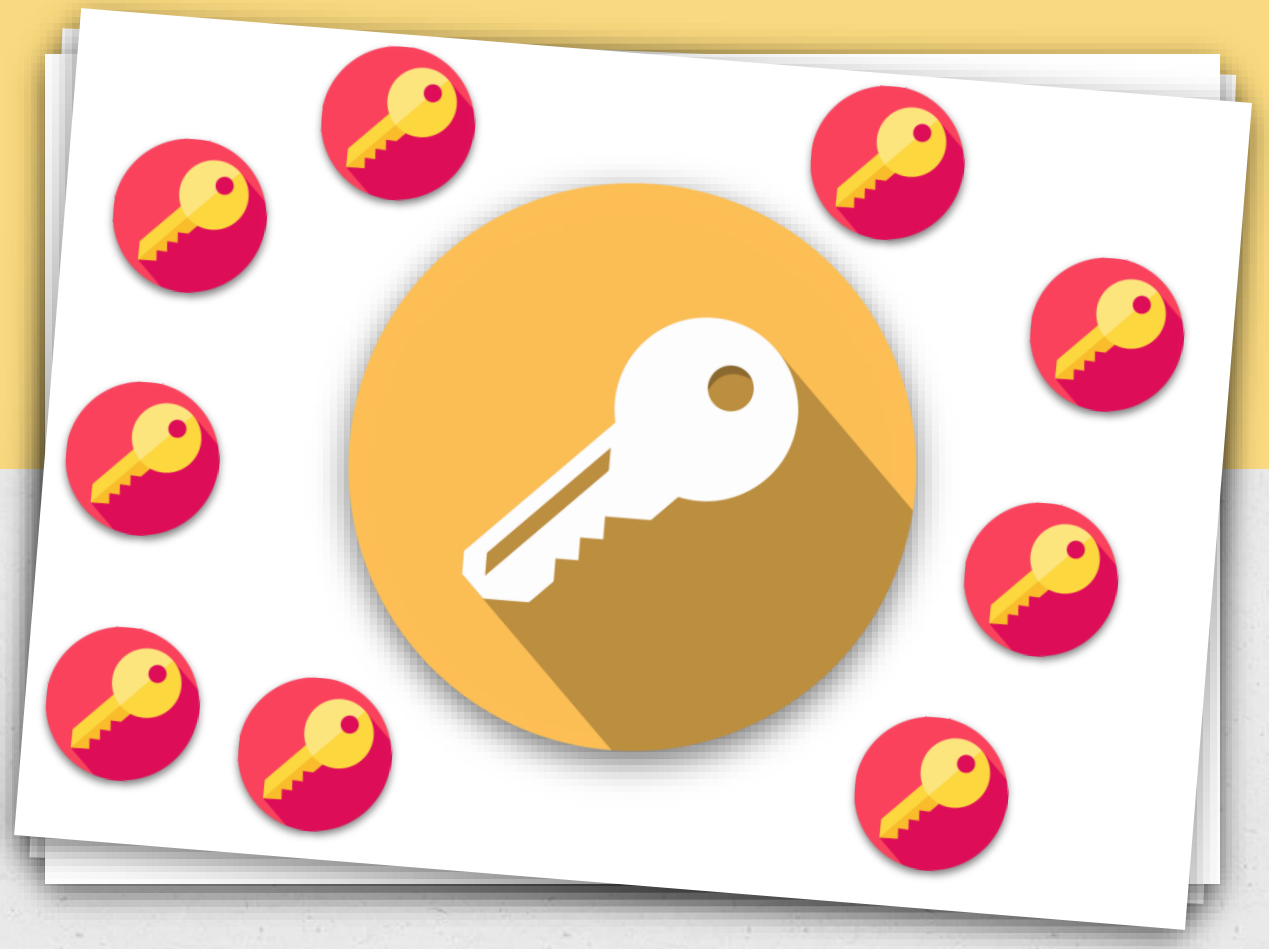
- Ron Rivest
- Adi Shamir
- Yael Tauman

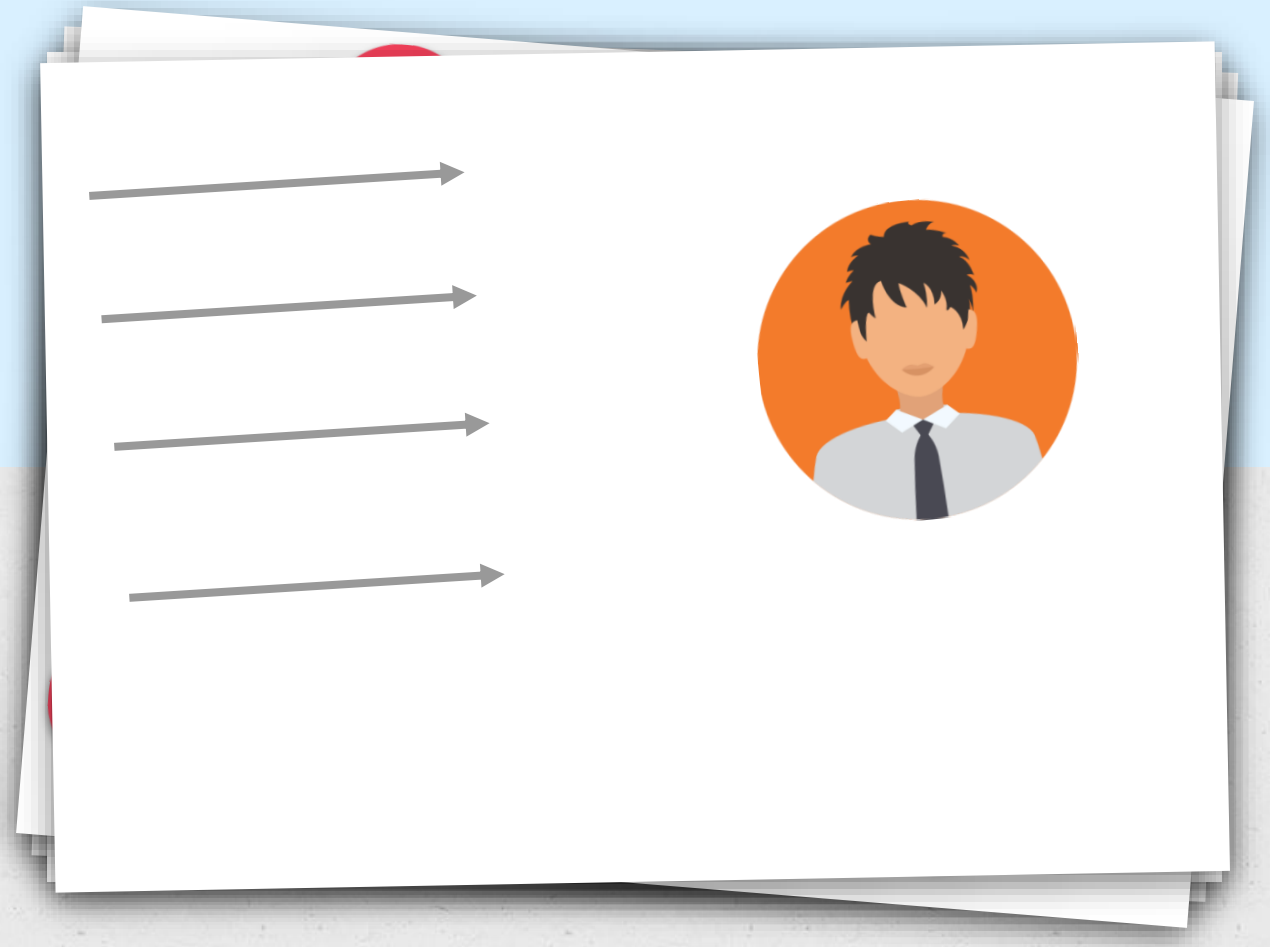
in 2001.

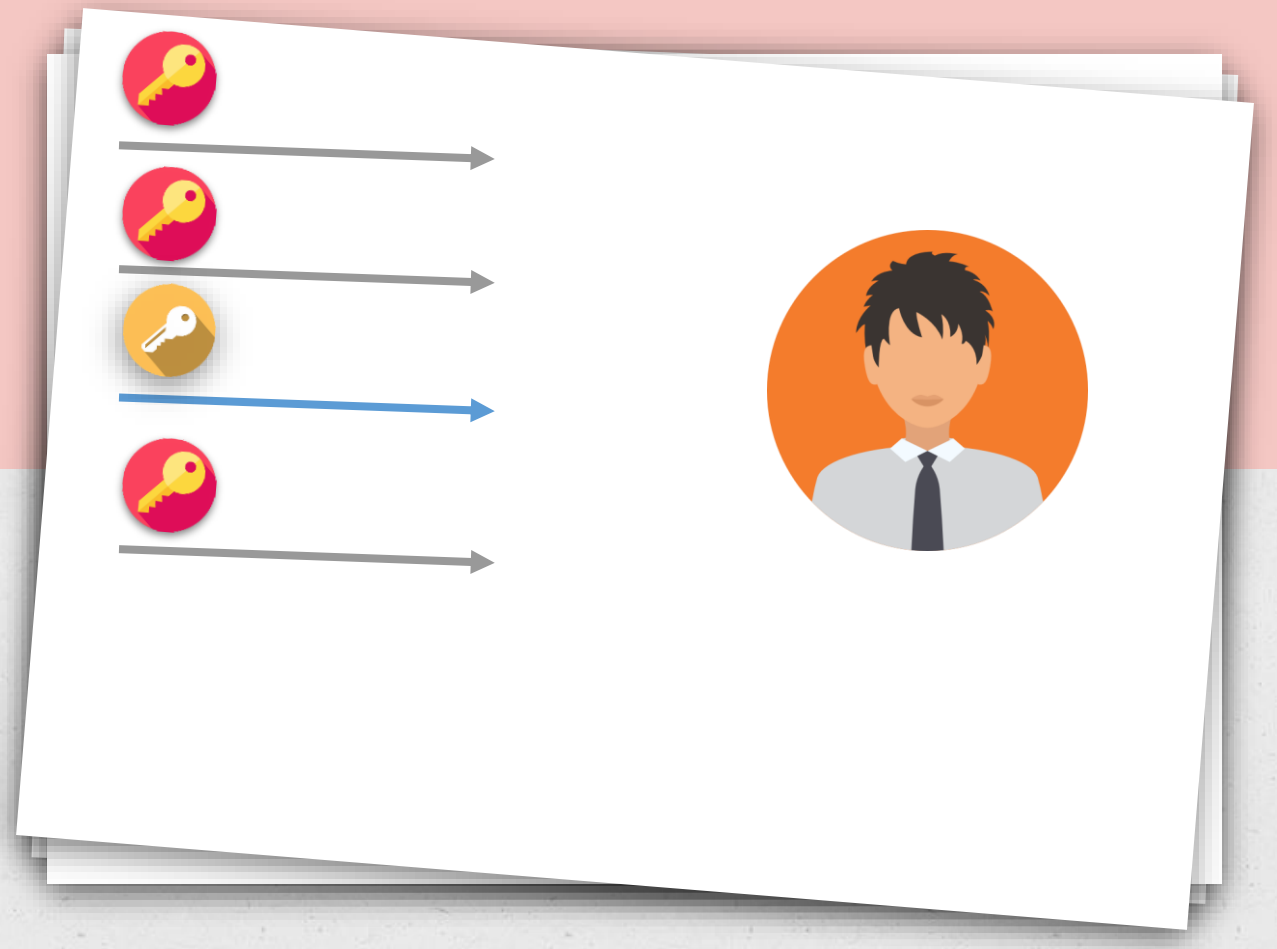

Alice
Bob

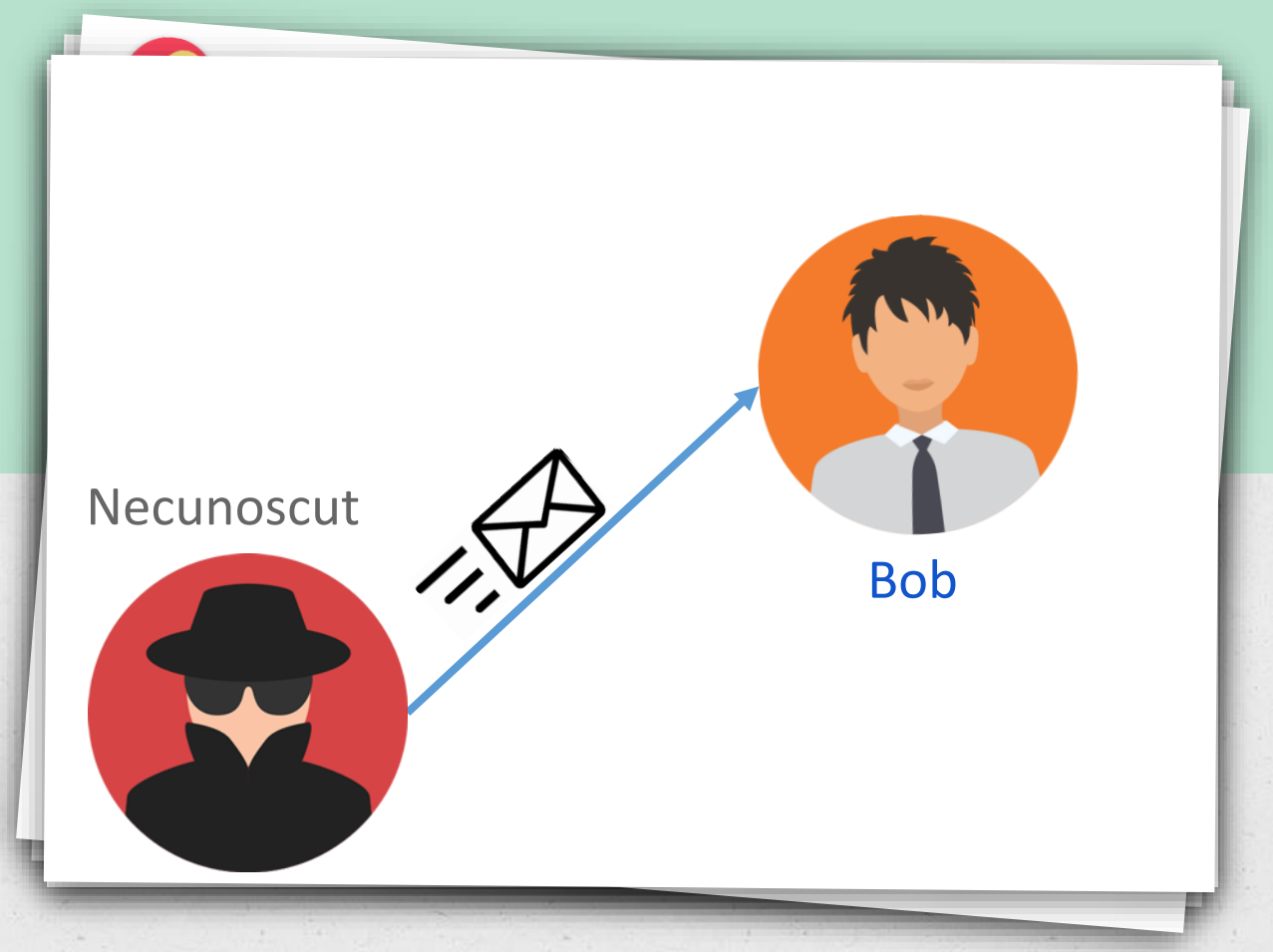

Alice

What is a key image?








Necunoscut
Bob

Threshold Ring Signature Schemes

- situations where the number of active participants is unknown

- parties can join and leave the system on demand

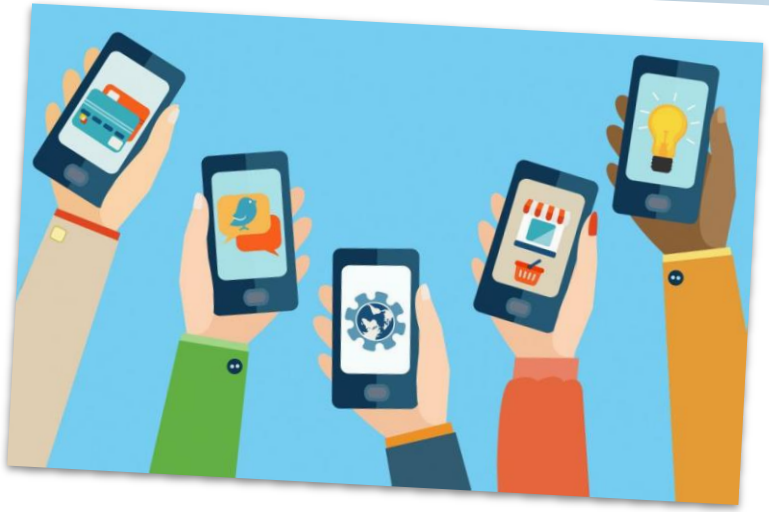
Accountable Ring Signatures

- anyone can confirm that the signature was created by a user who is a member of a set of potential signers

- actual signer can still be identified by a designated trusted entity

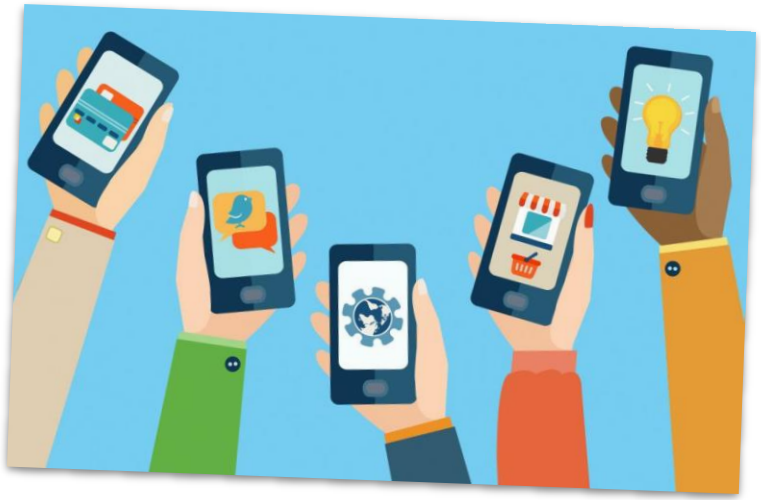
Secure Multi-Party Computation

- Secure Multi-Party Computation
- Restricted Interaction MPC
- Blockchains' use of multi-party computation



Secure Multi-Party Computation

- Yao first proposed MPC in 1982, offering decentralization as a solution to *The Millionaires' Problem*.
- In their 1987 work, Goldreich et al. expanded the two-party computation to include more parties.



What is it and how does it operate?

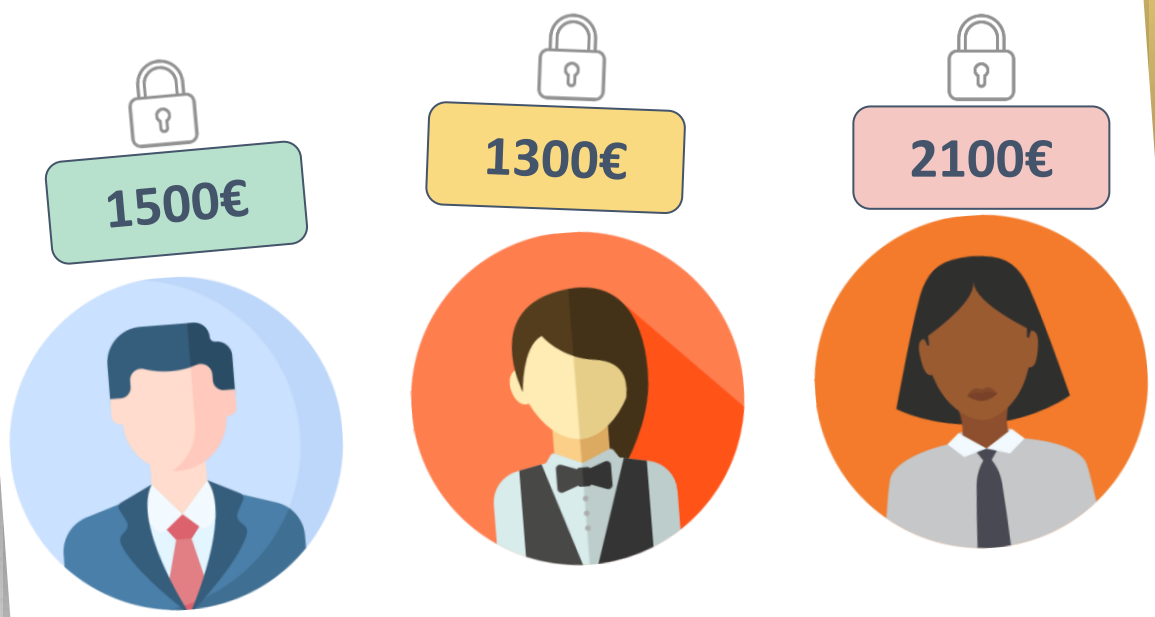
- A cryptographic scheme that aims for maximum functionality

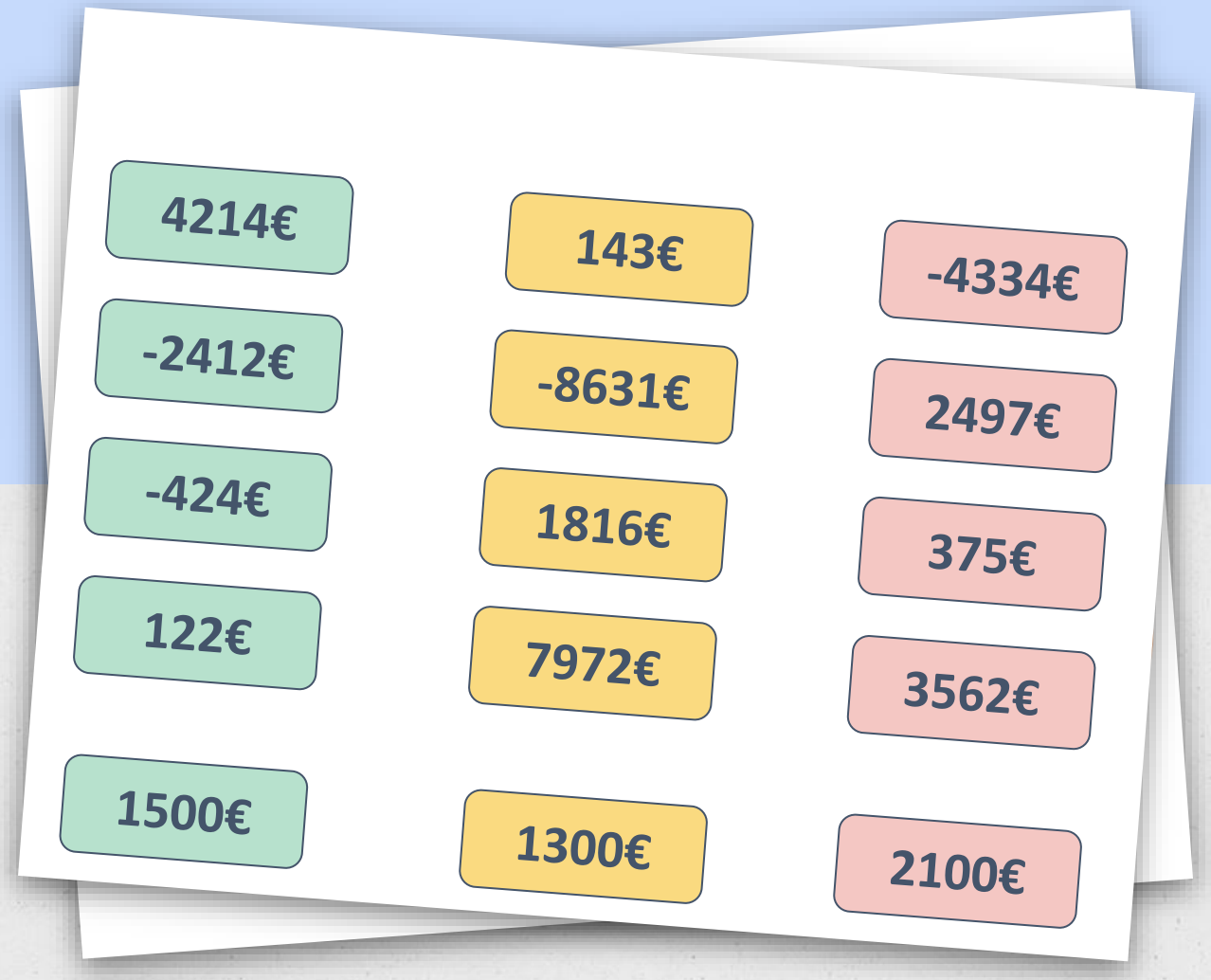
- The entering data is provided by each user. This data is put via an algorithm, which then gives each user a personalized response.

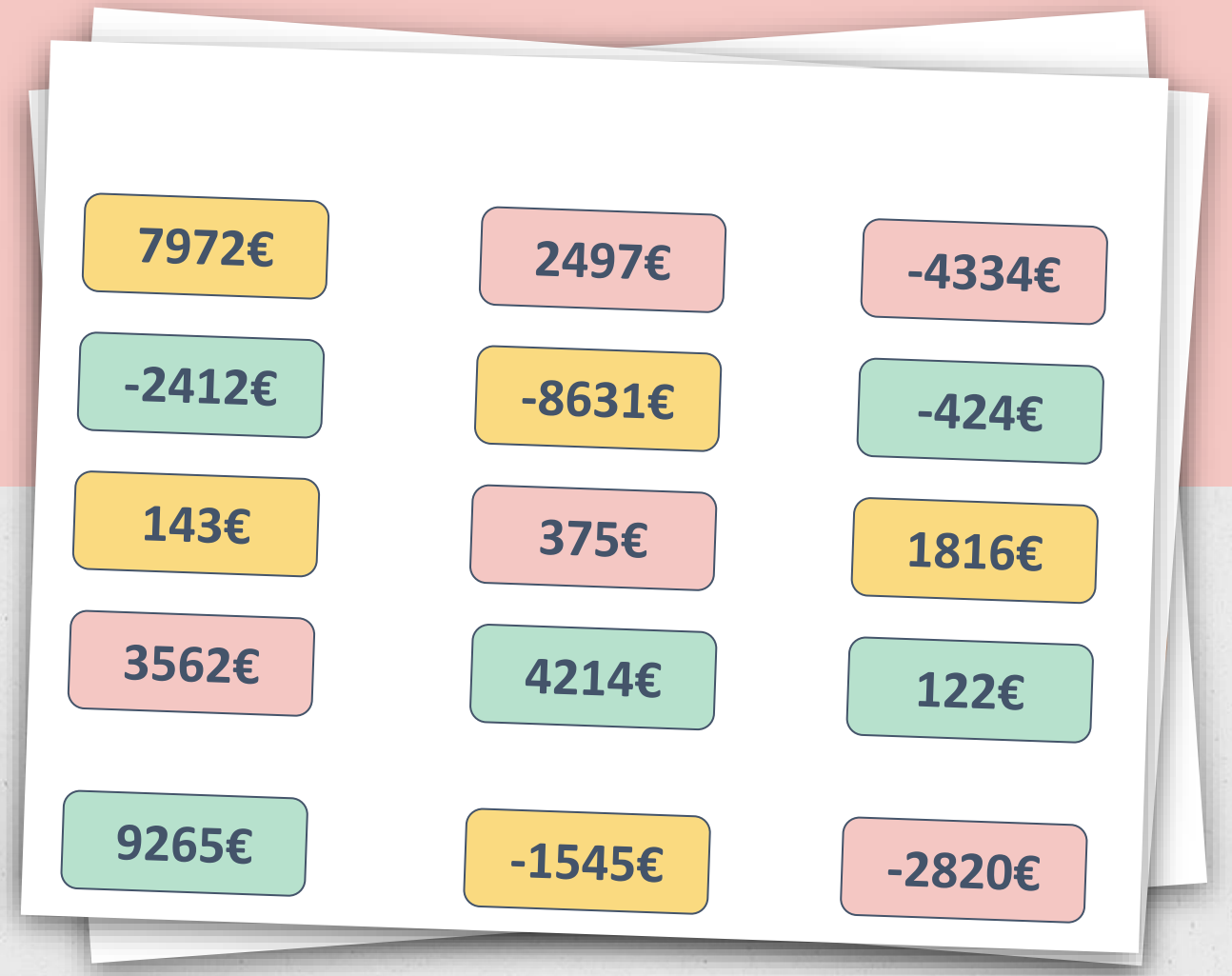
Real-world instance

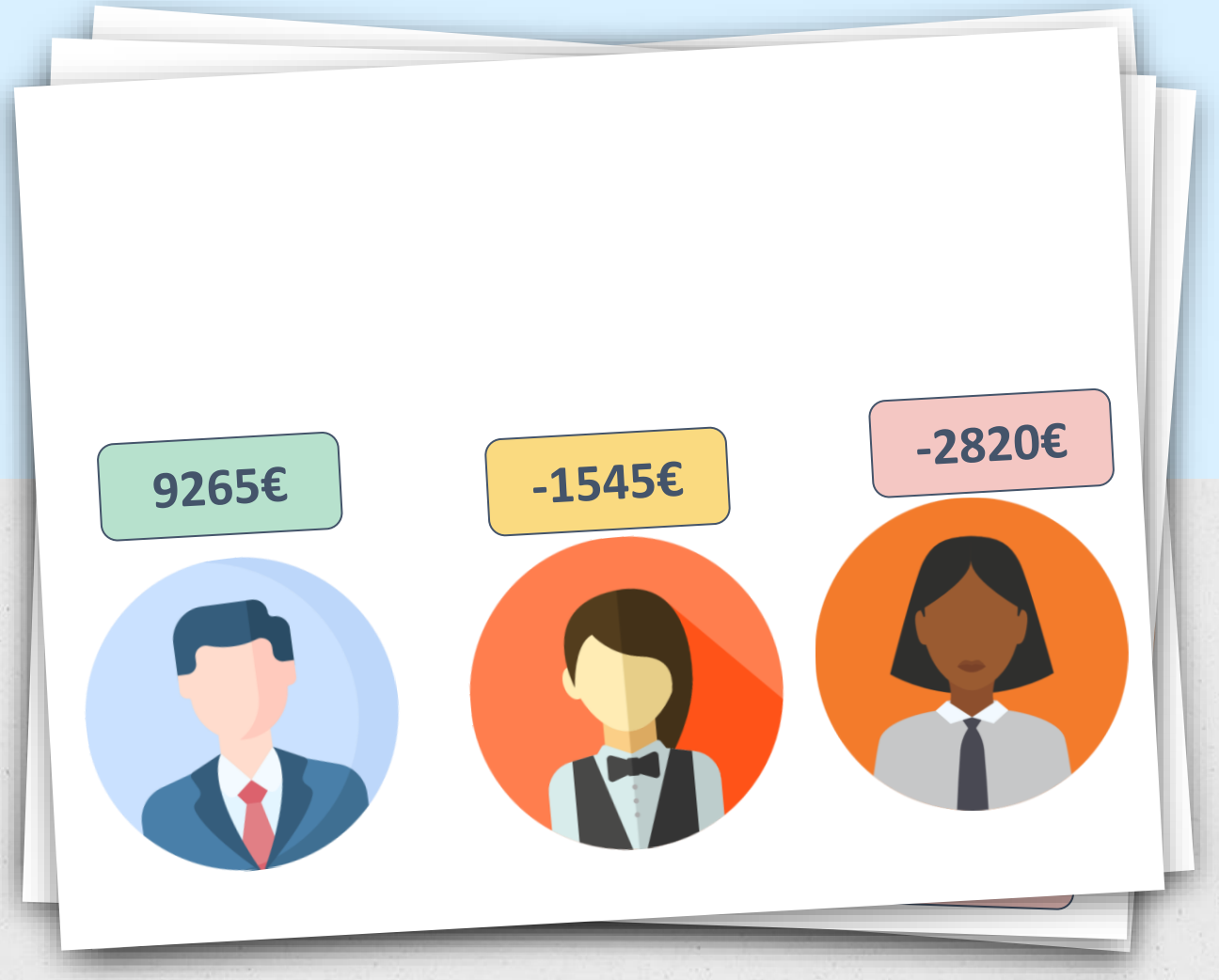
The employees of a firm want to know what the average pay is but no one likes to reveal their personal income. How can this be resolved?

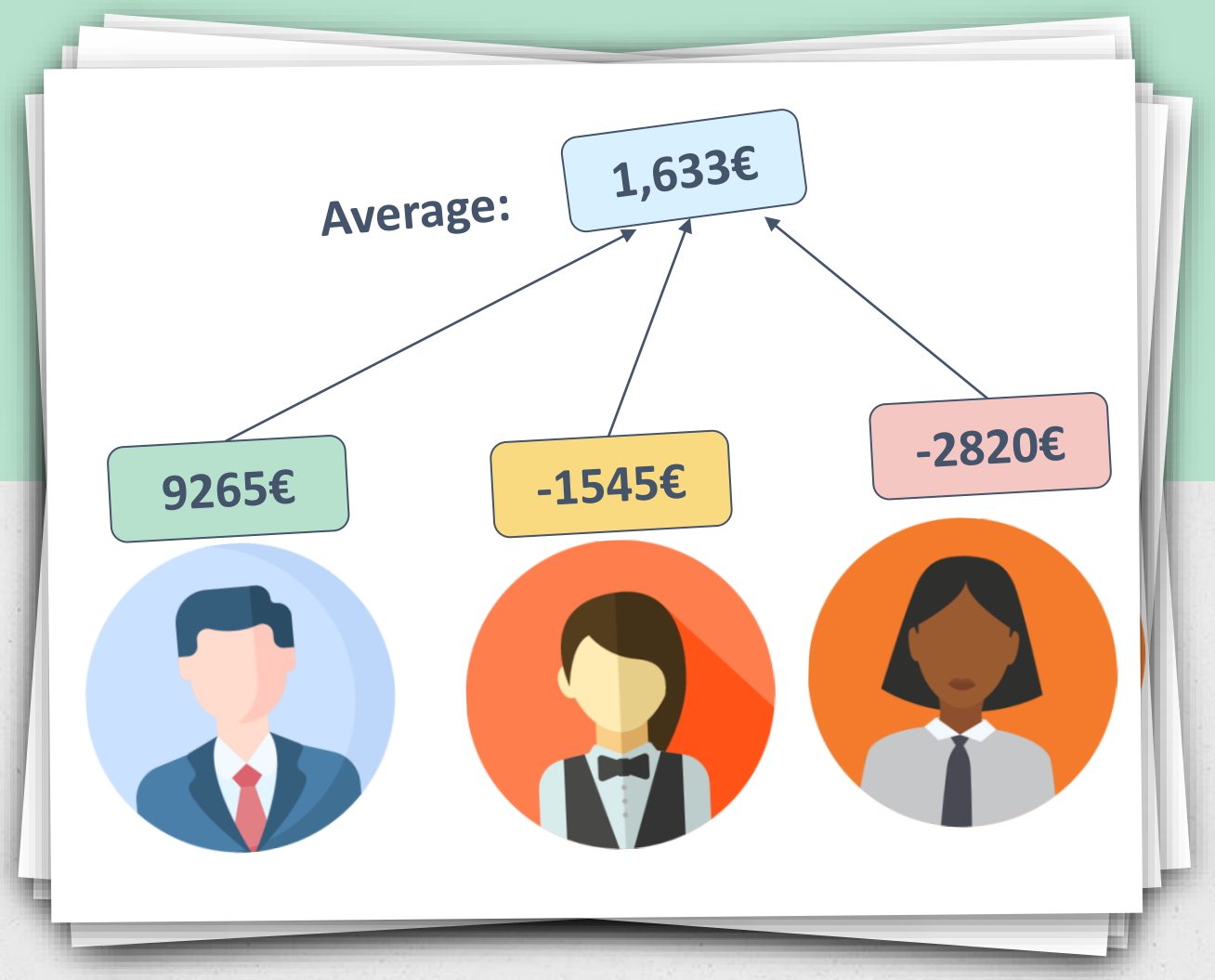
Average: ???

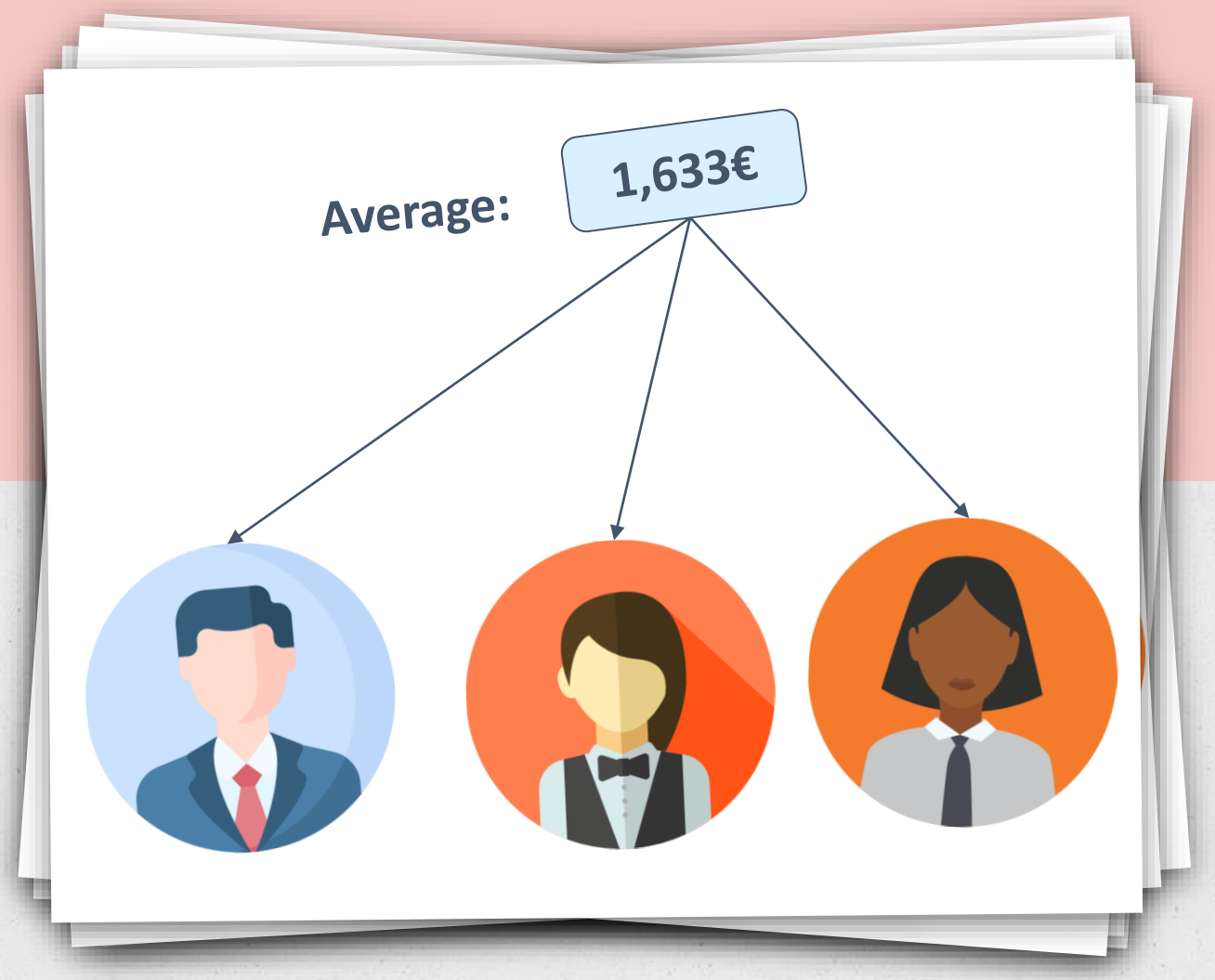



4214€
143€
-4334€
-2412€
-8631€
2497€
-424€
1816€
375€
122€
7972€
3562€
1500€
1300€
2100€


7972€
2497€
-4334€
-2412€
-8631€
-424€
143€
375€
1816€
3562€
4214€
122€
9265€
-1545€
-2820€


9265€
-1545€
-2820€


Average:
1,633€
9265€
-1545€
-2820€


Average:
1,633€

Restricted Interaction MPC

The initial researchers that looked into this topic were:

- Halevi
- Lindell
- Pinkas

Blockchains' use of multi-party computation

- Keeping identity wallets safe
- Transactions
- Transaction privacy and confidentiality

Conclusions