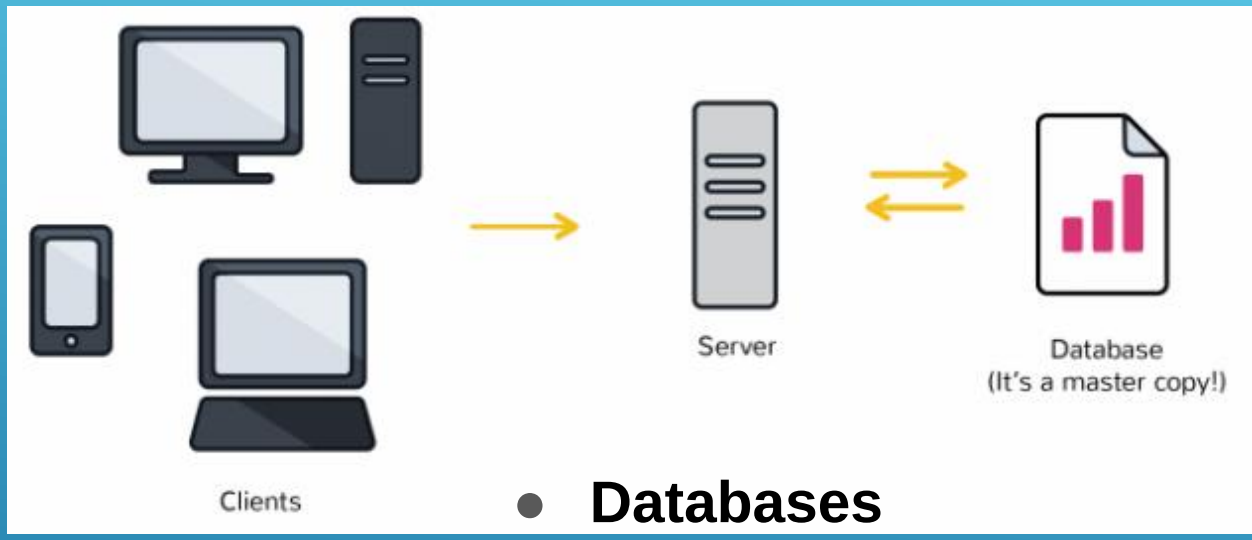
Course title: Innovation in FinTech

Lecture: Raising Capital: Credit Tech, Coin Offerings, and Crowdfunding

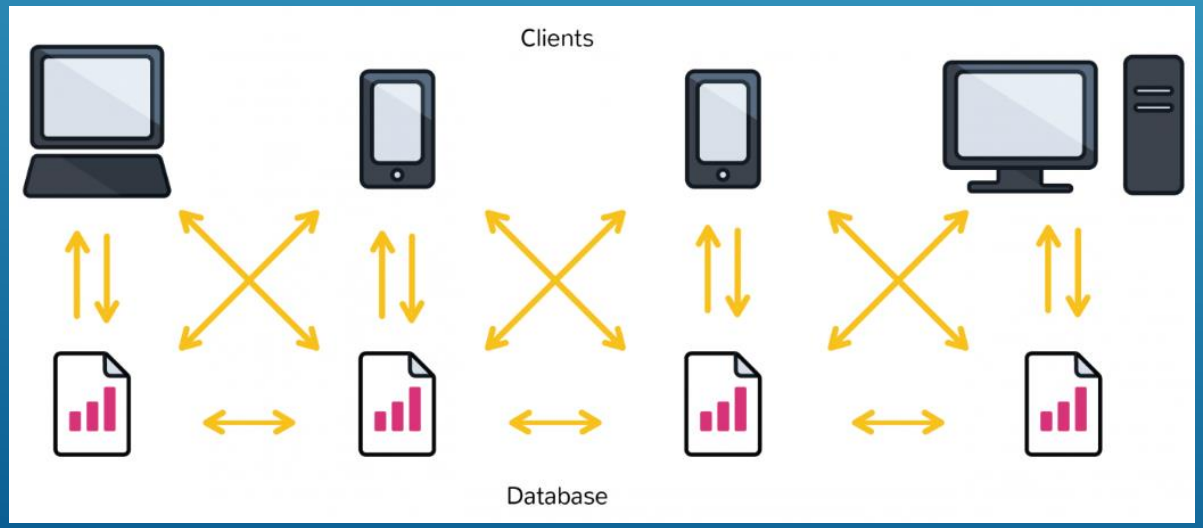
Lecturer Radjabov Jamsher

Distinction between databases and blockchain ledgers

- Distinction between databases and blockchain ledgers
  - *It begins with architecture*



- **Databases**



- **Blockchain ledgers**

Distinction between databases and blockchain ledgers

Databases 	VS	Blockchains 
Databases have admins & centralized control		No on is the admin or in-charge
Only entities with rights can access database		Anyone can access (public) blockchain
Only entities entitled to read or write can do so		Anyone with right proof of work can write on the blockchain
Databases are fast		Blockchains are slow
No history of records & ownership of digital records		History of records & ownership of digital records

Cryptography, hash functions and digital signatures

- **Cryptography**: the encryption and decryption of data
  - 2 main cryptographic concepts used in Blockchain:
    - Hashing
    - Digital Signatures
  - 3 forms of encryption that are widely used:

Symmetric cryptography	Asymmetric cryptography	Hashing
Same password to encrypt & decrypt	one password to encrypt, the other to decrypt	Maps to fixed size
2 ways function	Passwords come by pair	1 way function

Cryptography, hash functions and digital signatures

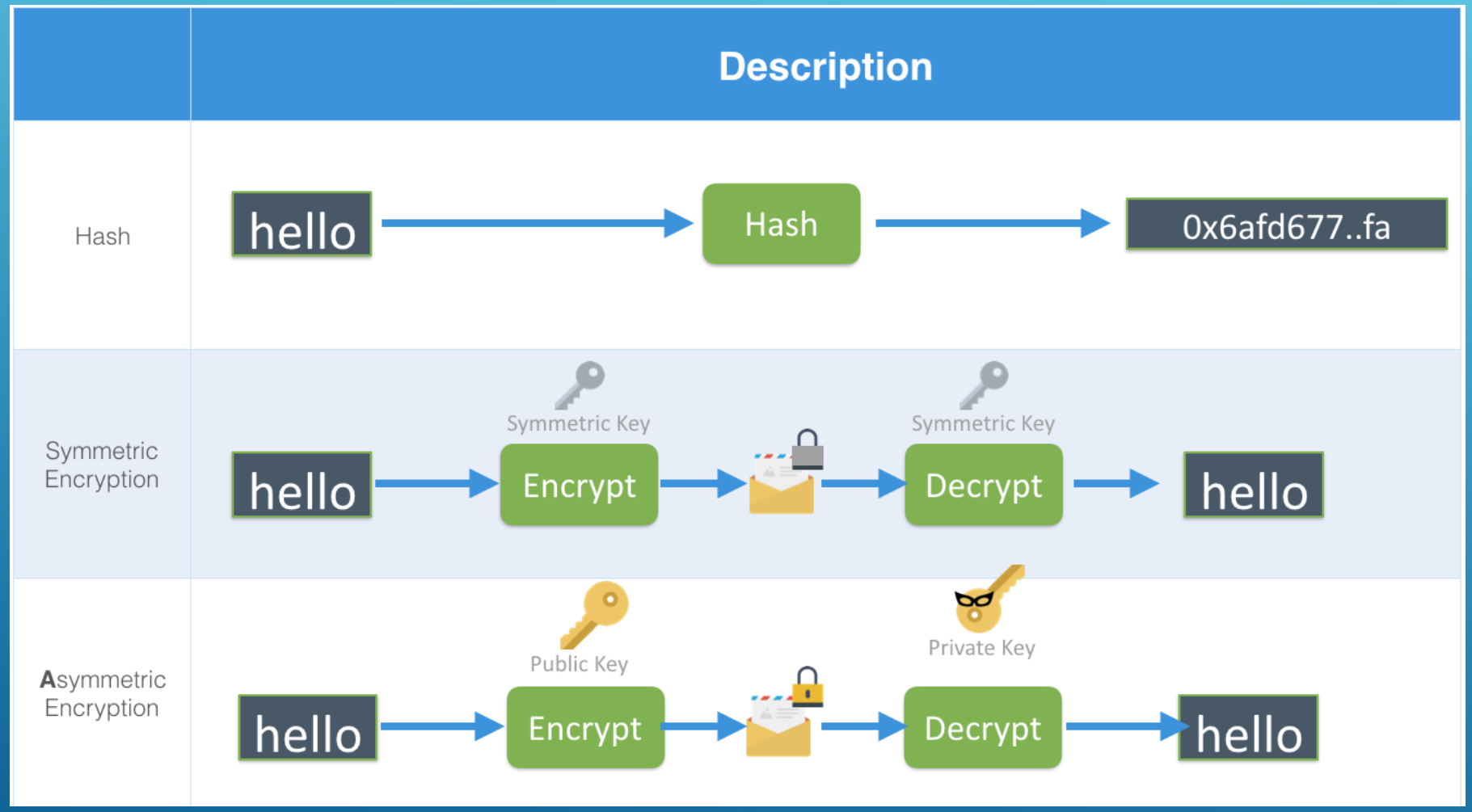


Image source: Scorechain

Cryptography, hash functions and digital signatures

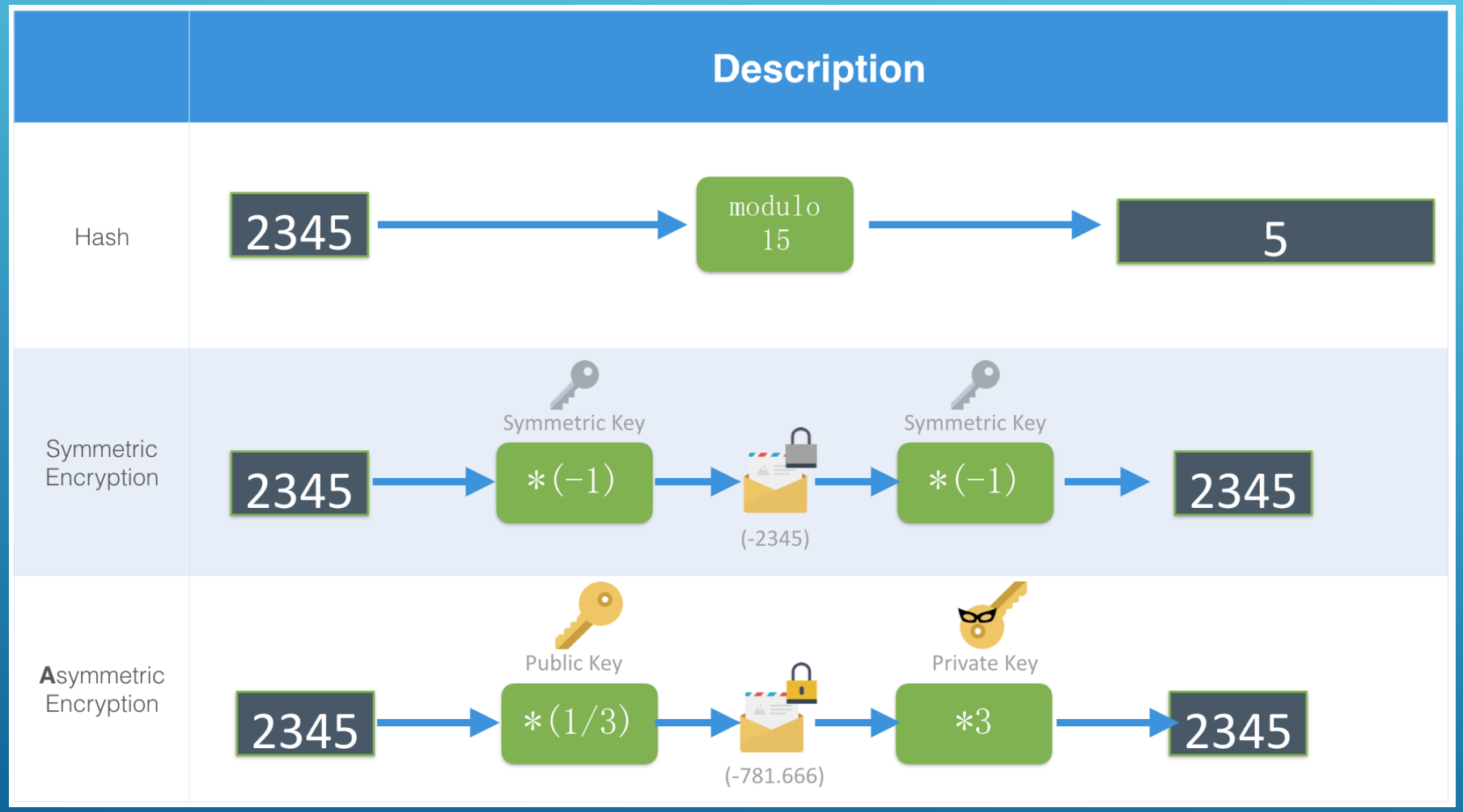


Image source: Scorechain

Cryptography, hash functions and digital signatures

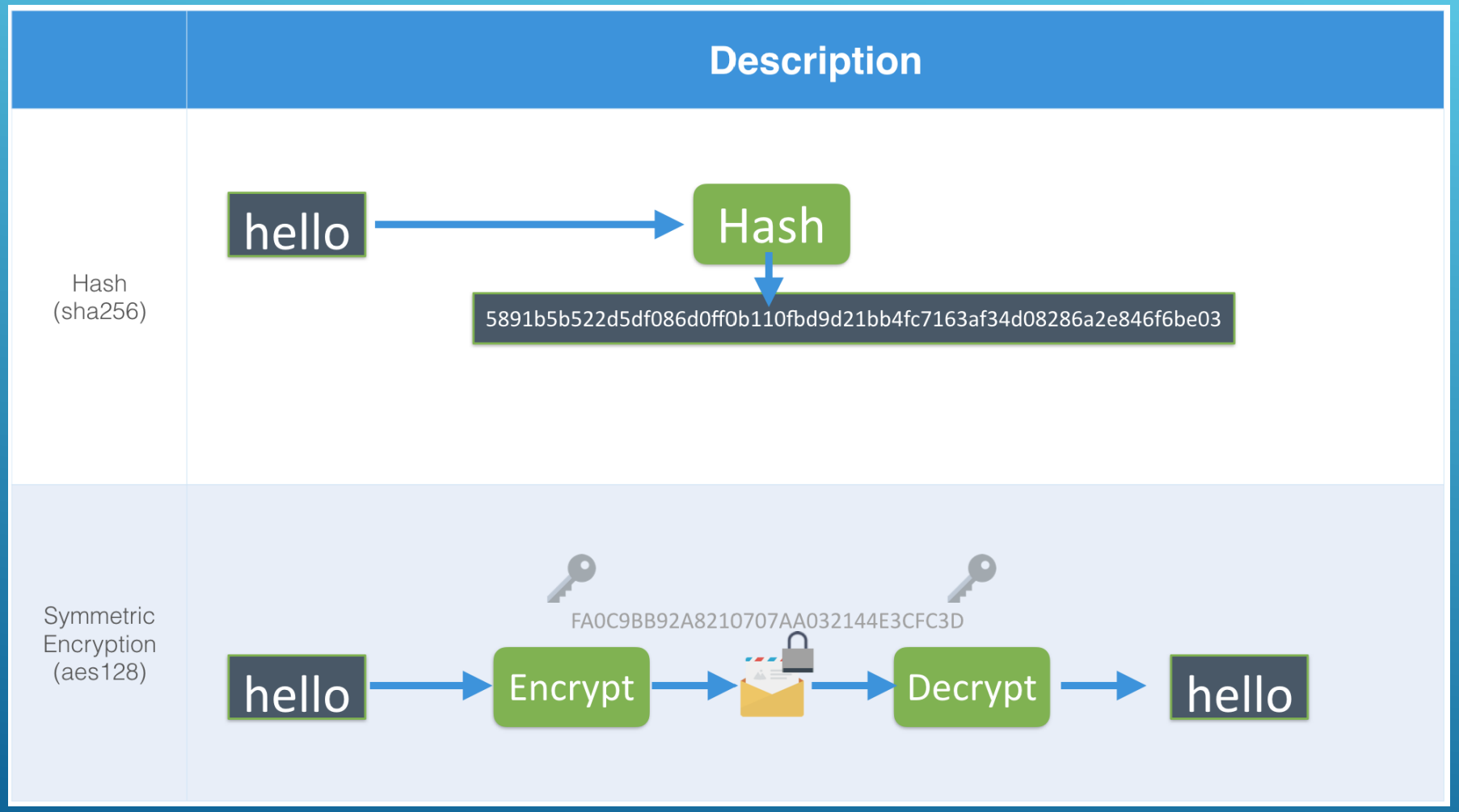


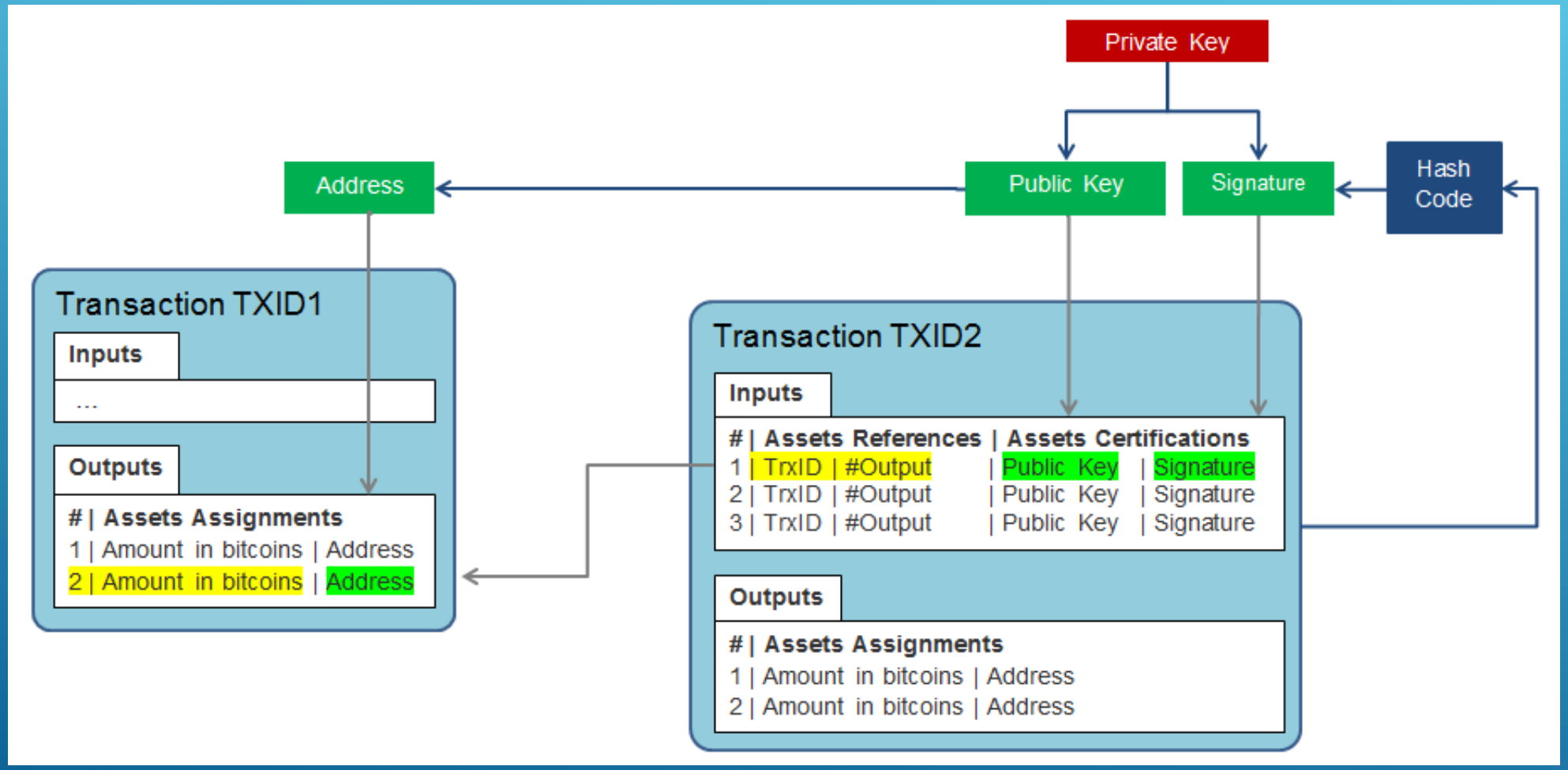
Image source: Scorechain

Cryptography, hash functions and digital signatures

	Description
Asymmetric Encryption	
Asymmetric Encryption (RSA 1024)	-----BEGIN RSA PRIVATE KEY----- MIICXQIBAAKBgQCISsEbRdh3GzIrfF4OFCApmVzzTWBYucXKgjs18XQ9B7peqtXj 9CeJxQTTXfpRjDkM+k6TCDrlyRhffrN7zAqSSmfFrelYHa37VE8XFZfP5UOyJv3W bwHJXGp0AAkHXr3bokh3Sgj4RFBdVvIBlFvumapQLn7Oze0kE37Je3kf2QIDAQAB AoGAIuoroCX7dz/DUXqRyb+ElcQFGNsopHIq5l8IdiA96+iP6PKQys3gVx3ex5sa pktqzhVNjcMc+4LRuJ0Hs94oksO3aKlG248vODjf2PYTKlNKLcHG5HmLUbaK8uCi GRJ+lxd1AGtH7ioyDcfseRhMltjQY1DSGGkg6sA1niS/AQECQQDAijCzzV4xlsWz onVk54V0gTkz4wUHvlZcheWfpZoy7yW1LO0zbH3XfCJbsKKagnY/vqQaA99uU6cO 8tBrOt5hAkEAtTaUR8Zr+isCspb7WZ7Dv0t5yfiFbkfeA0Cl7Ql7hptJA+66KUUC KV5BoUXHBGAfqYrgGm+aKevcPXZUm3yEeQJBALV+ThRfJUhXWHtRS5nXSAyfdx17 BRXcjKngqahlwUb7+S6EcAAGZ8VFRVnq8gv1qKPEAApp1ia4ggRsTJyXvGECQCik BvlZ7Nl8T+yRo+lji+8ZFEVRsUscXxRHqW7R05xKs0NohOPAkE2K0BlFNu8qR6+U b9I9+UsxIIFMSolckbECQQCvin3KbC8lBeretn5mOR8CVxUnxU42vk4E0EhJzy8q eWxZmTdqLWfcgm1M3dLIQCdbk15GDNKYSywdZxbF05Zz -----END RSA PRIVATE KEY-----	-----BEGIN PUBLIC KEY----- MIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQCISsEbRdh3GzIrfF4OFCApmVzz TWBYucXKgjs18XQ9B7peqtXj9CeJxQTTXfpRjDkM+k6TCDrlyRhffrN7zAqSSmfF relYHa37VE8XFZfP5UOyJv3WbwHJXGp0AAkHXr3bokh3Sgj4RFBdVvIBlFvumapQ Ln7Oze0kE37Je3kf2QIDAQAB -----END PUBLIC KEY-----
Asymmetric Encryption (secp256k1)	8ab2da1ed39fad3491ceb556b6bf2e124822614f6987056e07345f2b068a12fb	04e17e467d8f78110bea2ae18c8fa1a6963202d8ee9845c86080cb8ae5b5a 558ad279ae57e0b56259470f92021a2dccb0f7ceb68c88f25b13bce9f2c0e9c8adb8c

Image source: Scorechain

Cryptography, hash functions and digital signatures



Consensus components

- **Principles and paradigms of distributed systems**
  - ***Byzantine fault tolerance*** (BFT): the dependability of a fault-tolerant computer system, particularly distributed computing systems, where components may fail and there is imperfect information on whether a component has failed.

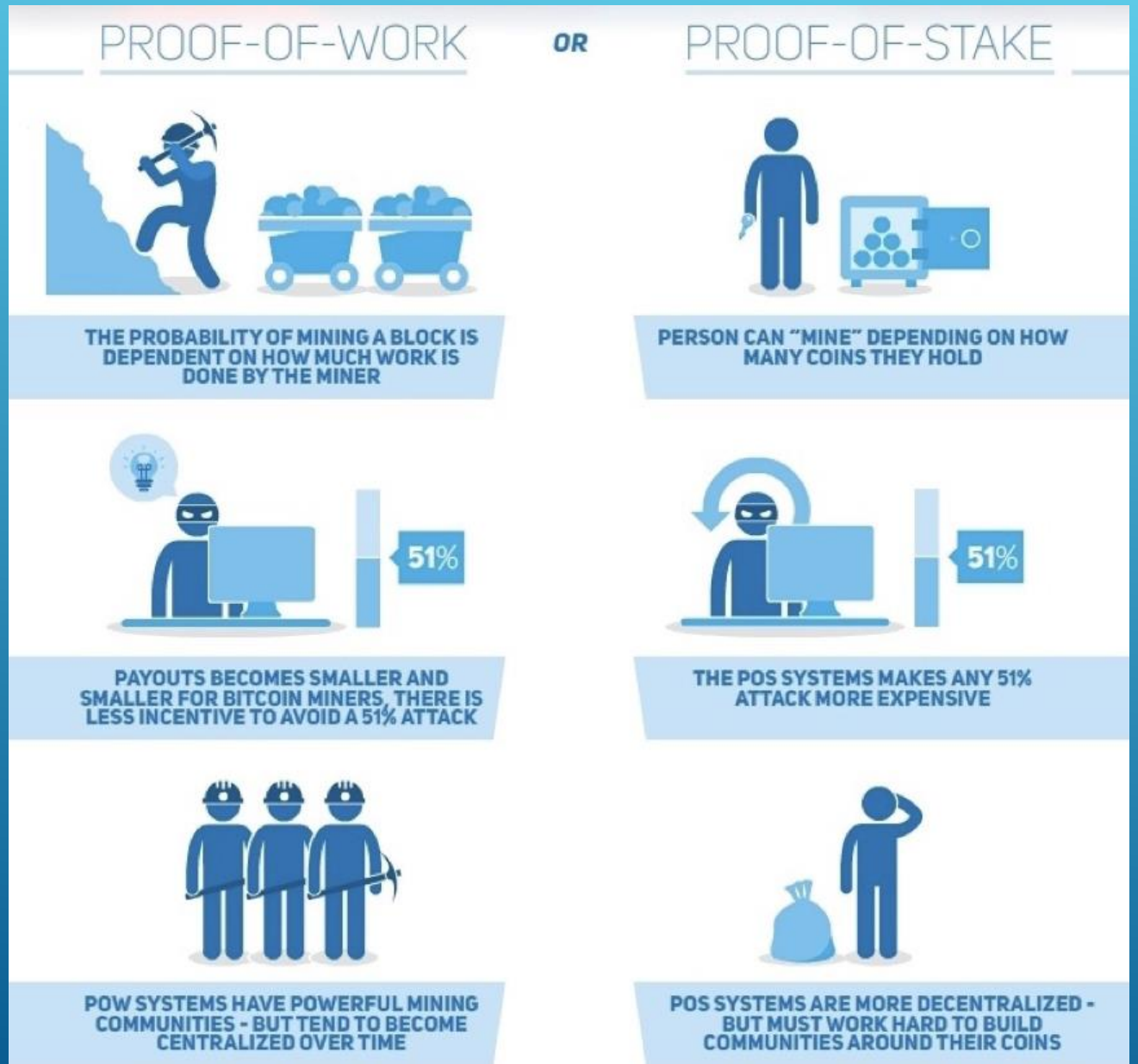
Consensus components

- **Principles and paradigms of distributed systems**
  - The objective of BFT is to defend against failures of system components with or without symptoms that prevent other components of the system from reaching an agreement among themselves, where such an agreement is needed for the correct operation of the system.

Consensus components

- **Principles and paradigms of distributed systems**
  - One example of BFT in use is bitcoin. The bitcoin network works in parallel to generate a blockchain with proof-of-work allowing the system to overcome Byzantine failures and reach a coherent global view of the system’s state.

Consensus components



Consensus components

- **Blockchain structure**
  - No more client/server architecture with name roles

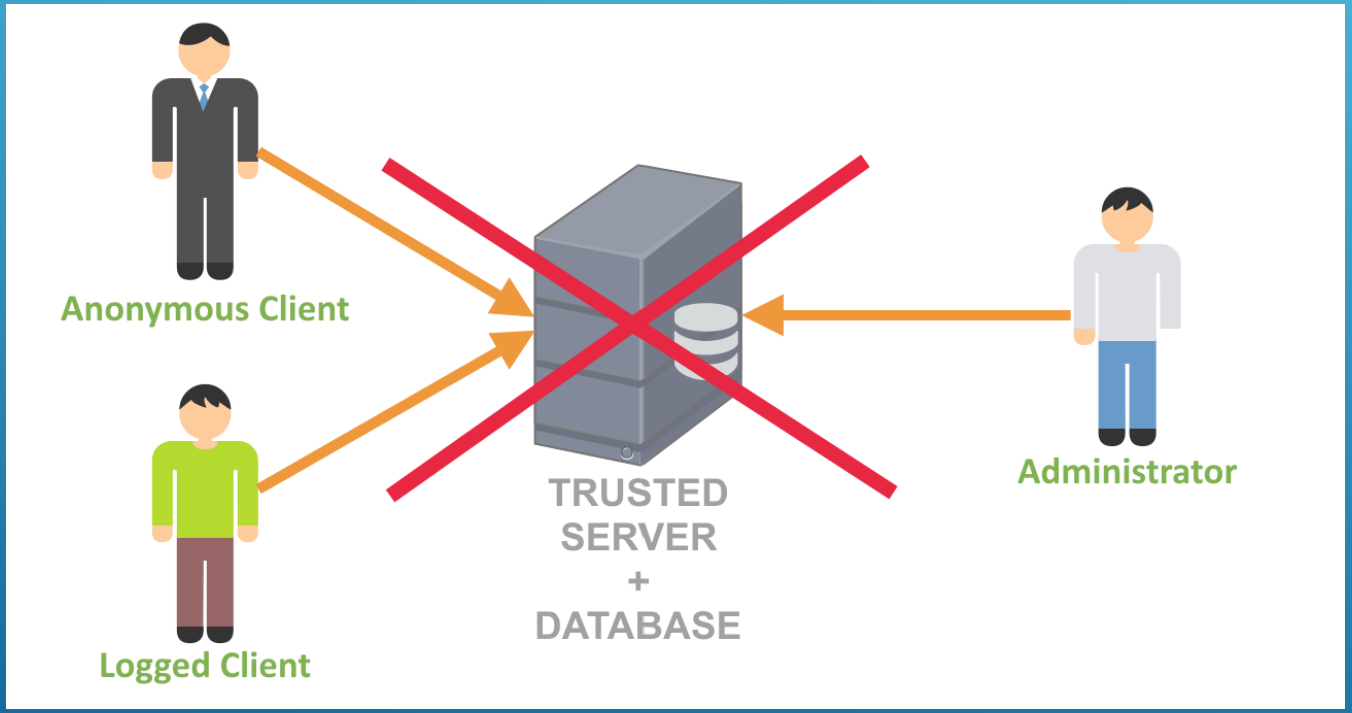


Image source: Scorechain

Consensus components

- **Blockchain structure**
  - Peer-to-peer Architecture with pseudonymous client bearing key pairs. Each node as a database copy.

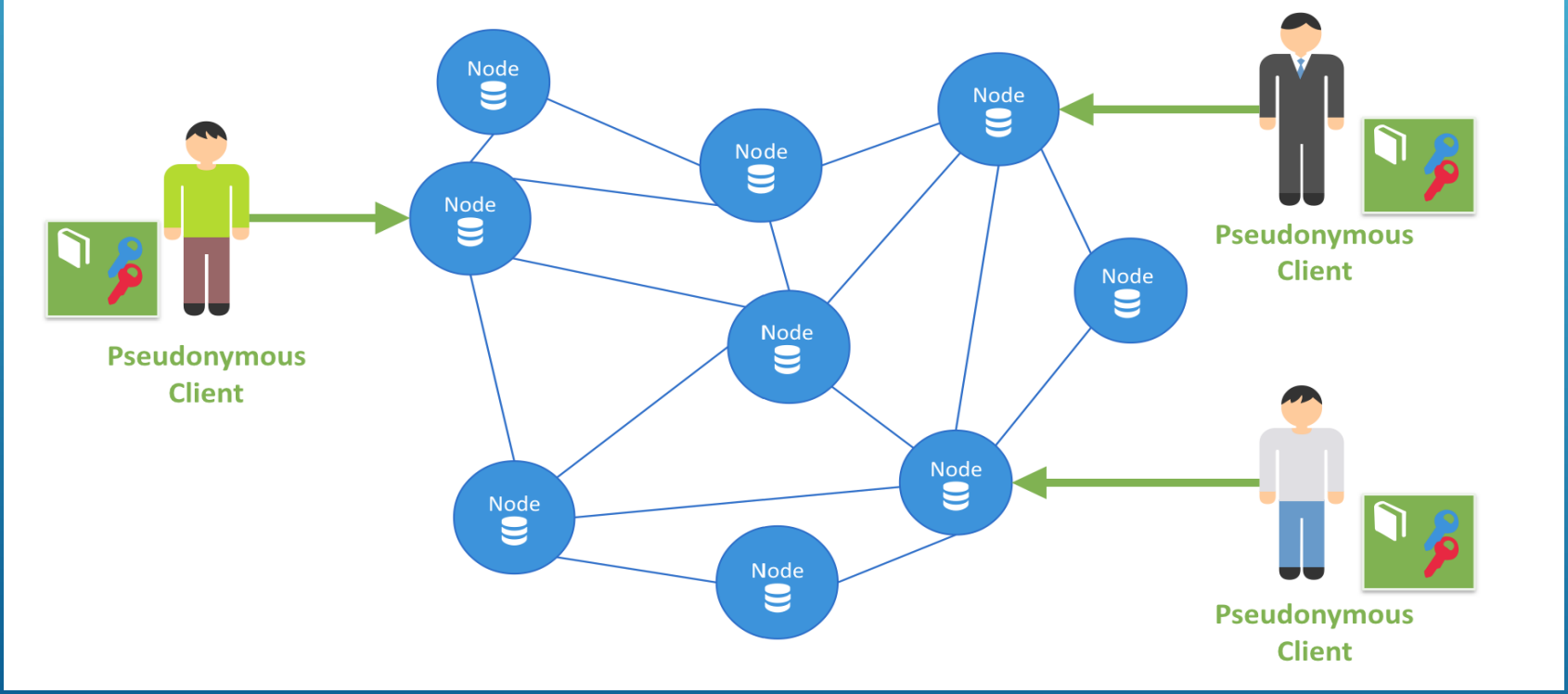


Image source: Scorechain

Consensus components

- **Blockchain structure**
  - Data structure:

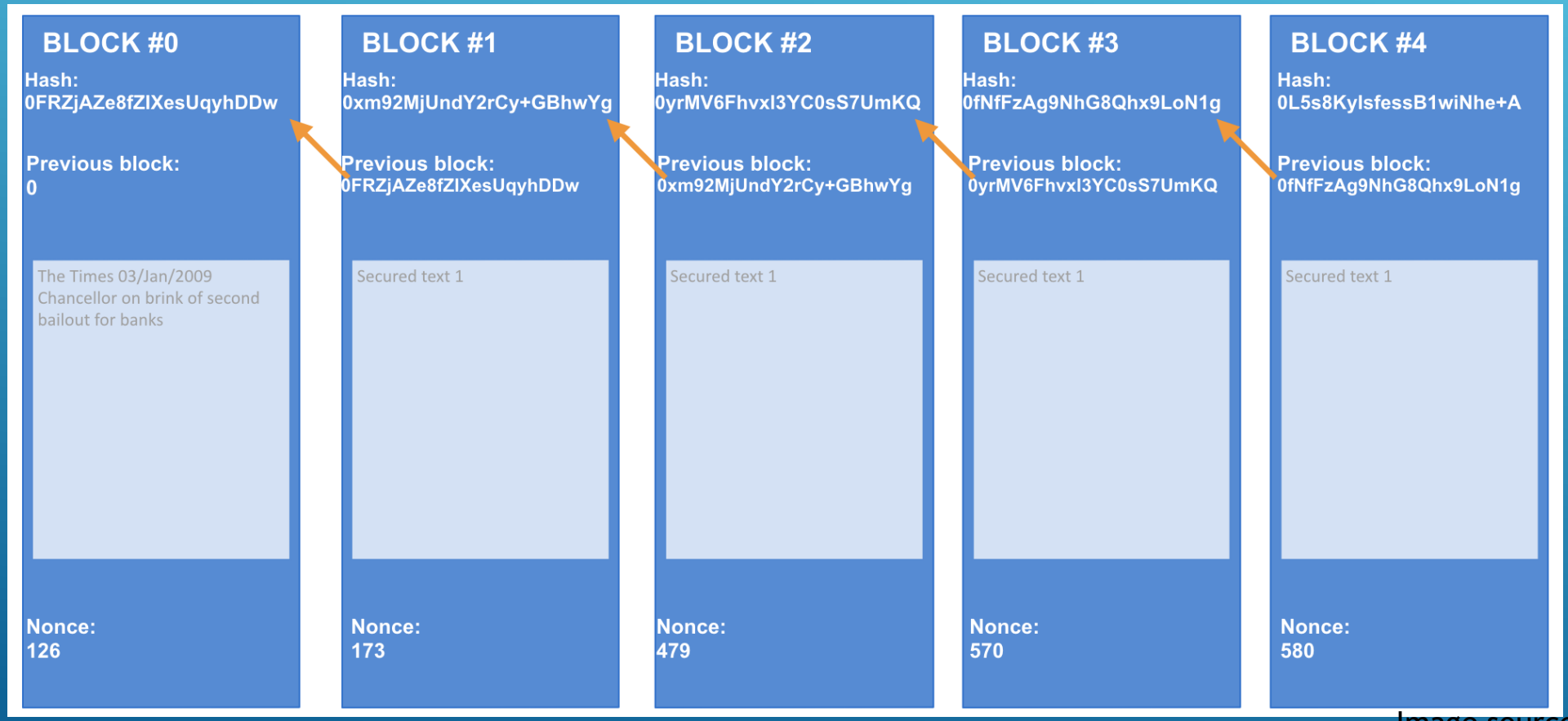


Image source: Scorechain

Consensus components

- **Types of blockchain**
  - There mainly three types of Blockchains that have emerged after Bitcoin introduced Blockchain to the world.
  - ✓ Public Blockchain:

  no one in charge, anyone can participate in reading/writing/auditing the blockchain (i.e. Bitcoin, Litecoin, etc.)

Soucre: https://coinsutra.com/different-types-blockchains

Consensus components

- **Types of blockchain**
  - ✓ Private Blockchain:

  a private property of an individual or an organization, there is one in charge of important things such as read/write or whom to selectively give access to read or vice versa (i.e. Bankchain)

Soucre: https://coinsutra.com/different-types-blockchains

Consensus components

- **Types of blockchain**
  - There mainly three types of Blockchains that have emerged after Bitcoin introduced Blockchain to the world.
  - ✓ Consortium or Federated Blockchain:

  More than one in charge. A group of companies or representative individuals come together and make decisions for the best benefit of the whole network (i.e. r3, EWF)

Soucre: https://coinsutra.com/different-types-blockchains

Smart Contract Theory and architecture

- **Smart Contract Theory**
  - A computer protocol designed digitally facilitate, verify, or enforce the negotiation or performance of a contract.
  - It allows the performance of credible transactions without the third parties.
  - The transactions are traceable and irreversible.

Source: https://en.wikipedia.org/wiki/Smart_contract

Smart Contract Theory and architecture

- **Smart Contract architecture**

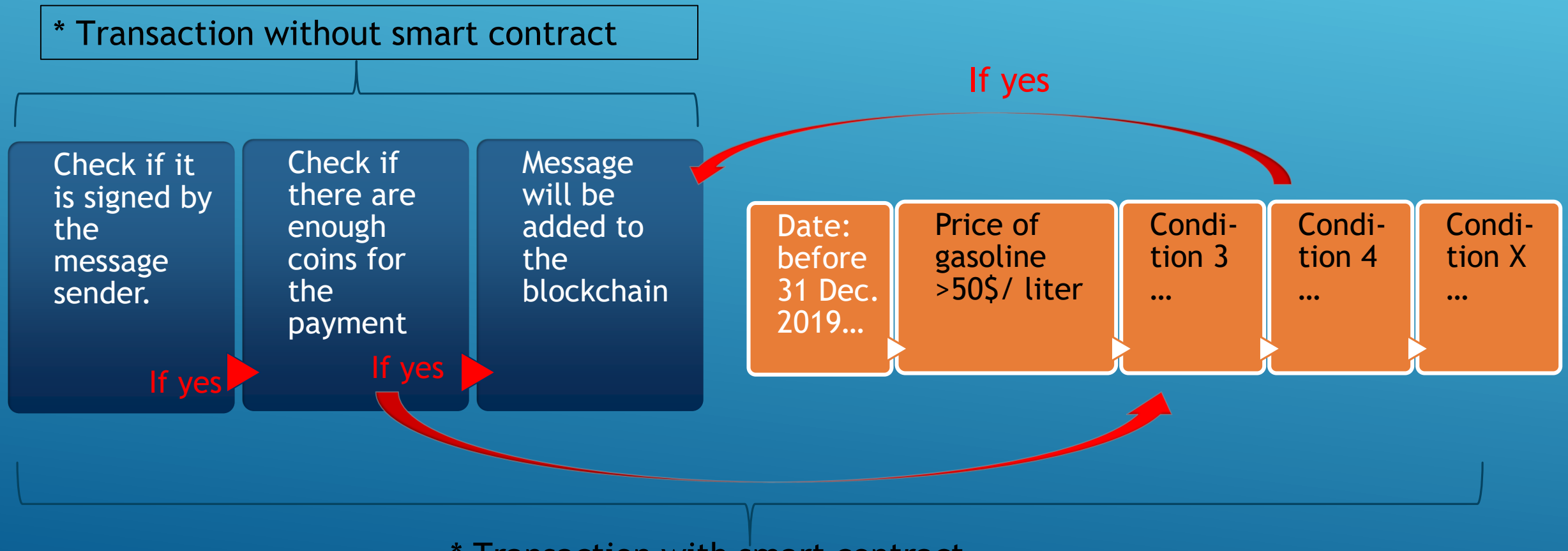


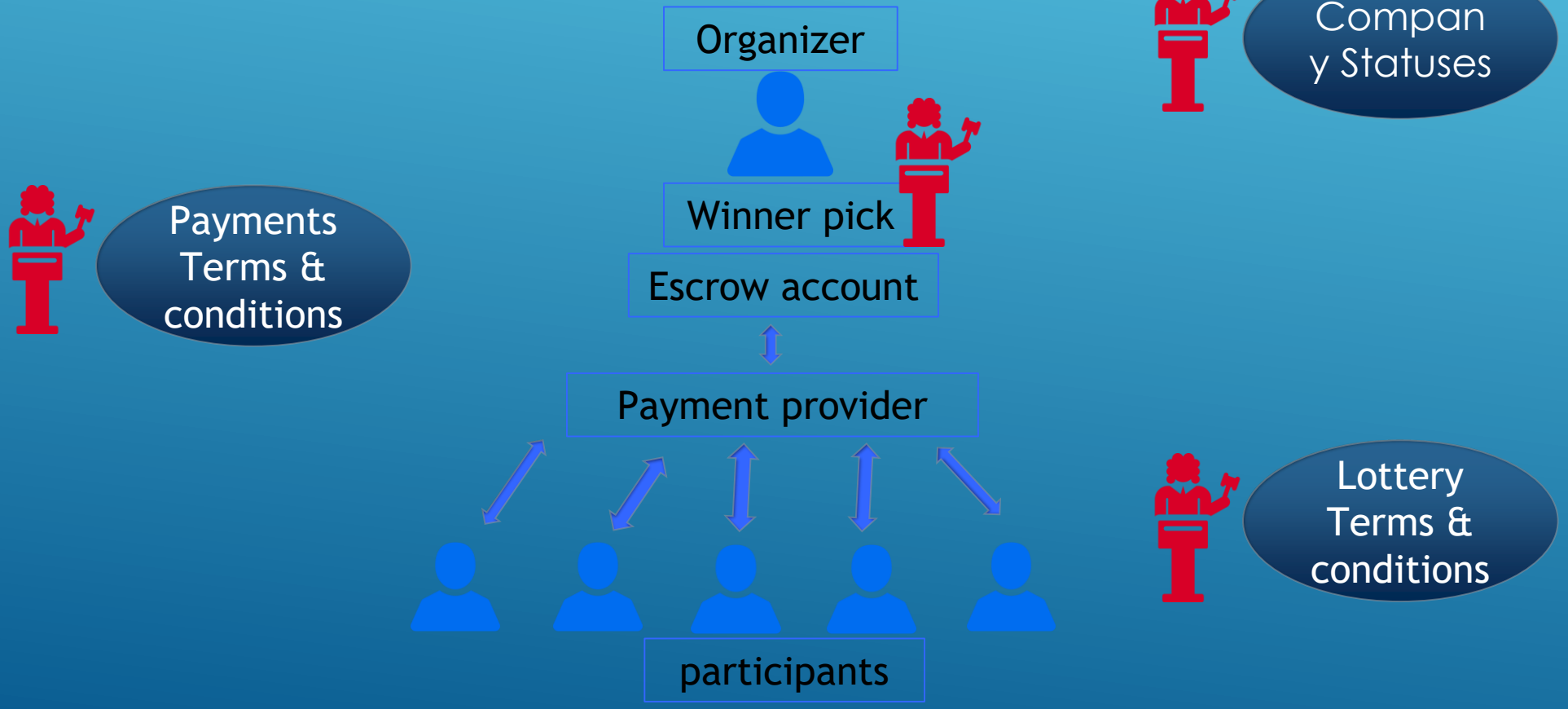
Image source: Scorechain

Architectures and decentralized autonomous systems

- DAO (Decentralized Autonomous Organization)
  - An organization represented by rules encoded as a computer program, which is transparent, controlled by shareholders and not influenced by a central government.
  - It's notionally like the example for getting funds for a small conference, except that it includes much more. Members buy shares in the DAO and can vote on things according to the number of shares they have. The dreamers have the idea they'll replace Democracy and run entire countries this way.
  - The DAO was the largest crowdfunding in history, having raised over $150m from more than 11,000 enthusiastic members. (ICO)
  - A DAO’s financial transaction record and program rules are maintained on a blockchain.

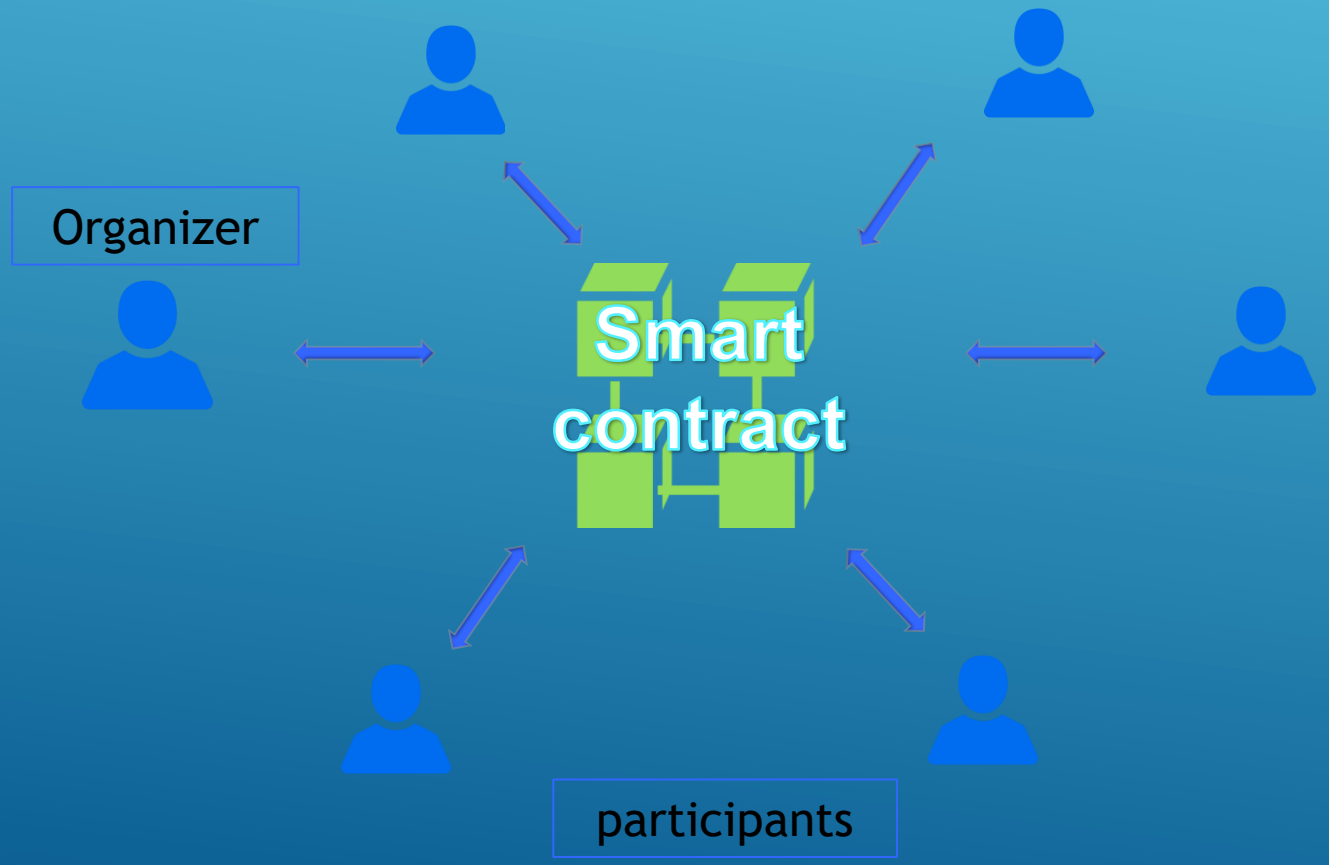
Smart contract application

- **Example 1: Lottery**
  - Lottery without smart contract



Smart contract application

- **Example 1: Lottery**
  - Lottery with smart contract

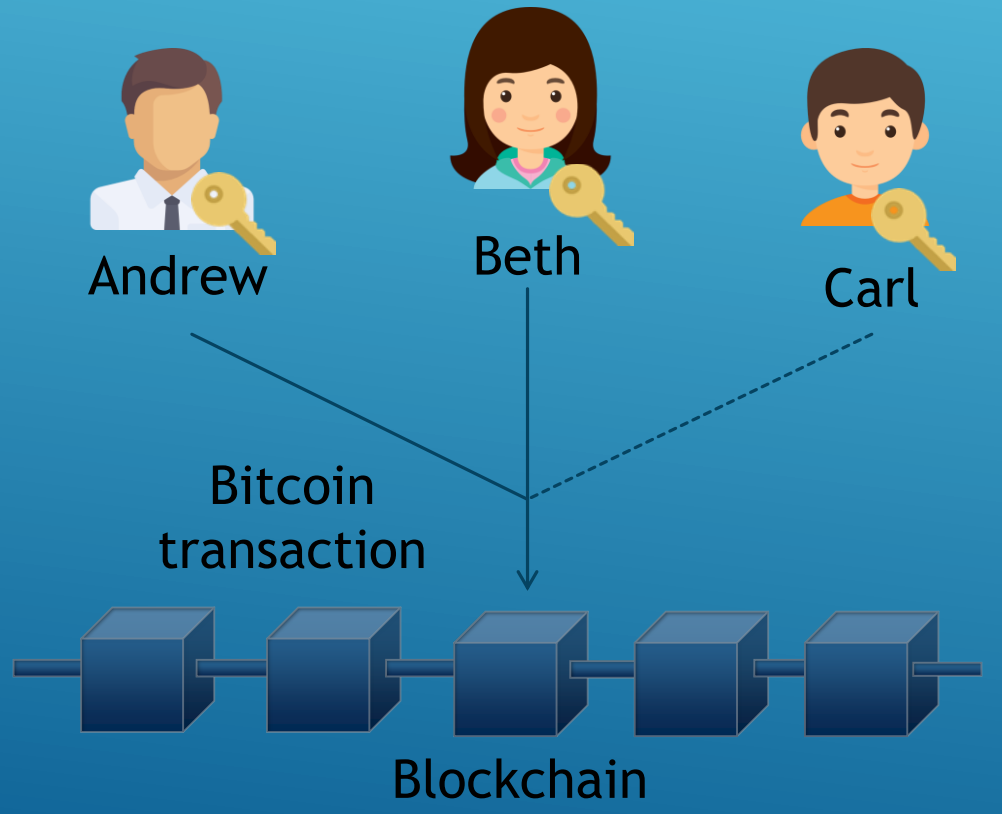


Source: https://www.slideshare.net/ThomasCharlesVanderstraeten/ethereum-smart-contract-101-with-cryptizensio

Smart contract application

- **Example 2-1: Group wallets**
  - Enforcing at least 2 out of 3 people of a group to agree to create a valid transaction

```
2 <pubKeyAndrew>
<pubKeyBeth>
<pubKeyCarl> 3
CHECKMULTISIG
```

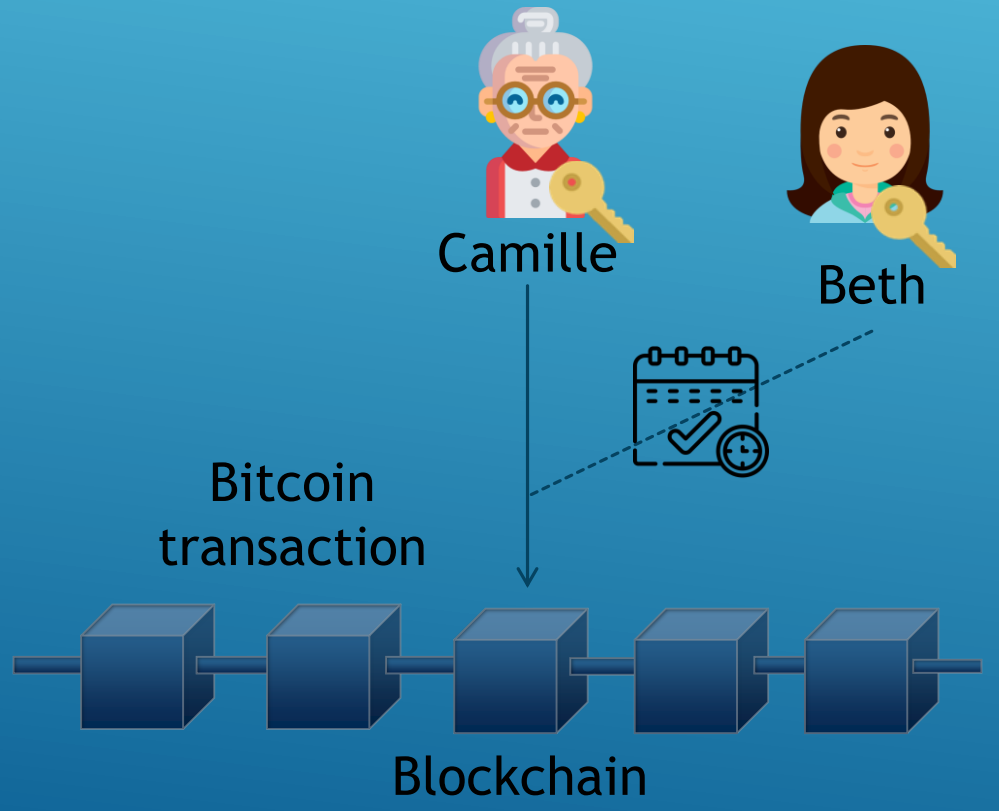


Source: https://www.slideshare.net/FedericoTenga/state-smart-contract-ttechnologies

Smart contract application

- **Example 2-2: Heritage wallets**
  - Enforcing that a transaction must be signed either by Camille OR by Beth after 5 years

```
IF
   <pubKeyCamille>
   CHECKSIG
ELSE
   <5 y> CLTV DROP
   <pubKeyBeth>
    CHECKSIG
ENDIF
```

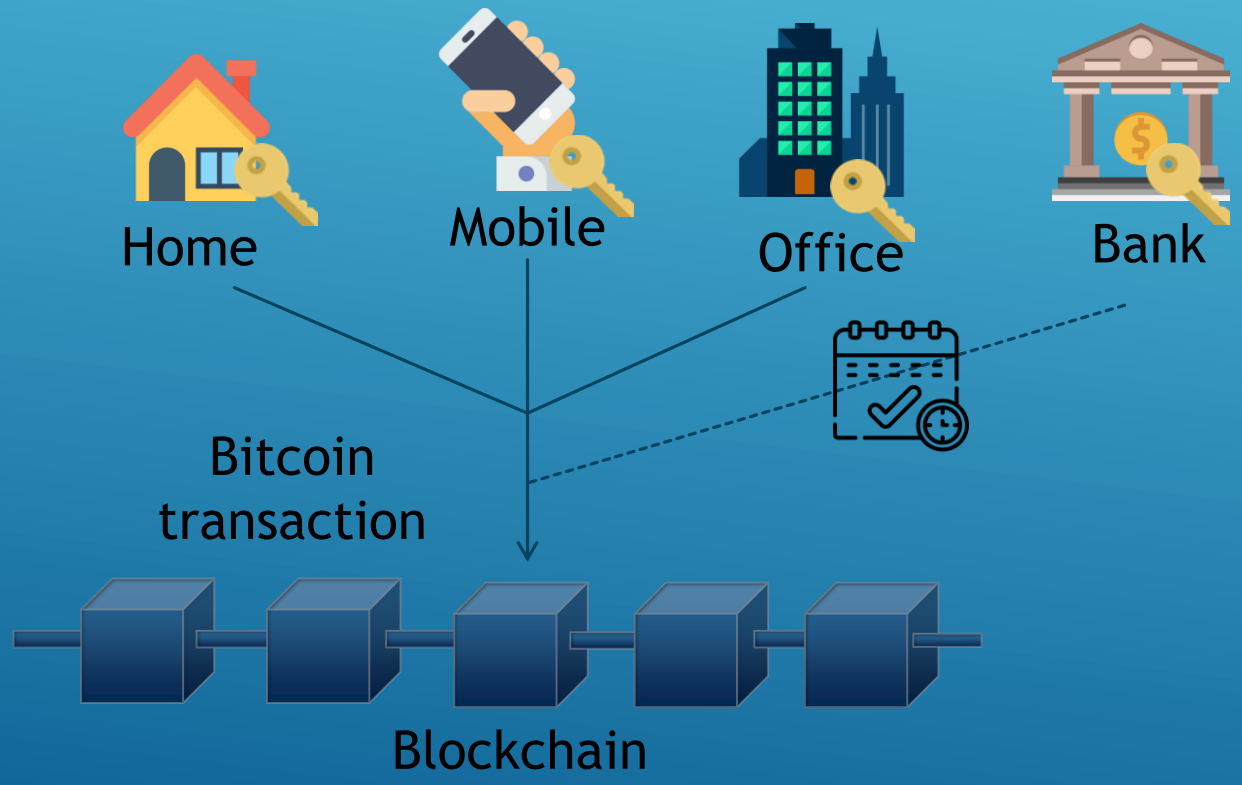


Source: https://www.slideshare.net/FedericoTenga/state-smart-contract-ttechnologies

Smart contract application

- **Example 2-3: Secure storage**
  - Enforcing that a transaction must be signed by either 3 devices in different locations OR a recovery key deposited in the bank after 8 months

```
IF
        3 <pubKeyHome>
         <pubKeyMobile>
        <pubKeyOffice> OP_3
         CHECKMULTISIG
ELSE
        <8 m> CLTV DROP
        <pubKeyBank>
        CHECKSIG
ENDIF
```



Source: https://www.slideshare.net/FedericoTenga/state-smart-contract-ttechnologies

Existing blockchain applications, related structures and architectures

- **ERC-20**
  - Proposed on November 19, 2015 by Fabian Vogelsteller.
  - A technical standard used for smart contracts on the Ethereum blockchain for implementing tokens. (ERC: Ethereum Request for Comment, 20: the number that was assigned to this request.)
  - It defines a common list of rules that an Ethereum token has to implement, allowing developers to program how new tokens will function within the Ethereum ecosystem. These rules include how the tokens are transferred between addresses and how data within each token is accessed.
  - + 142,200 ERC-20 token contracts (as of November 19, 2018): EOS, Bancor, Qash, etc…

Source: https://en.wikipedia.org/wiki/ERC-20

Existing blockchain applications, related structures and architectures

- **ERC-721: a class of unique tokens**
  - A free, open standard that describes how to build non-fungible or unique tokens on the Ethereum blockchain. While most tokens are fungible (every token is the same as every other token, i.e.ERC-20), ERC-721 tokens are all unique.
  - It defines a minimum interface a smart contract must implement to allow unique tokens to be managed, owned and traded.

Existing blockchain applications, related structures and architectures

- **ERC-725: Ethereum Identity Standard**
  - A proposed standard for blockchain-based identity which lives on the Ethereum blockchain.
  - It describes proxy smart contracts that can be controlled by multiple keys and other smart contracts, it can describe humans, groups, objects and machines.
  - Users should be able to own and manage their identity instead of ceding ownership of identity to centralized organizations.

Reference

1. The Innovation Ultimatum: Six strategic technologies that will reshape every business in the 2020s By Steve Brown.
2. Bank 4.0: Banking Everywhere, Never at a Bank By Brett King.
3. The World of Digital Payments: Practical Course By Pavlo Sidelov.
4. The PayTech Book Edited by a team of Susanne Chishti.
5. The Future Is Faster Than You Think: How Converging Technologies Are Disrupting Business, Industries, and Our Lives By Dr. Peter H. Diamandis.
6. Advances in Financial Machine Learning By Marcos Lopez de Prado
7. Financial Services Revolution: How Blockchain is Transforming Money, Markets, and Banking By Alex Tapscott.
8. The STO Financial Revolution: How Security Tokens Change Businesses Forever By Alex Nascimento.
9. FinTech Founders: Inspiring Tales from the Entrepreneurs that are Changing Finance By Agustín Rubini
10. The Innovation Ultimatum: Six strategic technologies that will reshape every business in the 2020s By Steve Brown