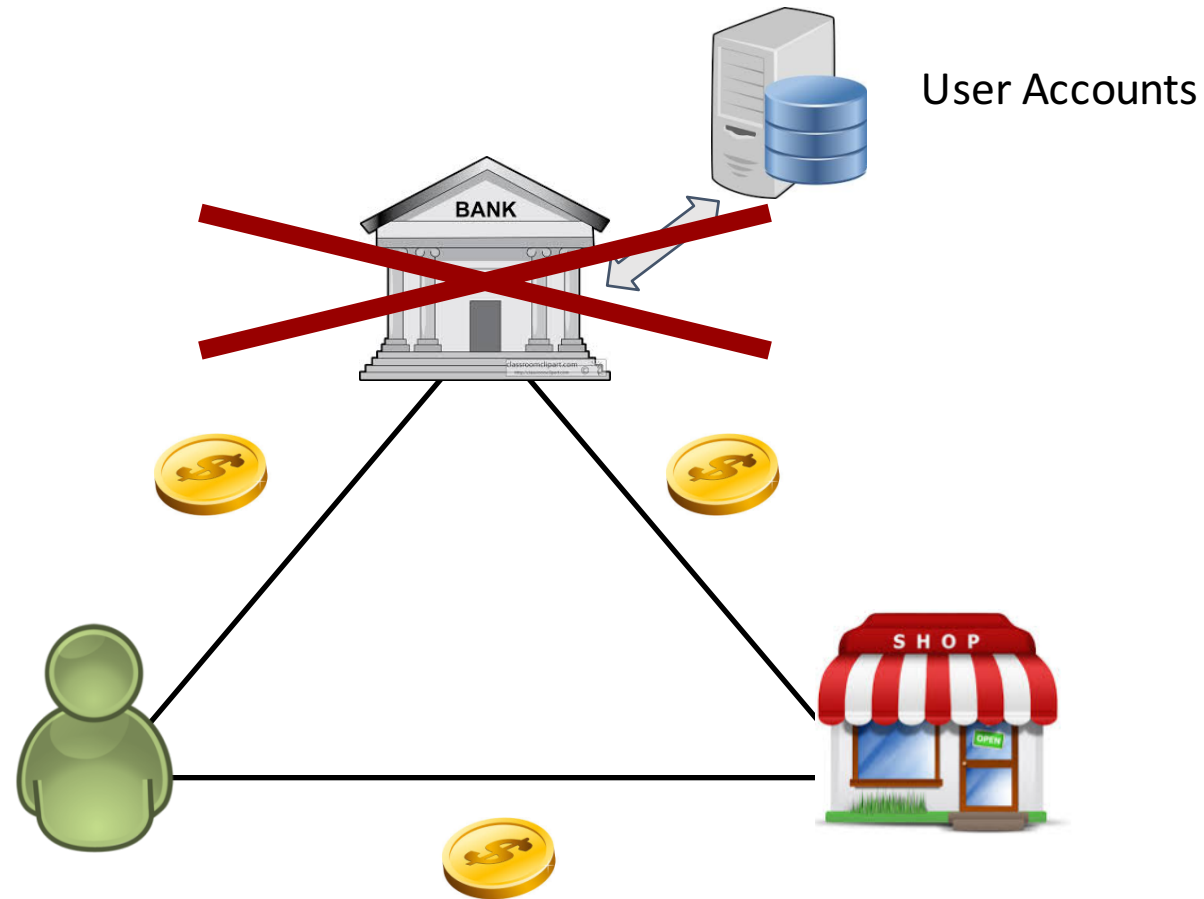


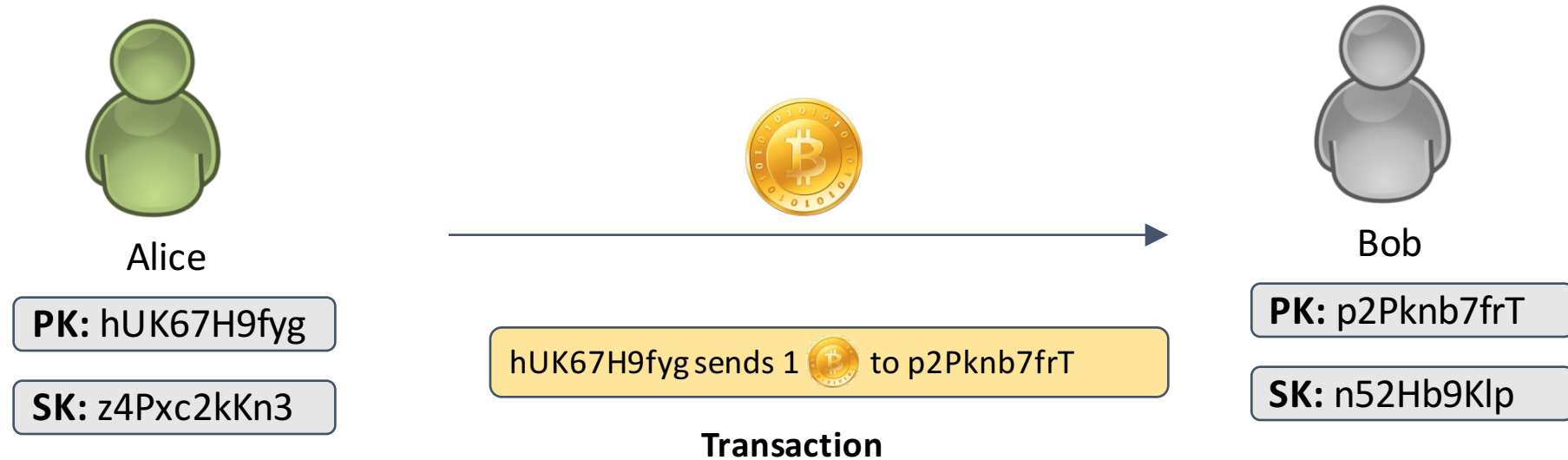
Blockchain-based Discussion Forum

ZHANG Haoqian, ZHAO Yancheng, YI Ke

Eliminating Centralized Authority

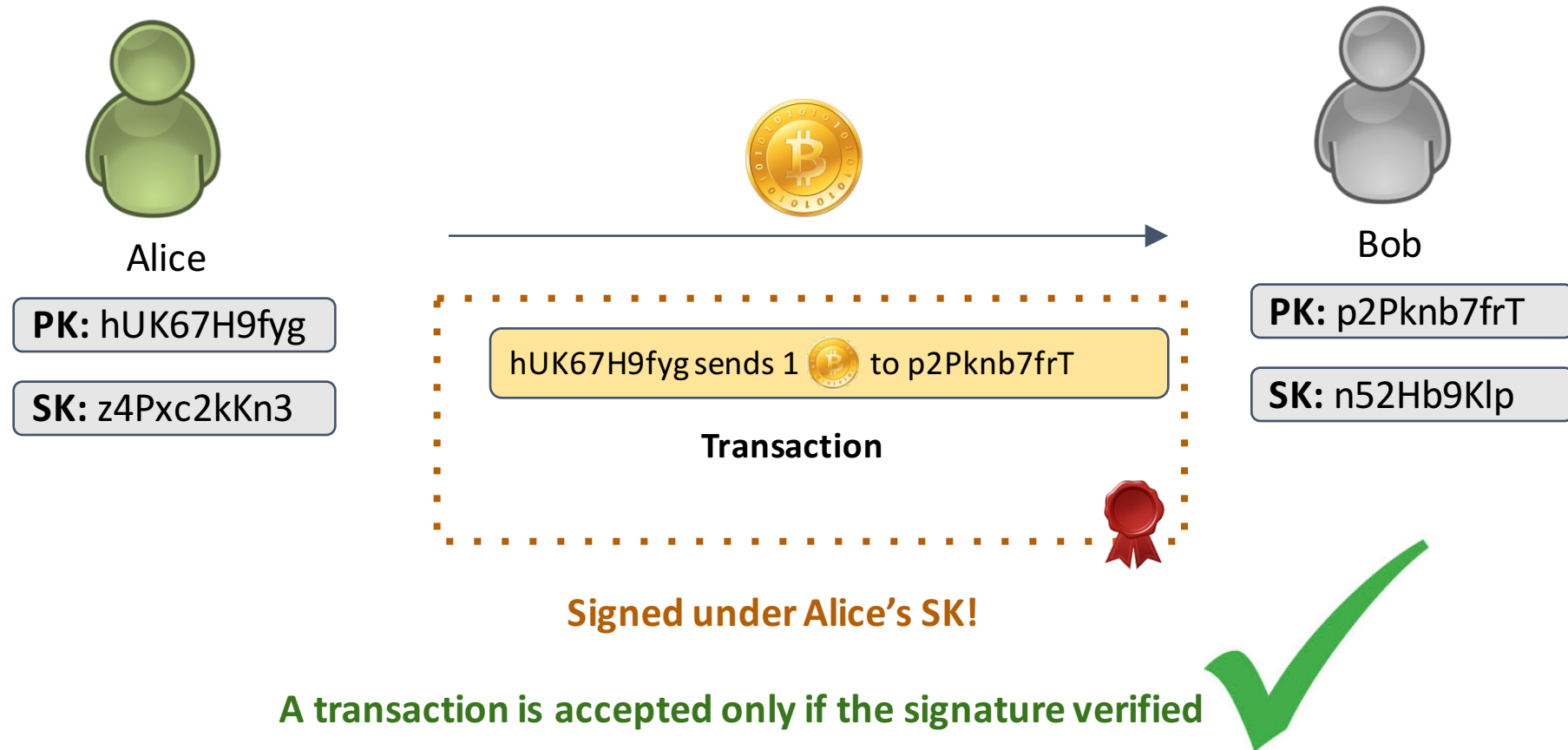


Bitcoin Transactions

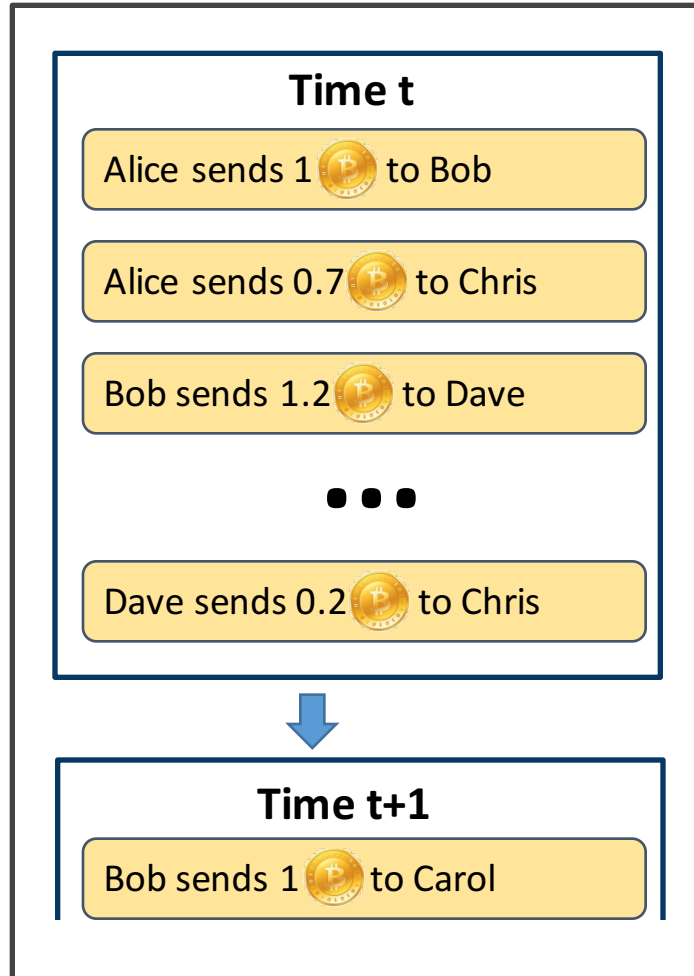


Bitcoin Transactions

Based on digital signatures

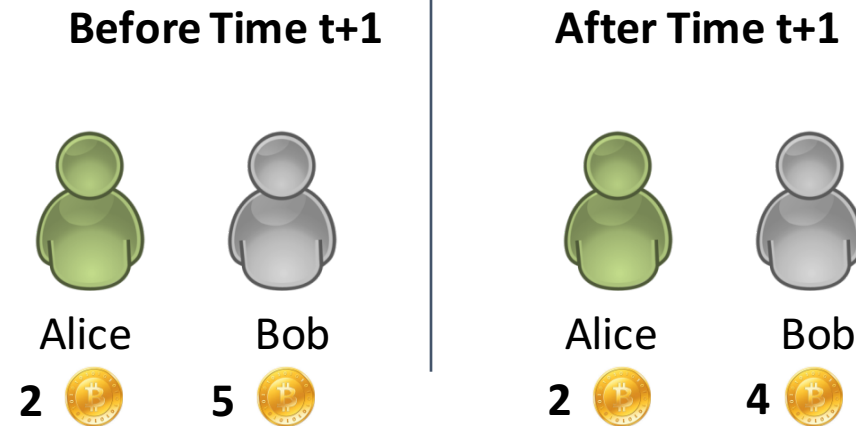


Transaction Ledger

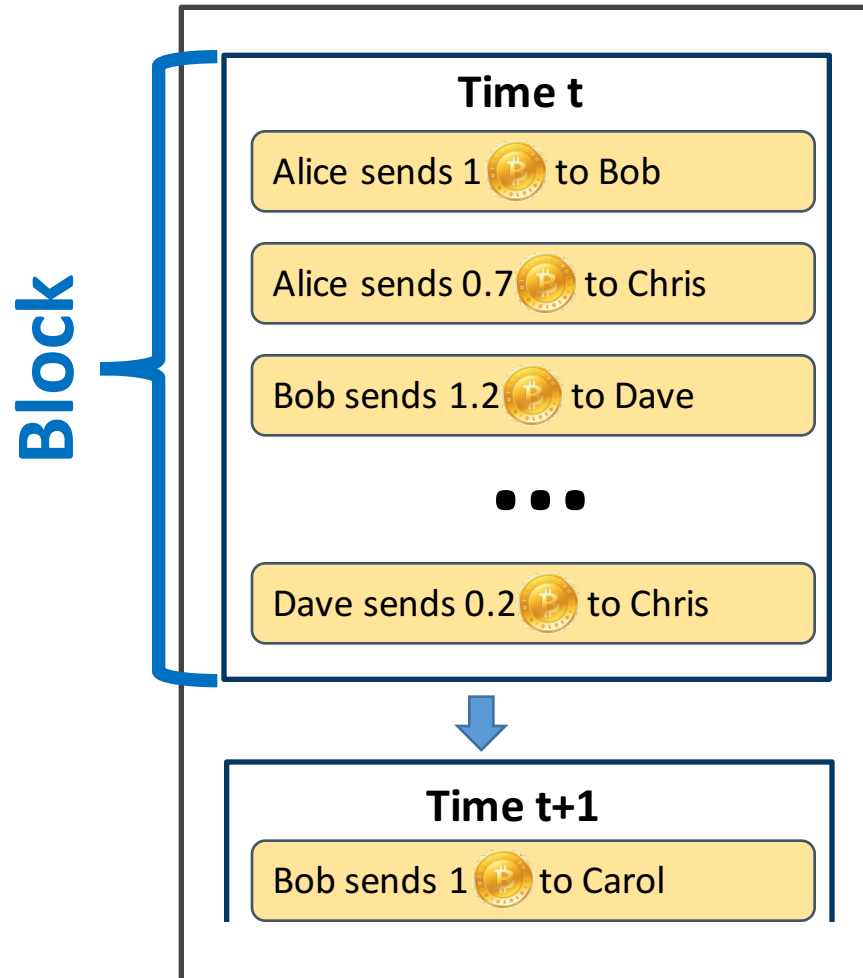


- Stores every transaction and is used to check users' balances
- Database

Example



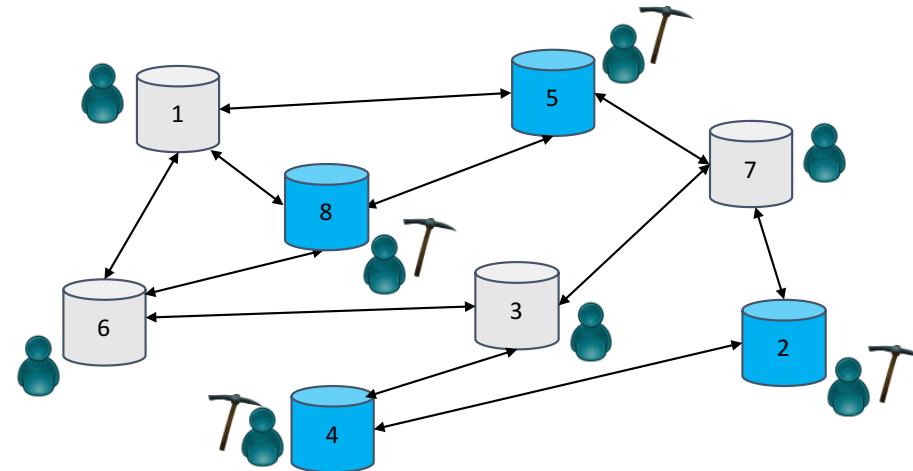
Blockchain



➤ Who maintains it?

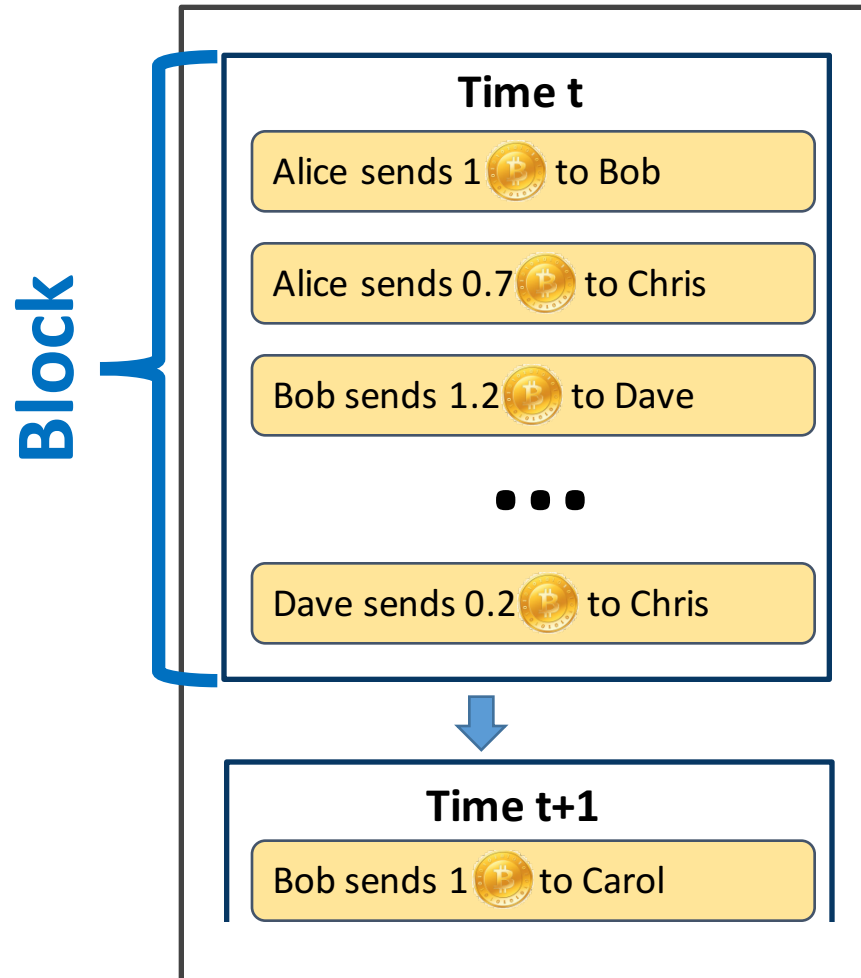


➤ The users themselves!



Miners: special types of users

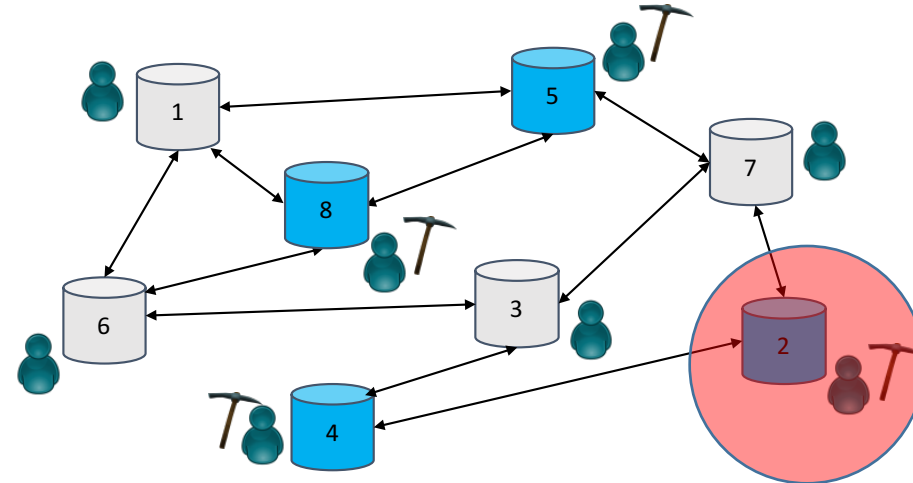
Blockchain



➤ Who maintains it?

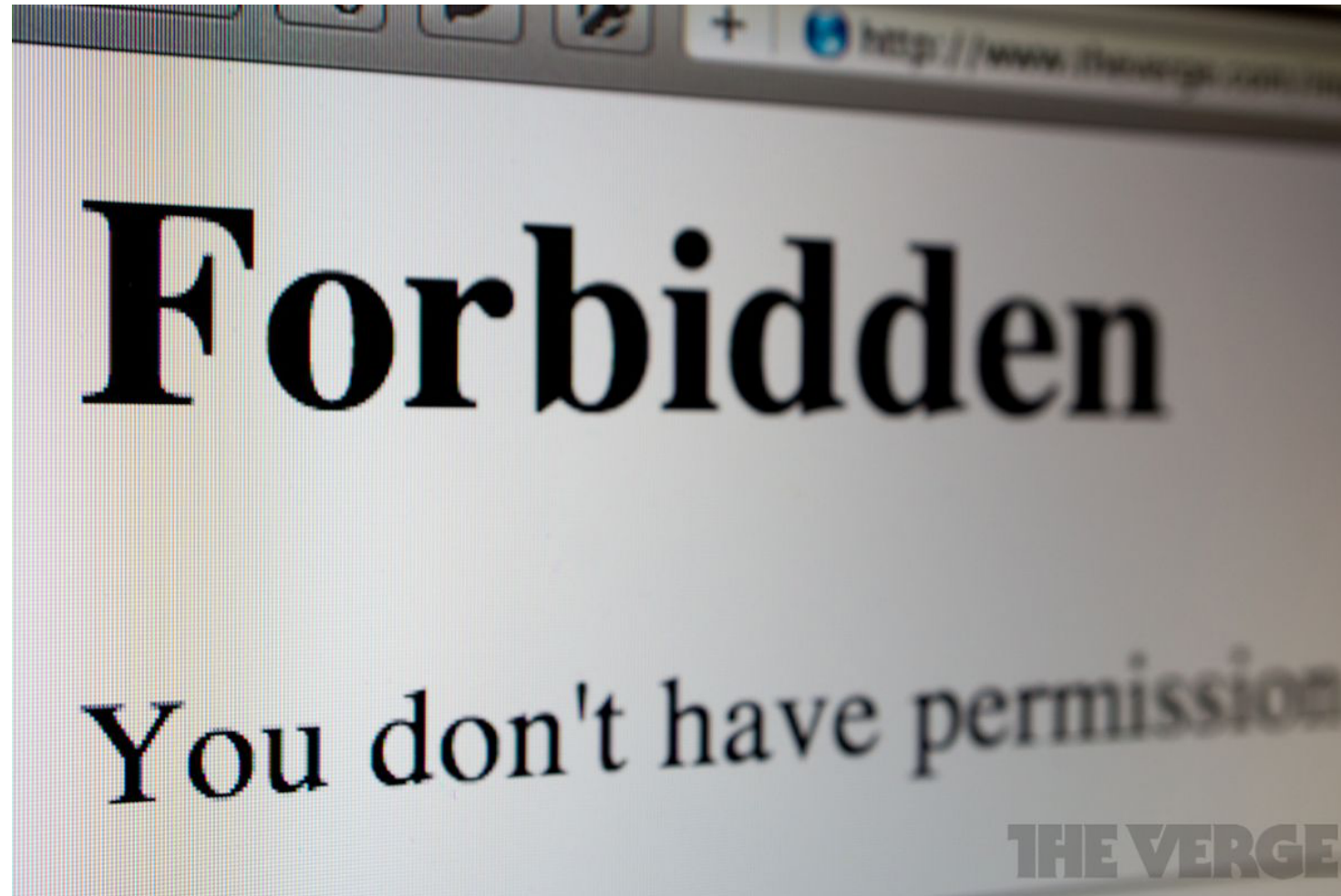


➤ The users themselves!

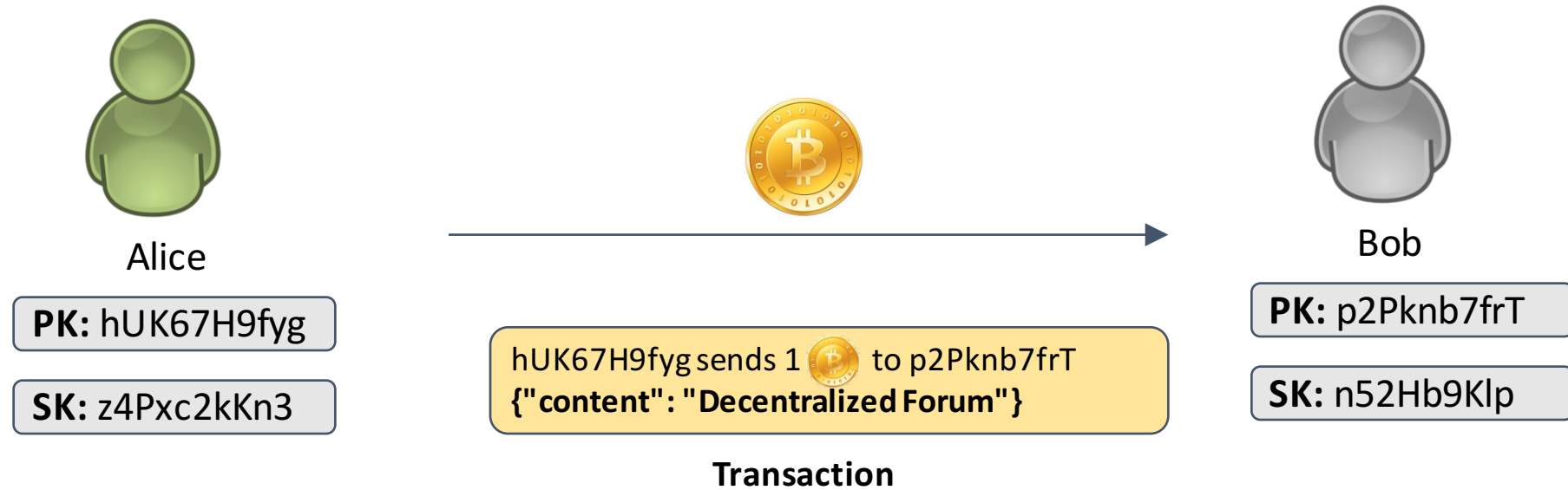


One miner will be chosen to write transactions into the Blockchain

Government Censorship



Solution1: Bitcoin Transactions with JSON

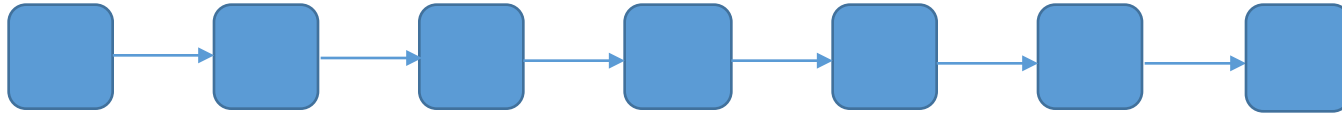


Solution2 : Multiple Chains With P2P Network

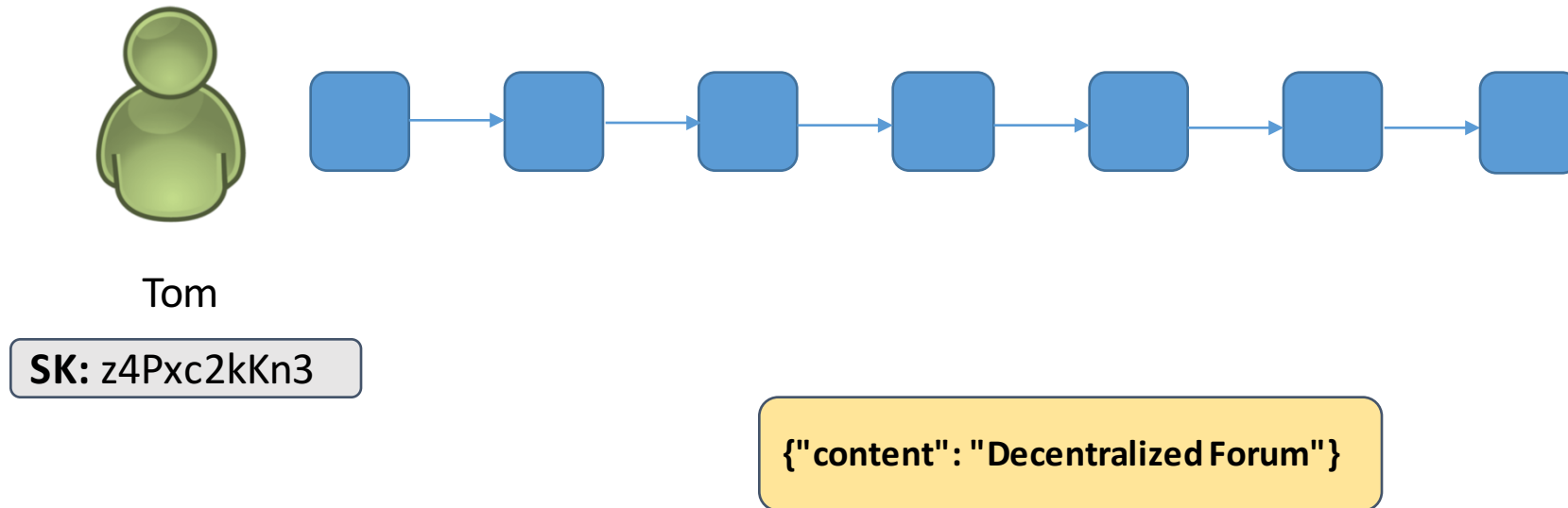


Tom

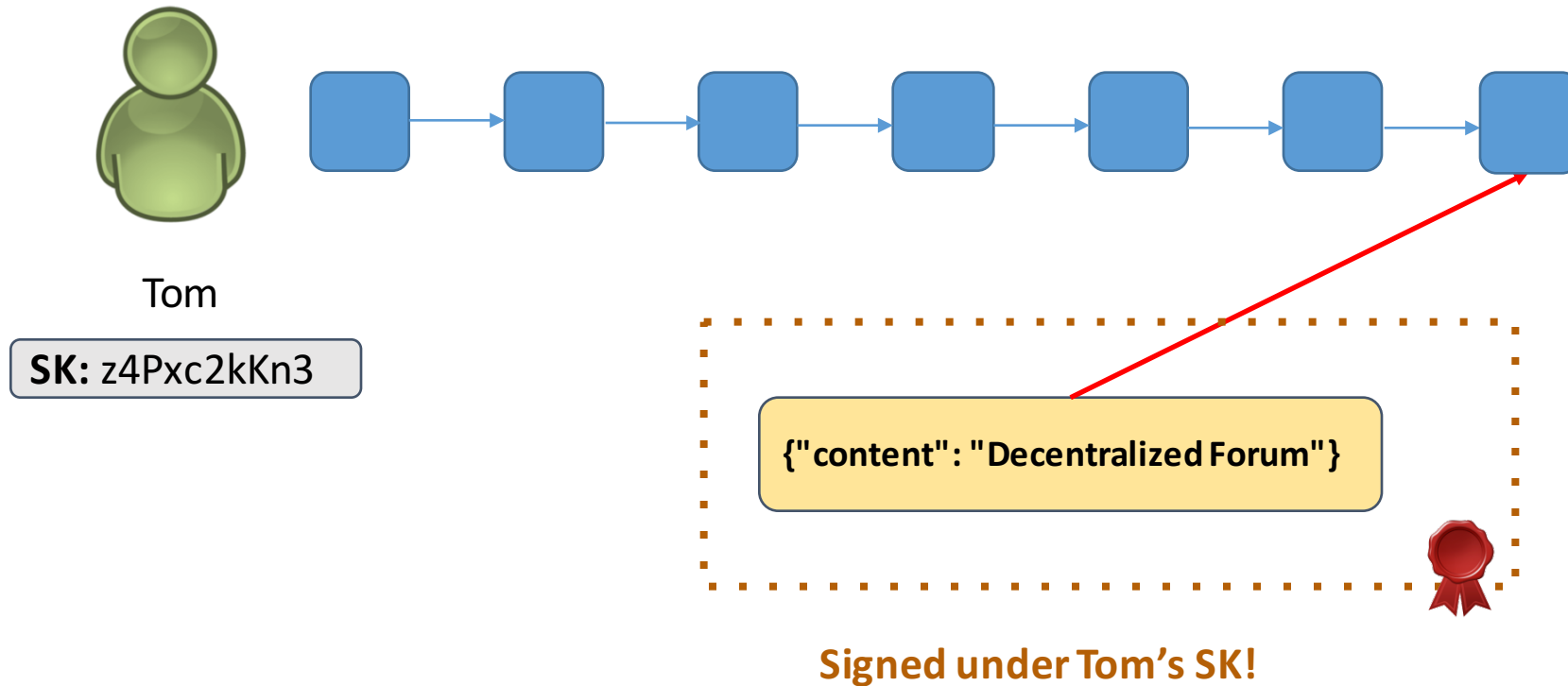
SK: z4Pxc2kKn3



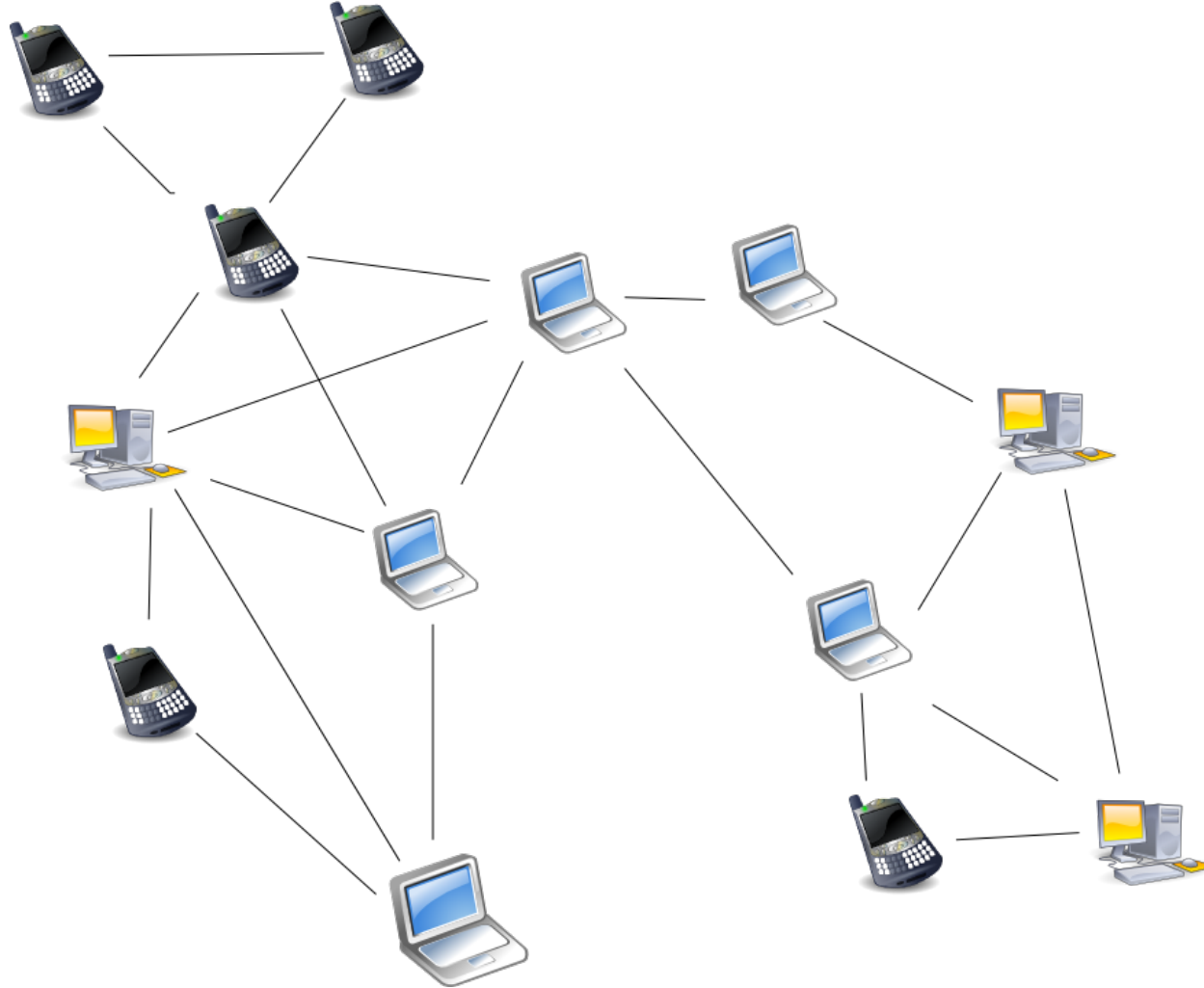
Solution2 : Multiple Chains With P2P Network



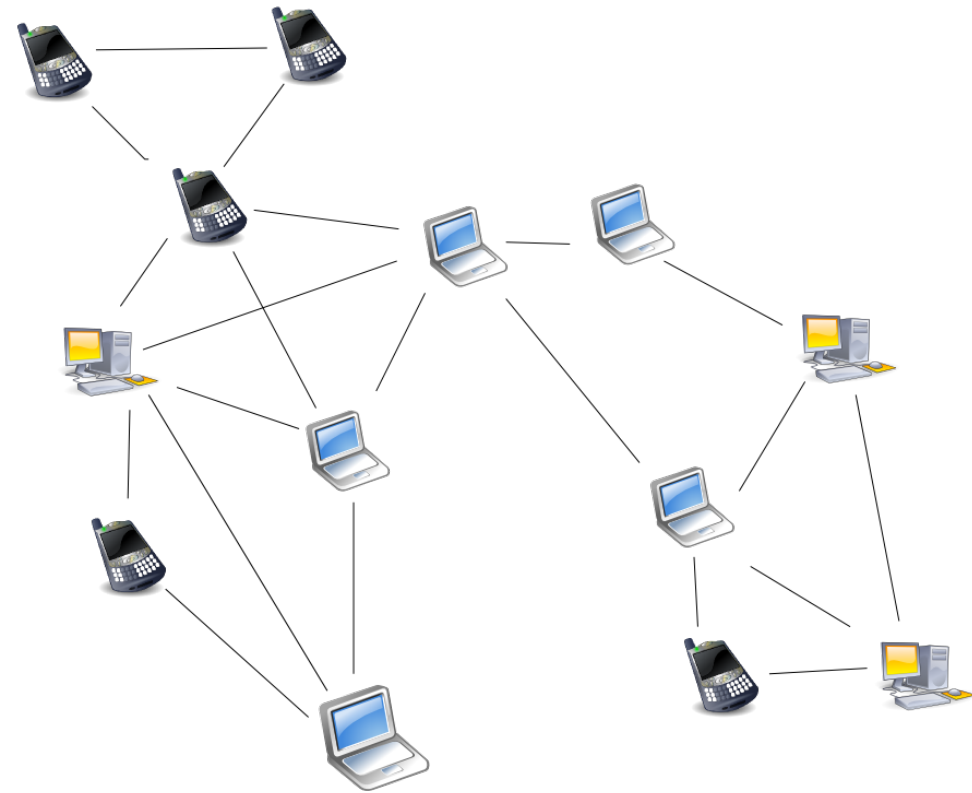
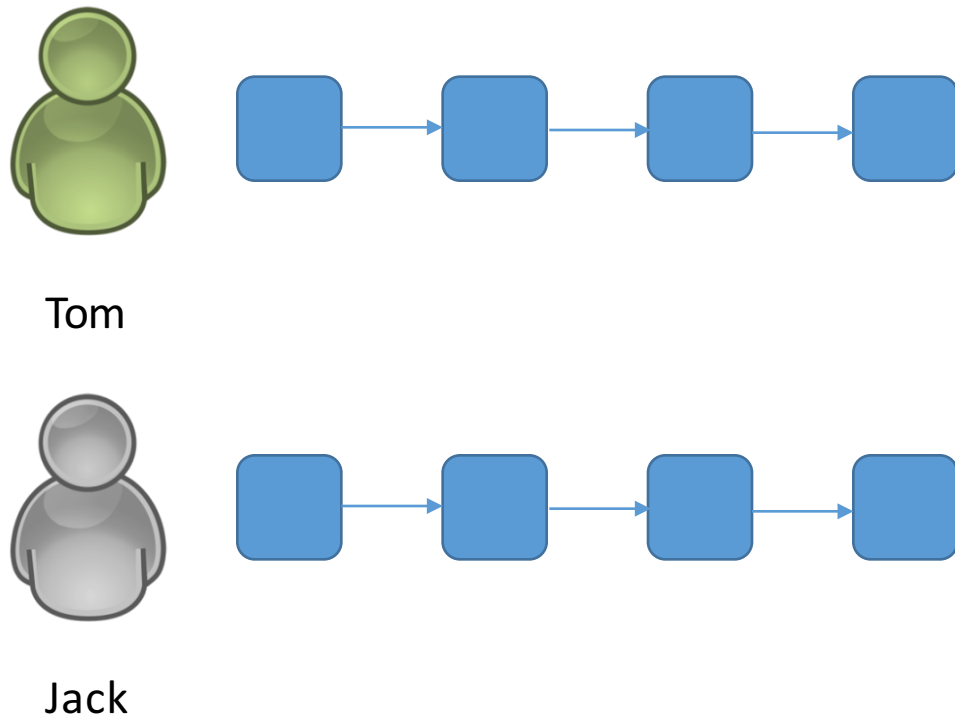
Solution2 : Multiple Chains With P2P Network





Solution2 : Multiple Chains With P2P Network



Solution2 : Multiple Chains With P2P Network




What we have done so far

Login 

MAIN >> GENERAL DISCUSSION >> TITLE

Blockchain - Wiki



Vergil
Post: 2

A **blockchain**, originally **block chain**, is a growing list of records, called blocks, which are linked using cryptography. Each block contains a cryptographic hash of the previous block, a timestamp, and transaction data (generally represented as a merkle tree root hash).

By design, a blockchain is resistant to modification of the data. It is "an open, distributed ledger that can record transactions between two parties efficiently and in a verifiable and permanent way". For use as a distributed ledger, a blockchain is typically managed by a peer-to-peer network collectively adhering to a protocol for inter-node communication and validating new blocks. Once recorded, the data in any given block cannot be altered retroactively without alteration of all subsequent blocks, which requires consensus of the network majority. Although blockchain records are not unalterable, blockchains may be considered secure by design and exemplify a distributed computing system with high Byzantine fault tolerance. Decentralized consensus has therefore been claimed with a blockchain.


Blockchain was invented by Satoshi Nakamoto in 2008 to serve as the public transaction ledger of the cryptocurrency bitcoin. The invention of the blockchain for bitcoin made it the first digital currency to solve the double-spending problem without the need of a trusted authority or central server. The bitcoin design has inspired other applications, and blockchains which are readable by the public are widely used by cryptocurrencies. Private blockchains have been proposed for business use. Some marketing of blockchains has been called "snake oil".

Submitted at: Just now

Post a new Reply

Content

Great description.

 Styling with Markdown is supported

PUBLISH REPLY

What we have done so far



Works needed to be done

- Coding
 - Multi Chains Library
 - P2P network Library (websocket)
- Paper
 - The Web Conference (Deadline Oct 29th 2018)

Resource

- Bitcoin: A Peer-to-Peer Electronic Cash System
- CSIT 5710: Cryptography and Security (Fall 2019)
- Princeton University: Bitcoin and Cryptocurrency Technologies

Question?