Bitcoin

https://bitcoin.org/bitcoin.pdf

The Greatest Mystery Invention?

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 proof-of-work chain as proof of what happened while they were gone.

1. Introduction

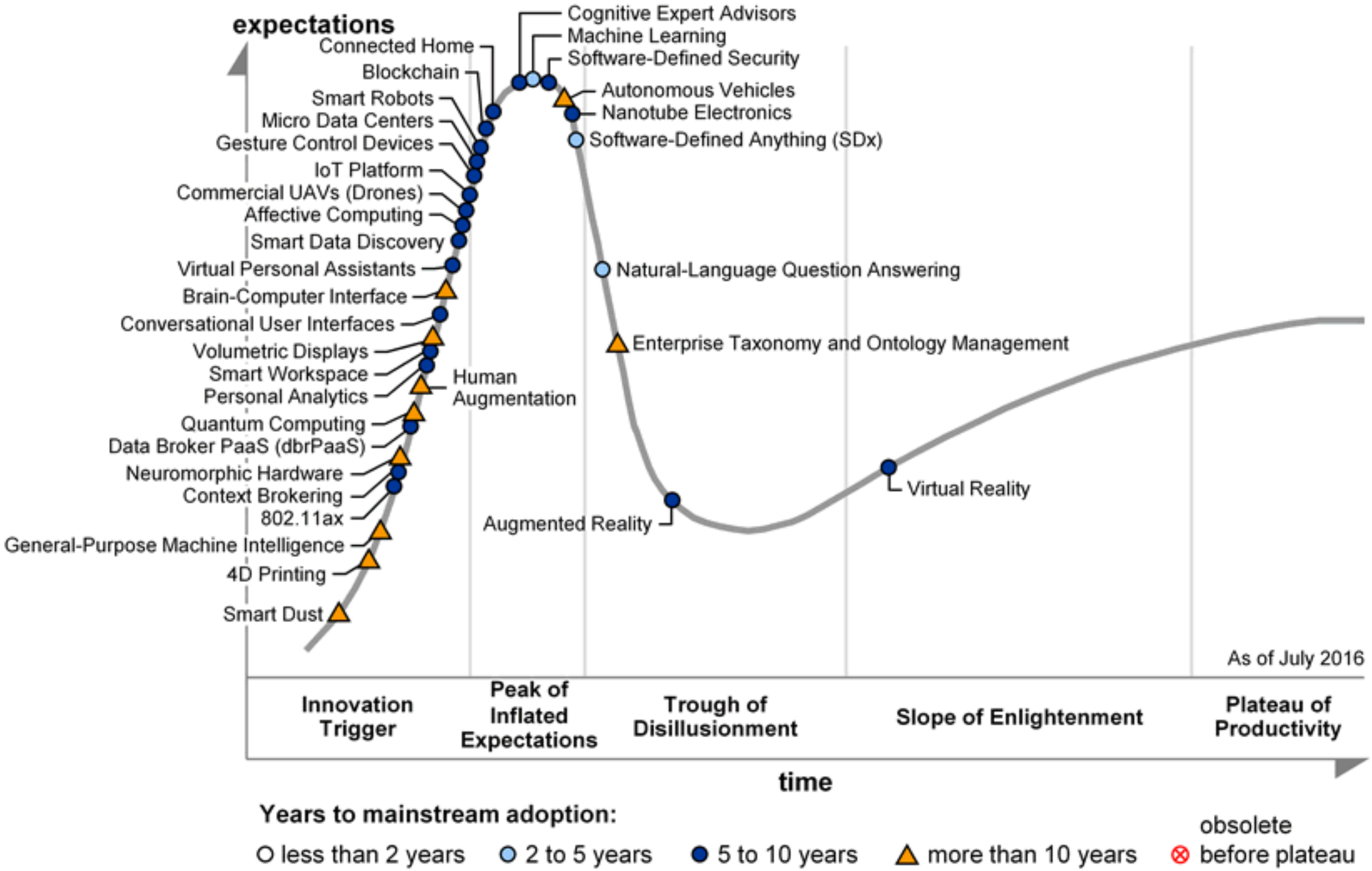
Commerce on the Internet has come to rely almost exclusively on financial institutions serving as trusted third parties to process electronic payments. While the system works well enough for most transactions, it still suffers from the inherent weaknesses of the trust based model. Completely non-reversible transactions are not really possible, since financial institutions cannot avoid mediating disputes. The cost of mediation increases transaction costs, limiting the minimum practical transaction size and cutting off the possibility for small casual transactions, and there is a broader cost in the loss of ability to make non-reversible payments for non-reversible services. With the possibility of reversal, the need for trust spreads. Merchants must be wary of their customers, hassling them for more information than they would otherwise need.

https://bitcoin.org/bitcoin.pdf

UCD DUBLIN

Gartner Hype Cycle (July 2016)

https://en.wikipedia.org/wiki/Hype_cycle



What's the big deal?

I give you a gold sovereign for your horse…

I give you £50 for your horse…

I give you a cheque for £360 for your horse..

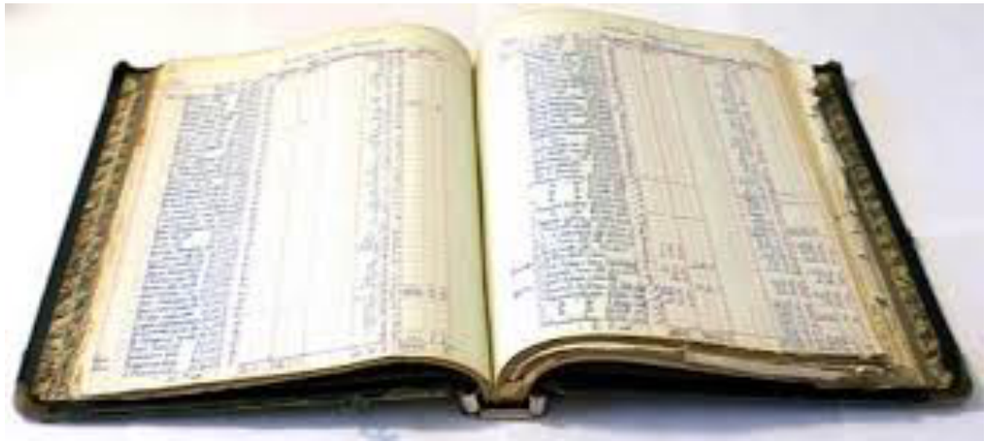
What's the big deal?

I give you a cheque for £360 for your horse..

What stops me writing another cheque for another horse?

The double spend problem

Bank keeps a ledger



2008 Financial Crisis

Bitcoin

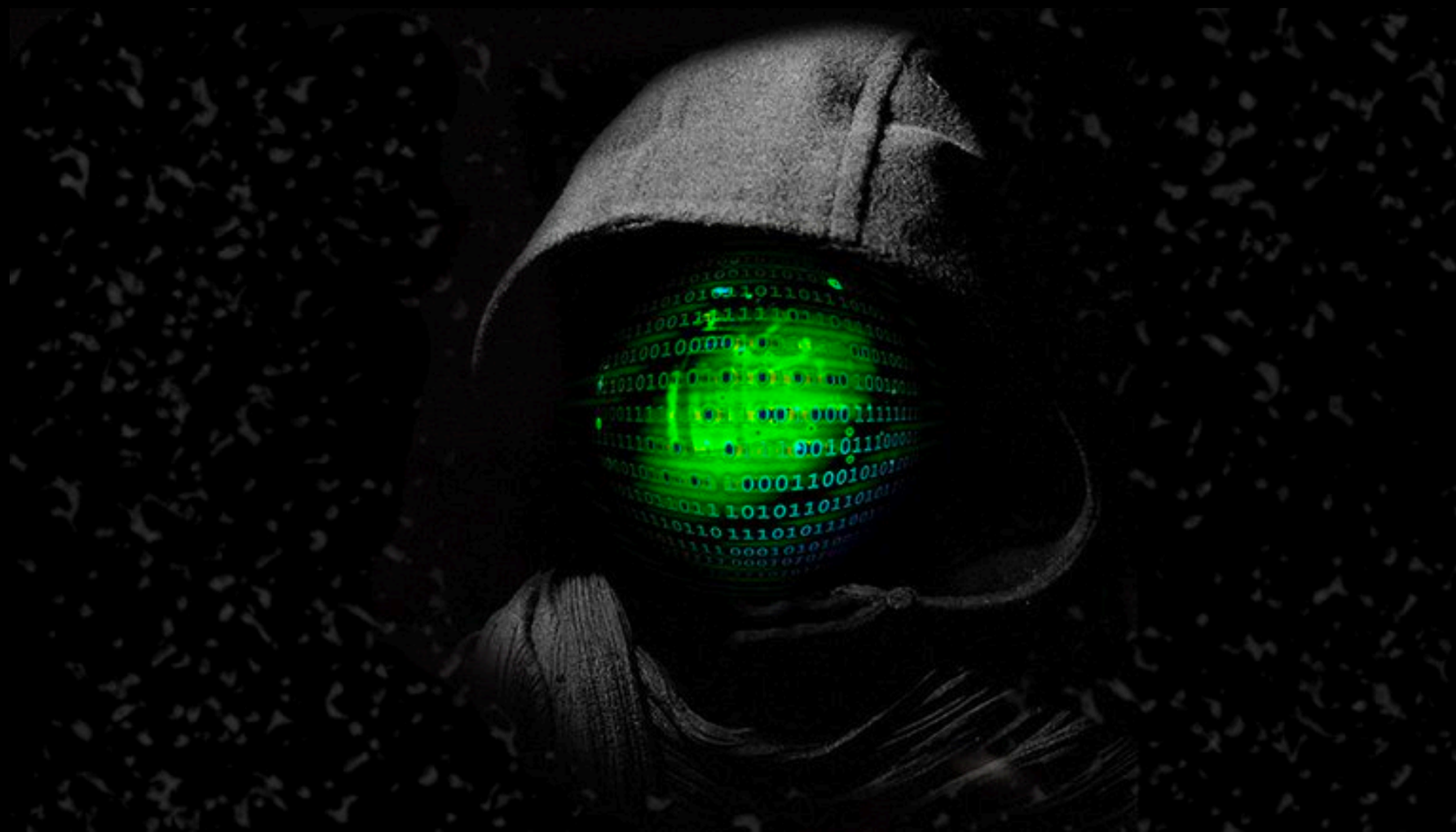
Digital Currency

Prevent double spending

Crypto allows us to ‘create’ tokens/assets that can be owned

How can receiver know that asset was not already spent?

Keep a central public ledger of all transactions
We don't want a centralised system



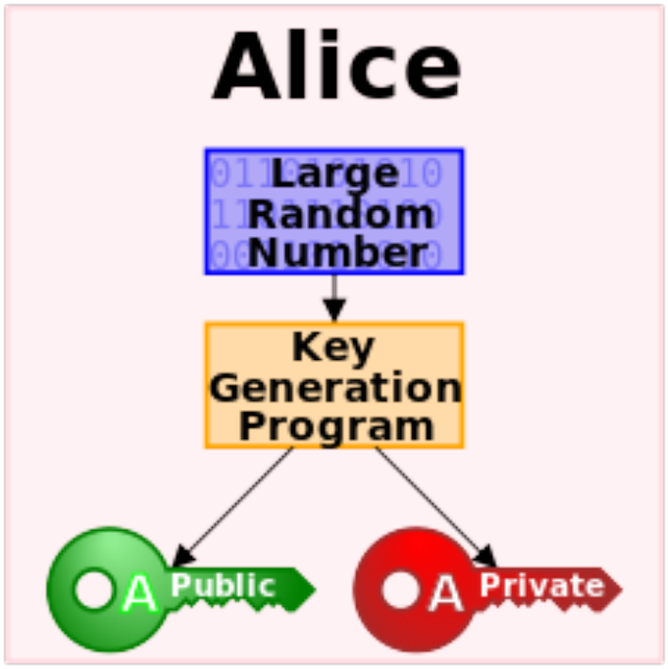
Bitcoin 4 key technologies

It represents the culmination of decades of research in cryptography, distributed system and essentially 4 key technologies:

1. A decentralised p2p network (the bitcoin protocol)
2. A public transaction ledger for storing transactions (blockchain)
3. A set of rules for independent transaction validation and currency issuance (consensus rules)
4. A mechanism for reaching global decentralised consensus on the valid blockchain (proof of work)

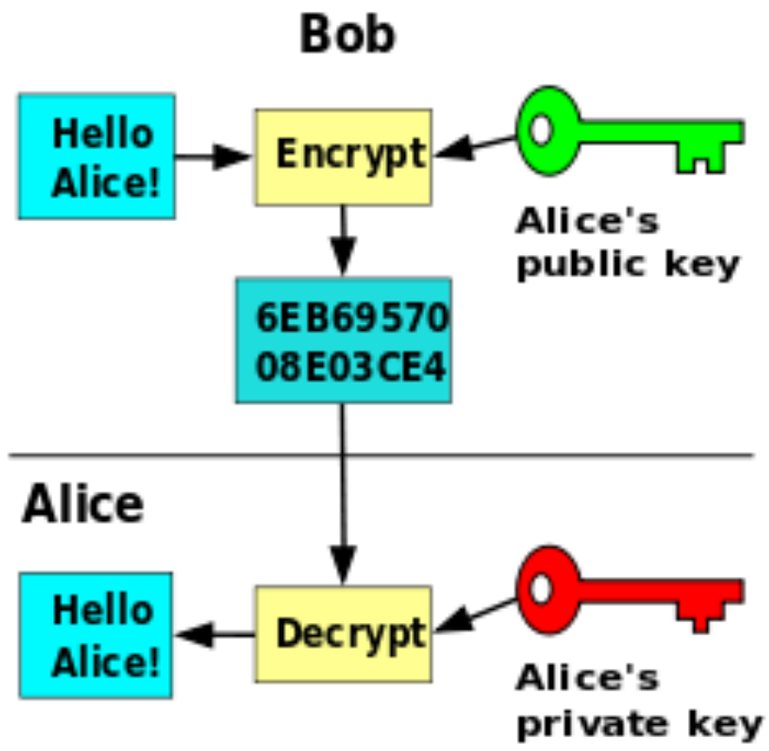
Encryption

e.g.
PGP
Pretty Good Privacy
Public Key



To participate Alice generates 2 keys, one private, one public
She shares the public key.

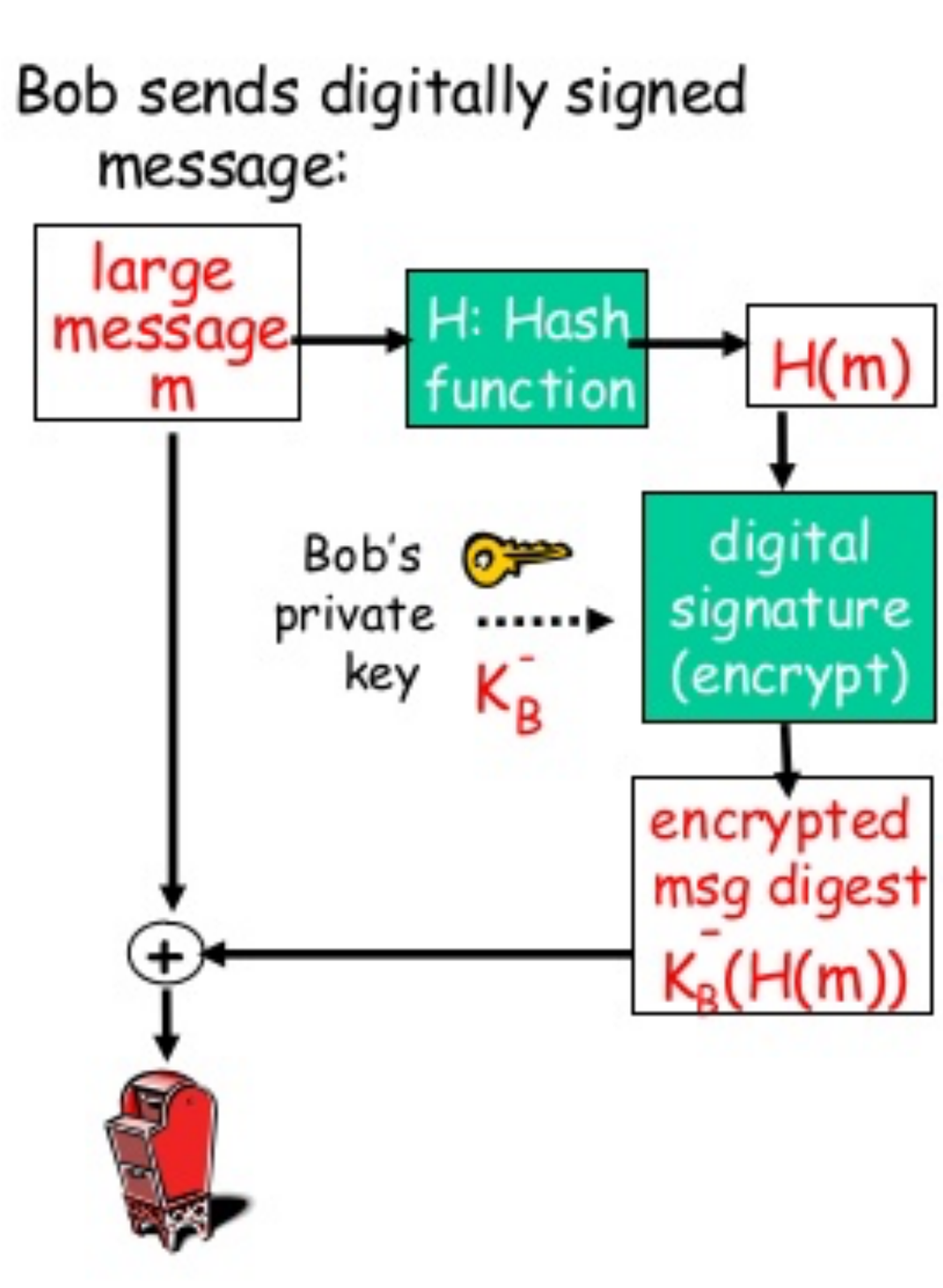
Phil Zimmermann

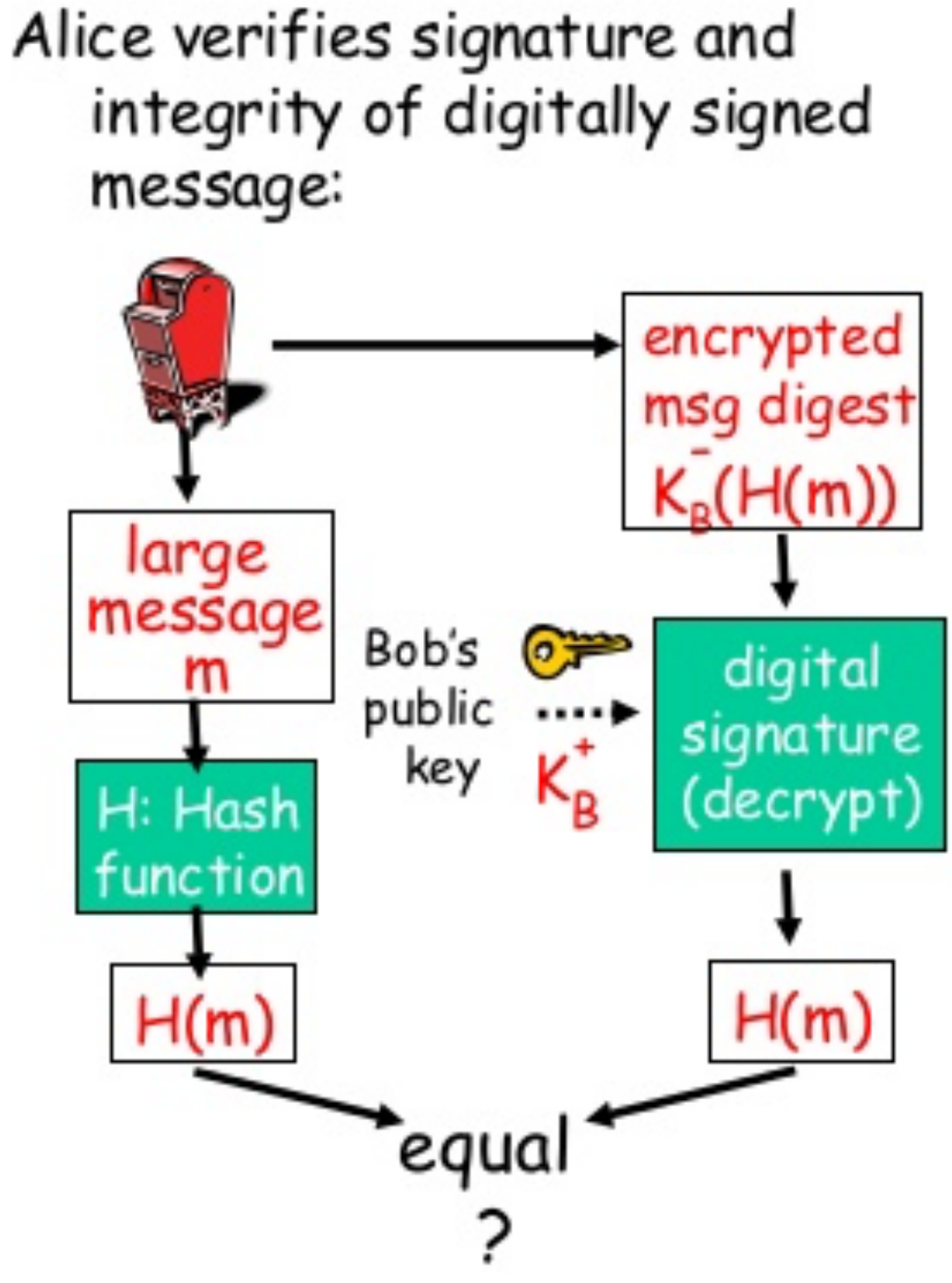


To send a message to Alice Bob encrypts it with her public key.

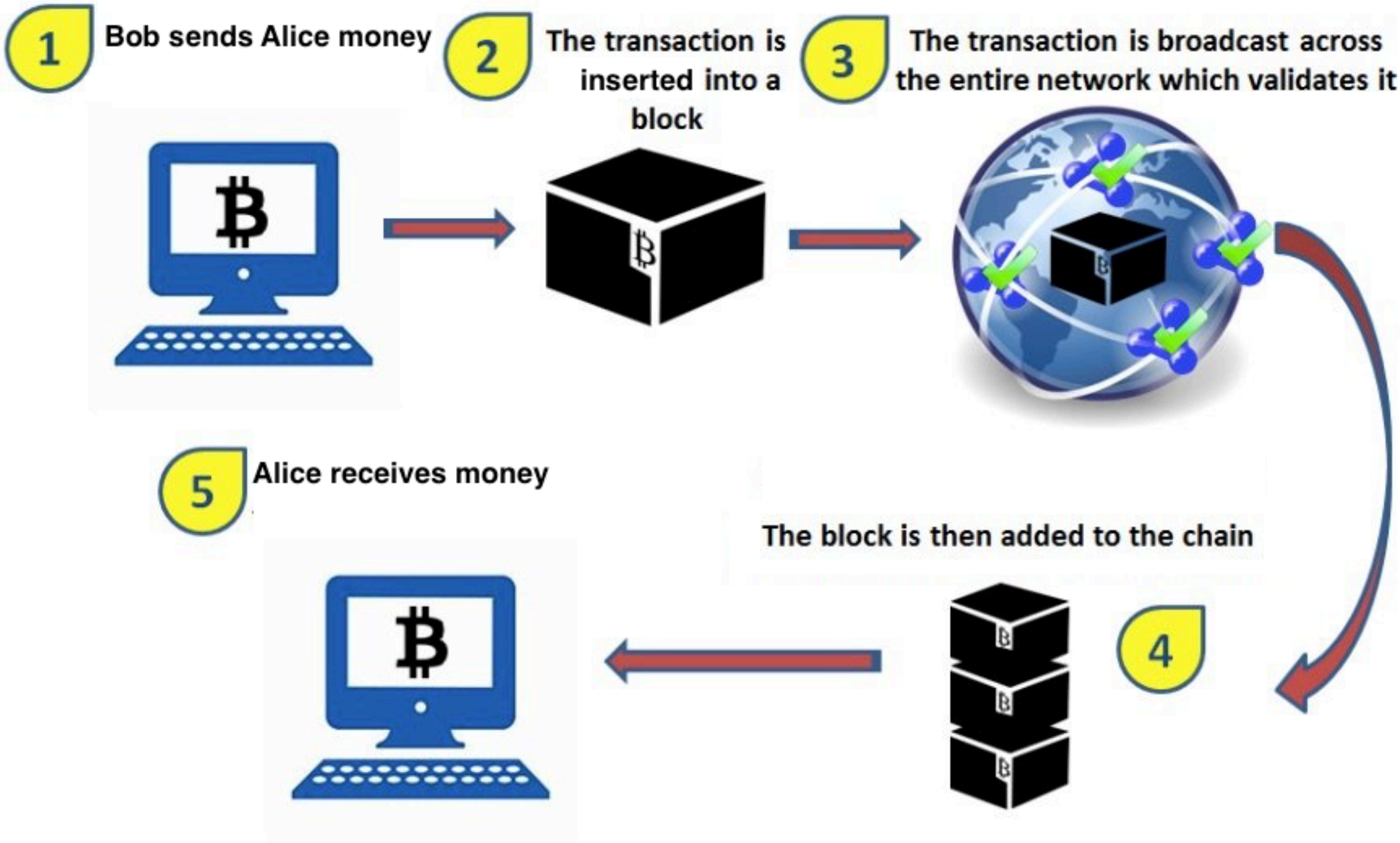
Alice decrypts it with her private key.

Digital Signature





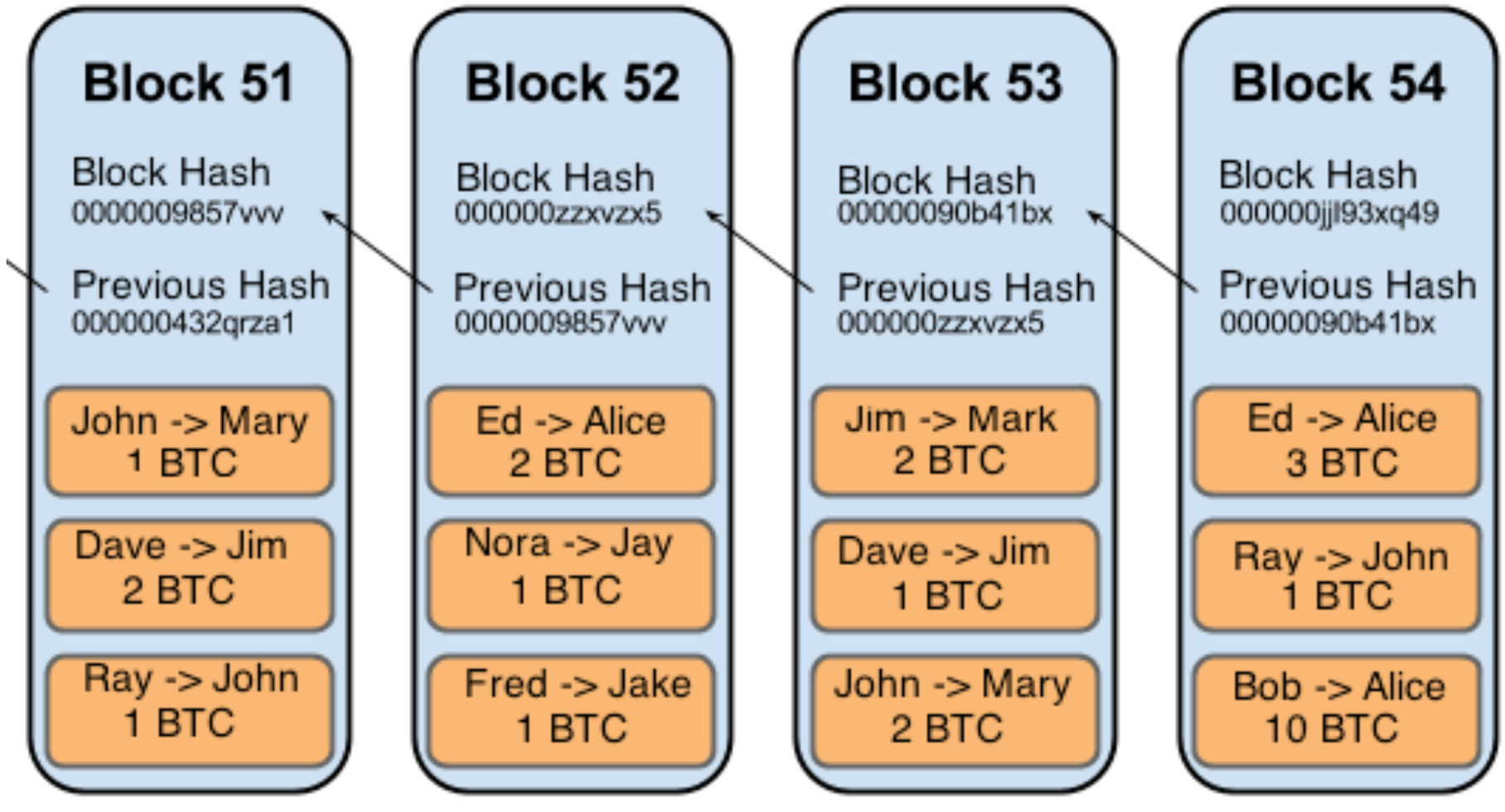
Bitcoin: Use Case



Source: Goldman Sachs Global Investment Research.

Bitcoin Network

1. New transactions are broadcast to all nodes.
2. Each node collects new transactions into a block.
3. Each node works on finding a difficult proof-of-work (PoW) for its block.
4. When a node finds a PoW, it broadcasts the block to all nodes.
5. Nodes accept the block only if all transactions in it are valid and not already spent.
6. Nodes express their acceptance of the block by working on the next block in the chain, incorporating the hash of the accepted block.



Bitcoin Transaction

Bitcoin focuses on transactions (not balances)

Transactions are a transfer of value between Bitcoin wallets

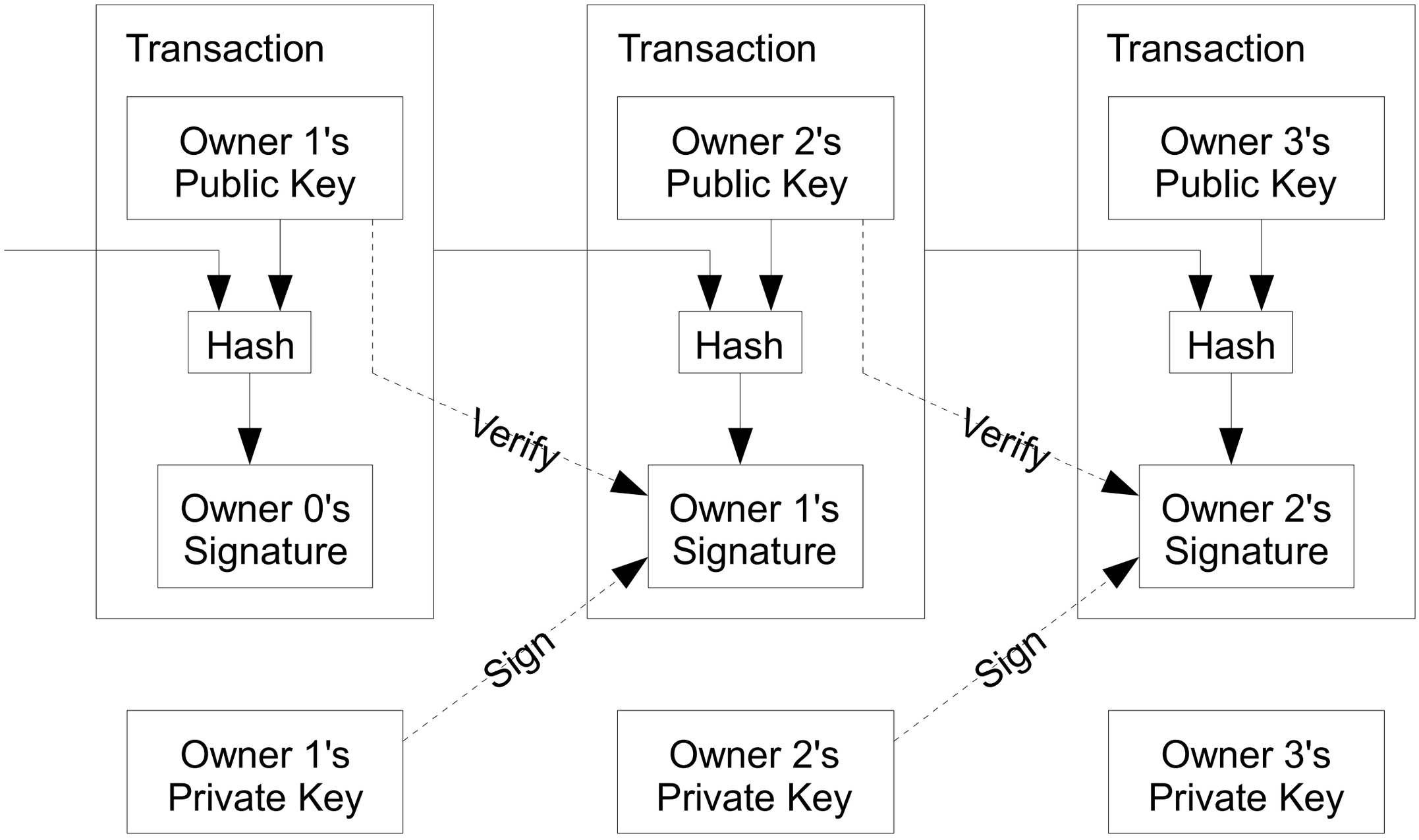
Transactions added to Blockchain

Blocks not just a simple record of transactions

Transactions are signed using senders private key
- cannot be altered
- cannot be **repudiated**

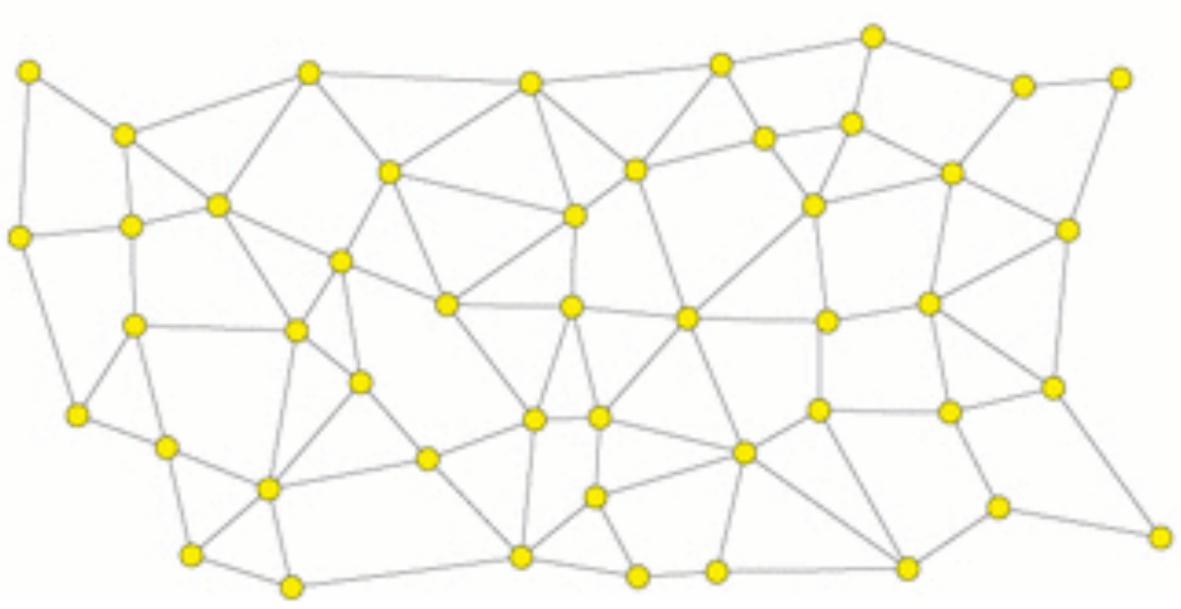
Blocks are broadcast between users
- confirmed by the network after about 10 minutes

Bitcoin Transactions



The Bitcoin Blockchain

The blockchain is distributed amongst all nodes



Nodes validate transactions and blocks

In Bitcoin block validation is rewarded with money, hence nodes are often referred to as miners.

Bitcoin: Consensus

Block validation underpins consensus.

Validated transactions are inserted into block.

Block validation: Proof of Work (PoW)

- Solve a cryptographic puzzle to prove resources expended.
- PoW required to prevent a person creating many validation nodes on a single computer.
- Without validation like PoW a person could be allocated validation rights unfairly.

What is Proof-of-Work?

Make participation in Consensus *expensive*
Solve a puzzle

Validating a block is rewarded with money - hence ***mining***

Find a crypto hash of the current block (+ *nonce*) below a value

e.g. find a hash of “Hello, world!<nonce>” < “000”

4250 tries

```
"Hello, world!0" => 1312af178c253f84028d480a6adc1e25e81caa44c749ec81976192e2ec934c64
"Hello, world!1" => e9afc424b79e4f6ab42d99c81156d3a17228d6e1eef4139be78e948a9332a7d8
"Hello, world!2" => ae37343a357a8297591625e7134cbea22f5928be8ca2a32aa475cf05fd4266b7
...
"Hello, world!4248" => 6e110d98b388e77e9c6f042ac6b497cec46660deef75a55ebc7cfdf65cc0b965
"Hello, world!4249" => c004190b822f1669cac8dc37e761cb73652e7832fb814565702245cf26ebb9e6
"Hello, world!4250" => 0000c3af42fc31103f1fdc0151fa747ff87349a4714df7cc52ea464e12dcd4e9
```

https://en.bitcoin.it/wiki/Proof_of_work

nonce: a number used once

Byzantine Generals Problem

Metaphor for **consensus** problems in CS since 1982

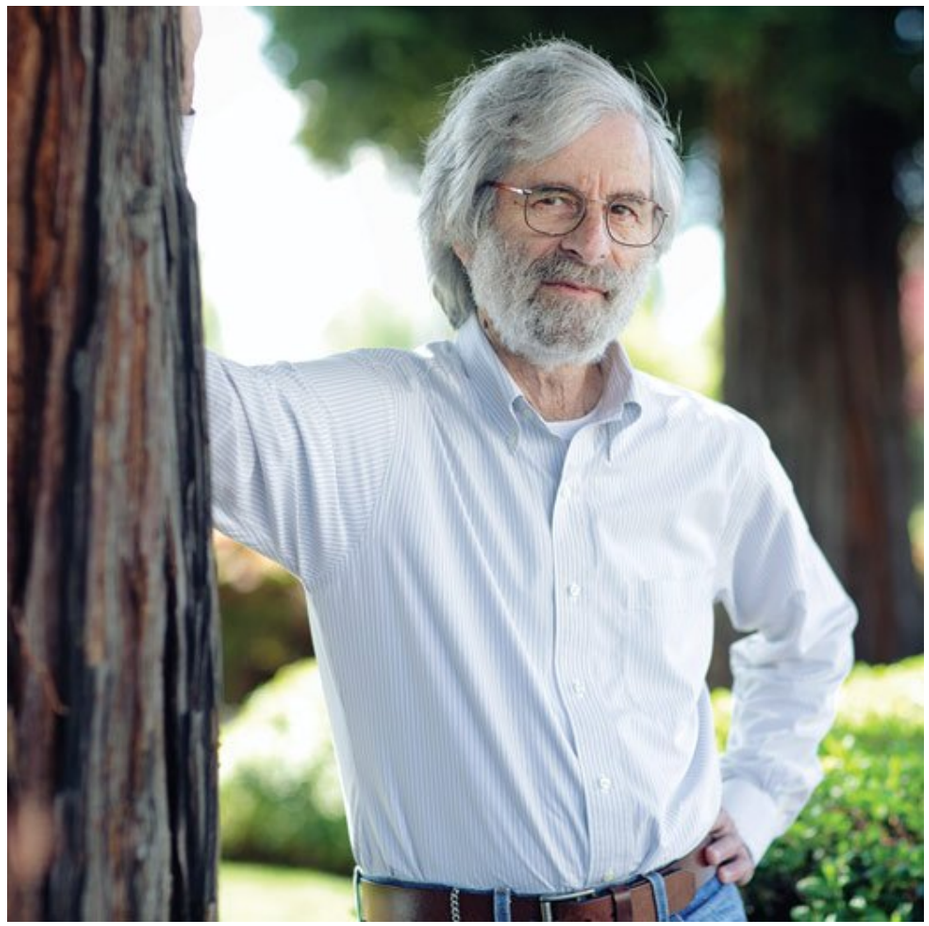
Generals & their armies surround city
- Different locations

Must attack together
- Half-hearted attack will become a rout
- Exchange messages agree to attack of not

Small number of traitorous generals

The Byzantine Generals Problem

LESLIE LAMPORT, ROBERT SHOSTAK, and MARSHALL PEASE
SRI International



Reliable computer systems must handle malfunctioning components that give conflicting information to different parts of the system. This situation can be expressed abstractly in terms of a group of generals of the Byzantine army camped with their troops around an enemy city. Communicating only by messenger, the generals must agree upon a common battle plan. However, one or more of them may be traitors who will try to confuse the others. The problem is to find an algorithm to ensure that the loyal generals will reach agreement. It is shown that, using only oral messages, this problem is solvable if and only if more than two-thirds of the generals are loyal; so a single traitor can confound two loyal generals. With unforgeable written messages, the problem is solvable for any number of generals and possible traitors. Applications of the solutions to reliable computer systems are then discussed.

Categories and Subject Descriptors: C.2.4. [**Computer-Communication Networks**]: Distributed Systems—*network operating systems*; D.4.4 [**Operating Systems**]: Communications Management—*network communication*; D.4.5 [**Operating Systems**]: Reliability—*fault tolerance*

General Terms: Algorithms, Reliability

Additional Key Words and Phrases: Interactive consistency

1. INTRODUCTION

A reliable computer system must be able to cope with the failure of one or more of its components. A failed component may exhibit a type of behavior that is often overlooked—namely, sending conflicting information to different parts of the system. The problem of coping with this type of failure is expressed abstractly as the Byzantine Generals Problem. We devote the major part of the paper to a discussion of this abstract problem and conclude by indicating how our solutions can be used in implementing a reliable computer system.

We imagine that several divisions of the Byzantine army are camped outside an enemy city, each division commanded by its own general. The generals can communicate with one another only by messenger. After observing the enemy, they must decide upon a common plan of action. However, some of the generals

This research was supported in part by the National Aeronautics and Space Administration under contract NAS1-15428 Mod. 3, the Ballistic Missile Defense Systems Command under contract DASG60-78-C-0046, and the Army Research Office under contract DAAG29-79-C-0102.
Authors' address: Computer Science Laboratory, SRI International, 333 Ravenswood Avenue, Menlo Park, CA 94025

Consensus PoW & PoS

Proof-of-Work

Solving the puzzle gives you a vote

Too expensive for malicious actors to acquire many votes

Proof-of-Stake

Validation based on stake rather than work

Stakeholders have a say in proportion to their stake

Validators own a stake in the network, use this as a bond

- e.g. Ether in Ethereum

Use bond to bet on which block to include next

- You lose you lose the bond.

Not wasteful of computer resources

Bitcoin: Technology

Pros:

Decentralized – No single authority
Secure – Difficult to tamper with
Distributed - Fault tolerant
Transparent – Anyone can verify validity
Permanent – Cannot be changed

Cons:

Maximum 7 transactions per second
10 minute block commit time
Computationally wasteful
Value fluctuates

Distributed Ledger

An asset database that can be shared across a network
multiple sites, geographies or institutions

All participants within a network can have their own identical copy of the ledger.

Any changes to the ledger are reflected in all copies in minutes, or in some cases, seconds.

https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/492972/gs-16-1-distributed-ledger-technology.pdf

Distributed Ledger

A distributed ledger is a **consensus** of replicated, shared, and synchronized digital data geographically spread across multiple sites, countries, and/or institutions.

A blockchain is a distributed ledger, comprised of unchangable, digitally recorded data in packages called *blocks*.

Not all distributed ledgers are blockchains

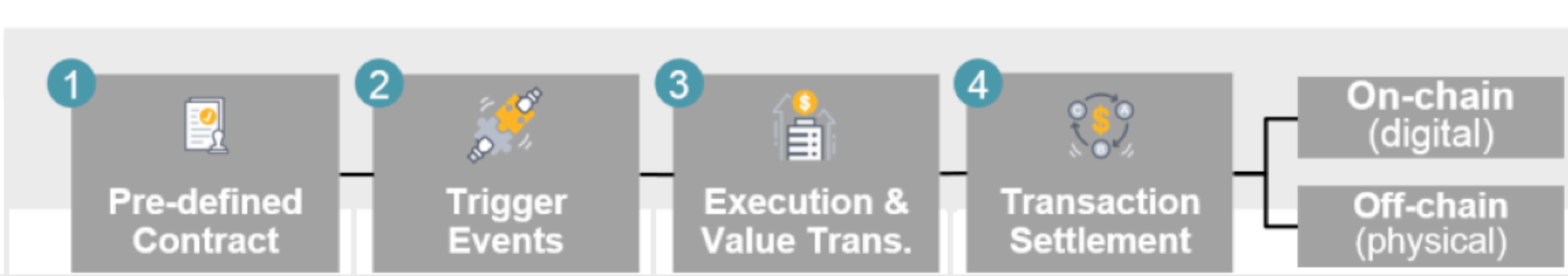
Modern Blockchains

Recent blockchains attempt to correct the issues with Bitcoin.
- Lower transaction latency
- Higher transaction throughput
- More efficient validation

Blockchain development has moved away from public cryptocurreny use cases.

Blockchains have expanded functionality since Bitcoin.
- Assets, Stocks, Securities
- Smart Contracts

Smart Contracts



Example: Travel Insurance	If person misses flight -> cost of ticket refunded	I miss the flight -> Phone automatically messages blockchain	Smart contract determines flight has been missed	Ticket cost refunded automatically to my blockchain account

Summary - from KPMG report on Moodle

Blockchain: A type of distributed ledger database that maintains a continuously growing list of transaction records ordered into blocks with various protections against tampering and revision.

Distributed ledger: A digital record of ownership that differs from traditional database technology, since there is no central administrator or central data storage; instead, the ledger is replicated among many different nodes in a peer- to-peer network, and each transaction is uniquely signed with a private key.

Consensus mechanism: A method of authenticating and validating a value or transaction on a Blockchain or a distributed ledger without the need to trust or rely on a central authority. Consensus mechanisms are central to the functioning of any blockchain or distributed ledger.

Nodes: Members or systems of a consensus network or a server that holds a replicated copy of the ledger and can have varying roles: to issue, verify, receive, inform, etc. For all intents and purposes, a node can be a virtual machine (VM) instance.

Conclusion

Blockchain has the potential to revolutionise certain industries.

Smart contracts are an emerging area which may have far reaching applications.

While Bitcoin may not be successful, the underlying technology, blockchain is here to stay.

Beyond Bitcoin

“It has been estimated that the energy requirements to run Bitcoin are in excess of 1GW and may be comparable to the electricity usage of Ireland”

Distributed Ledger Technology: beyond block chain
A report by the UK Government Chief Scientific Adviser

- https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/492972/gs-16-1-distributed-ledger-technology.pdf

Almost certainly BS but the “*Consensus by PoW/mining*” idea is wasteful.

Blockchain

Why?

Preliminaries - Cryptography
- Encryption
- Authentication
  - Cryptographic signature

Bitcoin
- Transactions
- Proof of Work

Distributed Databases
- Distributed Ledger Technologies
- Consensus
  - Proof of Work
  - Proof of Stake