CSO43A: Blockchain Technology

Examination Scheme:

Class Continuous Assessment: 100 Marks Credit: 2

Course Objectives:

- To familiarize the students with functional/operational aspects of cryptocurrency Ecosystem.
- To explain the working of bitcoin and Blockchain Architecture.
- To explore the most prominent smart contract platform - Ethereum and Hyperledger

Course Outcomes:

After completion of this course students will be able to:

- understand the functional/operational aspects of cryptocurrency Ecosystem.
- describe the working of bitcoin and Blockchain Architecture.
- elaborate Ethereum and Hyperledger platforms.

Pre-requisites

- Distributed systems and Networking
- Cryptography
- Data Structures

Syllabus

Unit: I	**Fundamentals** **History:** Traditional financial arrangements, The trouble with credit cards online, From Credit to (Crypto) Cash. **Introduction to Cryptography & Cryptocurrencies:** Cryptographic Hash Functions, Hash Pointers and Data Structures, Digital Signatures, Public Keys as Identities **Bitcoin:** Introduction to Bitcoin, Bitcoin users - Full Client, Light Client, Web Client.	**6 Hrs**
Unit: II	**Bitcoin Mechanics** Centralization vs. Decentralization, Distributed consensus, Byzantine Generals Problem, Implicit Consensus, Bitcoin consensus algorithm, Stealing Bitcoins, Validation Algorithms: Proof of work, Proof of Stake, Proof of Authority, Proof of Activity, Proof of Burn, Proof of Capacity. Block Reward, Transaction fees, Bitcoin transactions, Bitcoin Scripts, Bitcoin blocks, Bitcoin network.	**6 Hrs**
Unit: III	**Blockchain Architecture** Introduction, Structure of a Block, Block Header, Block Identifiers - Block Header Hash and Block Height, The Genesis Block, Linking Blocks in the Blockchain, Types of blockchain, Merkle Trees and Simplified Payment Verification (SPV), Blockchain P2P architecture. Bitcoin Mining- The task of Bitcoin miners, Mining Hardware- CPU mining, GPU mining, FPGA mining, ASIC mining.	**5 Hrs**

Syllabus (Continue)

Unit: IV	**Ethereum & Hyperledger** Ethereum Virtual Machine, **S**mart contract, wallets for Ethereum, Ethereum Programming Language – Solidity, Mining in Ethereum, uses and benefits of Ethereum Hyperledger architecture, Consensus in Hyperledger, Hyperledger frameworks Bitcoin Security-Security principles, User Security Best Practices.	**5 Hrs**
Books:-(Text)	Arvind Narayanan, Joseph Bonneau, Edward Felten, Andrew Miller and Steven Goldfeder, "Bitcoin and Cryptocurrency Technologies: A Comprehensive Introduction", Princeton University Press (July 19, 2016)	
Books:-(Reference)	Andreas Antonopoulos, "Mastering Bitcoin: Unlocking Digital Cryptocurrencies", O'Reilly, ISBN-13: 978-1449374044	

Guidelines for CCA

Examination Scheme

Sr. No.	Examination Scheme	Marks
1.	Class Continuous Assessment (CCA)	100

CCA Marks Distribution

Examination	Weightage	Marks
Theory Assignments	20 %	20
Mid-Term Theory Exam	15 %	15
Active Learning	25 %	25
Practical Assignments / Case Studies Evaluation	40 %	40
	Total	100

Unit-I : Fundamentals

- **History:** Traditional financial arrangements, The trouble with credit cards online, From Credit to (Crypto) Cash.
- **Introduction to Cryptography & Cryptocurrencies:**
- Cryptographic Hash Functions, Hash Pointers and Data Structures, Digital Signatures, Public Keys as Identities
- **Bitcoin:** Introduction to Bitcoin, Bitcoin users - Full Client, Light Client, Web Client.

डिब्बों की जंजीर

पाप और पुण्य का लेखा जोखा ॥
उसे लोकतंत्र ने दफ्तर में लिखा ॥
जब लिखा तो उसे लोगों ने देखा ॥
उसीको समय ने बराबर रोका ॥
उसके बाद कोई बदल नहीं सका ॥
सही पकड़े, तो होगा उन्नति का झरोखा ॥

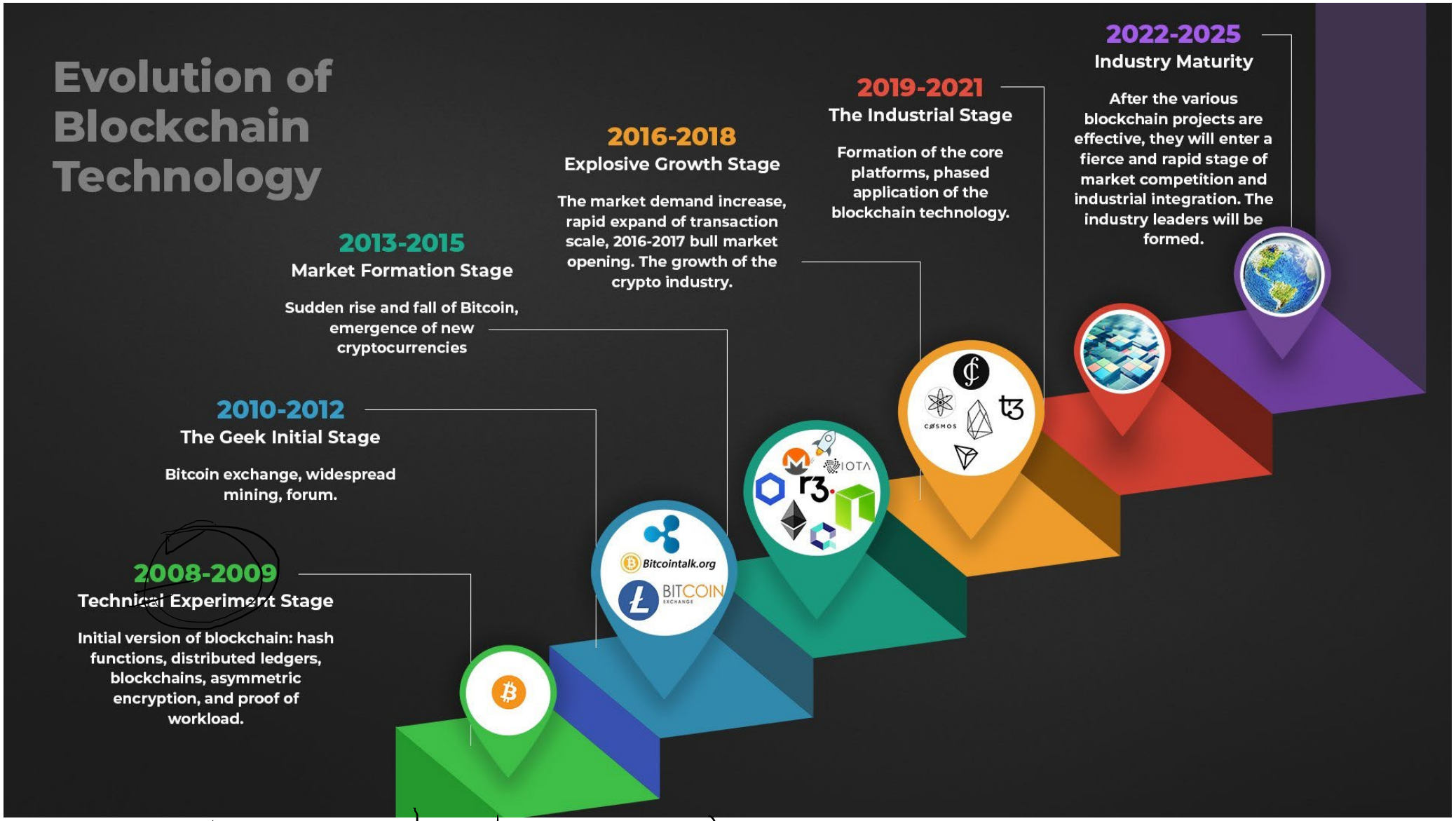
Informally speaking

In an autonomous, connected world, good or bad actions committed by living or nonliving things, which can not be rolled back, and which are witnessed by majority.

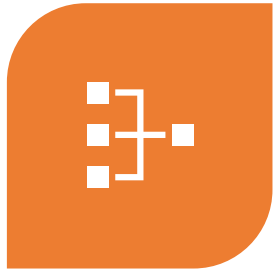
T/C applies

Blockchain What it is?

- Blockchain is **a system of recording information in a way** that makes it difficult or impossible to change, hack, or cheat the system.
- A blockchain is essentially a digital ledger of transactions that is duplicated and distributed across the entire network of computer systems on the blockchain.


Evolution of Blockchain Technology
2008-2009
Technical Experiment Stage
Initial version of blockchain: hash functions, distributed ledgers, blockchains, asymmetric encryption, and proof of workload.
2010-2012
The Geek Initial Stage
Bitcoin exchange, widespread mining, forum.
2013-2015
Market Formation Stage
Sudden rise and fall of Bitcoin, emergence of new cryptocurrencies
2016-2018
Explosive Growth Stage
The market demand increase, rapid expand of transaction scale, 2016-2017 bull market opening. The growth of the crypto industry.
2019-2021
The Industrial Stage
Formation of the core platforms, phased application of the blockchain technology.
2022-2025
Industry Maturity
After the various blockchain projects are effective, they will enter a fierce and rapid stage of market competition and industrial integration. The industry leaders will be formed.
Bitcointalk.org
BITCOIN EXCHANGE
IOTA
r3
COSMOS

Blockchain Technology Pillars



DISTRIBUTED NETWORK

CRYPTOGRAPHY

CONSENSUS ALGORITHMS

DATA BASES

Block Applications Pillars

Traditional Database Technology

Parallel and Distributed Computing

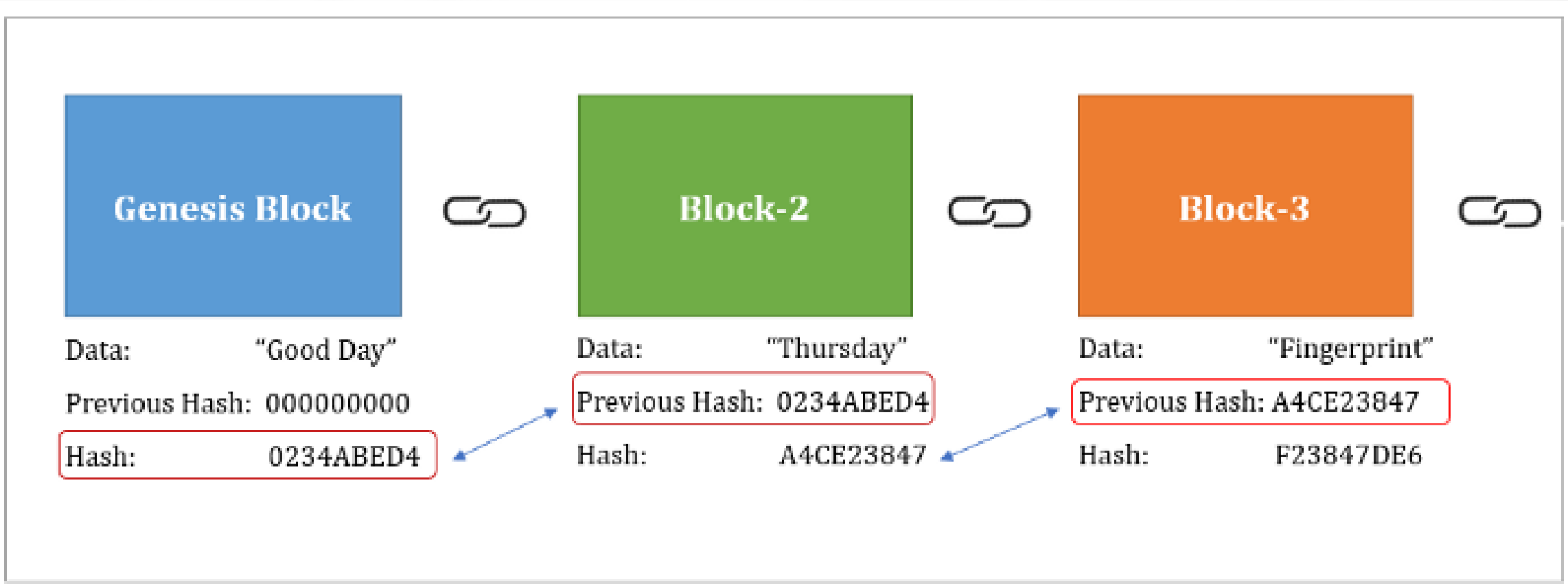
Sensor and IoT Technologies

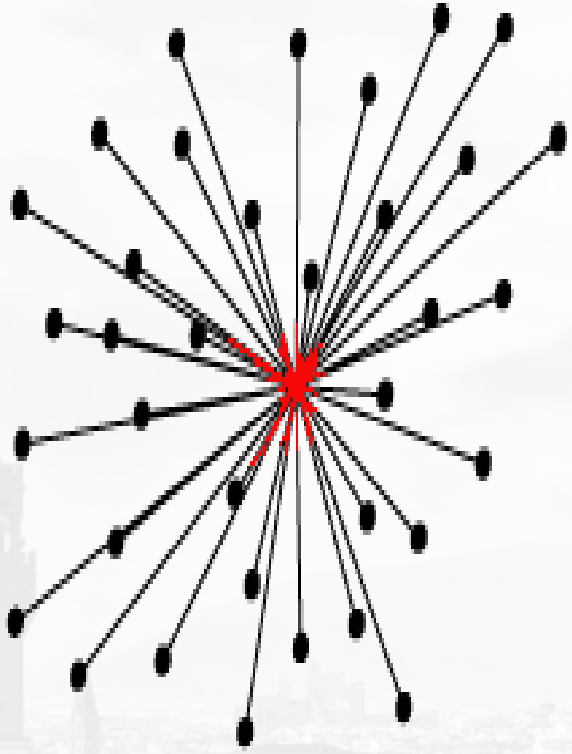
Communication Technologies

Cloud Computing

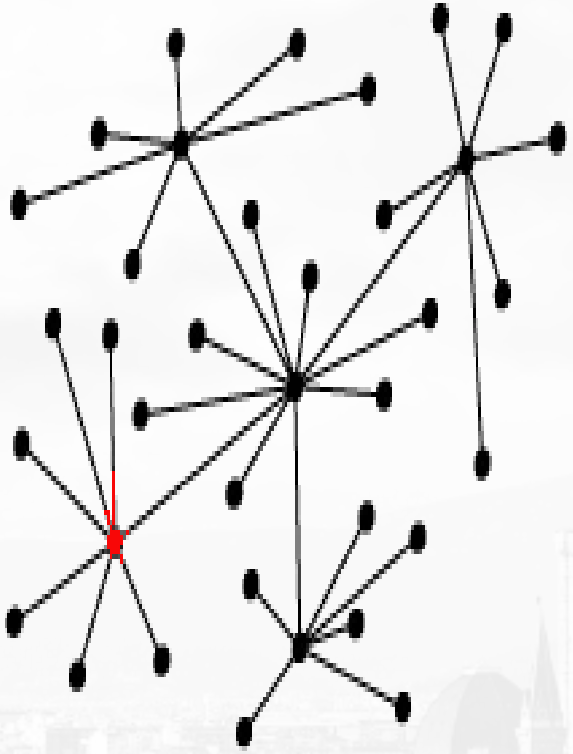
Artificial Intelligence and Machine Learning

Blockchain

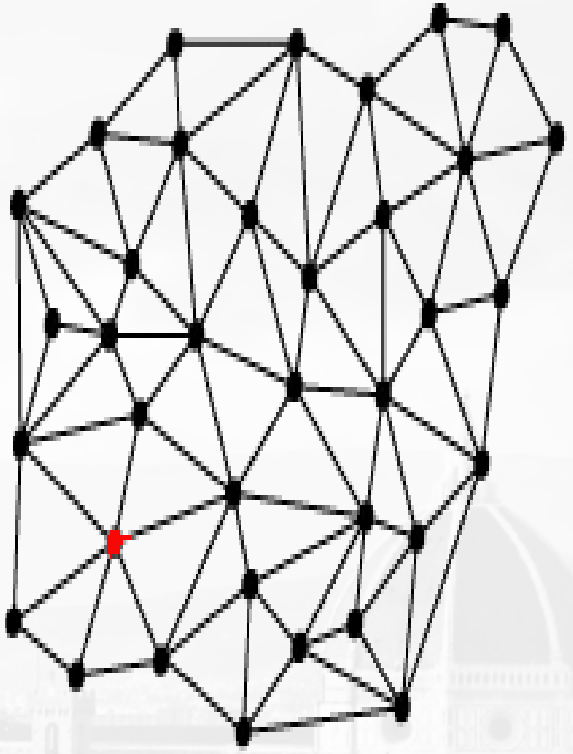

Genesis Block
Block-2
Block-3
Data: "Good Day"
Previous Hash: 000000000
Hash: 0234ABED4
Data: "Thursday"
Previous Hash: 0234ABED4
Hash: A4CE23847
Data: "Fingerprint"
Previous Hash: A4CE23847
Hash: F23847DE6



centralised

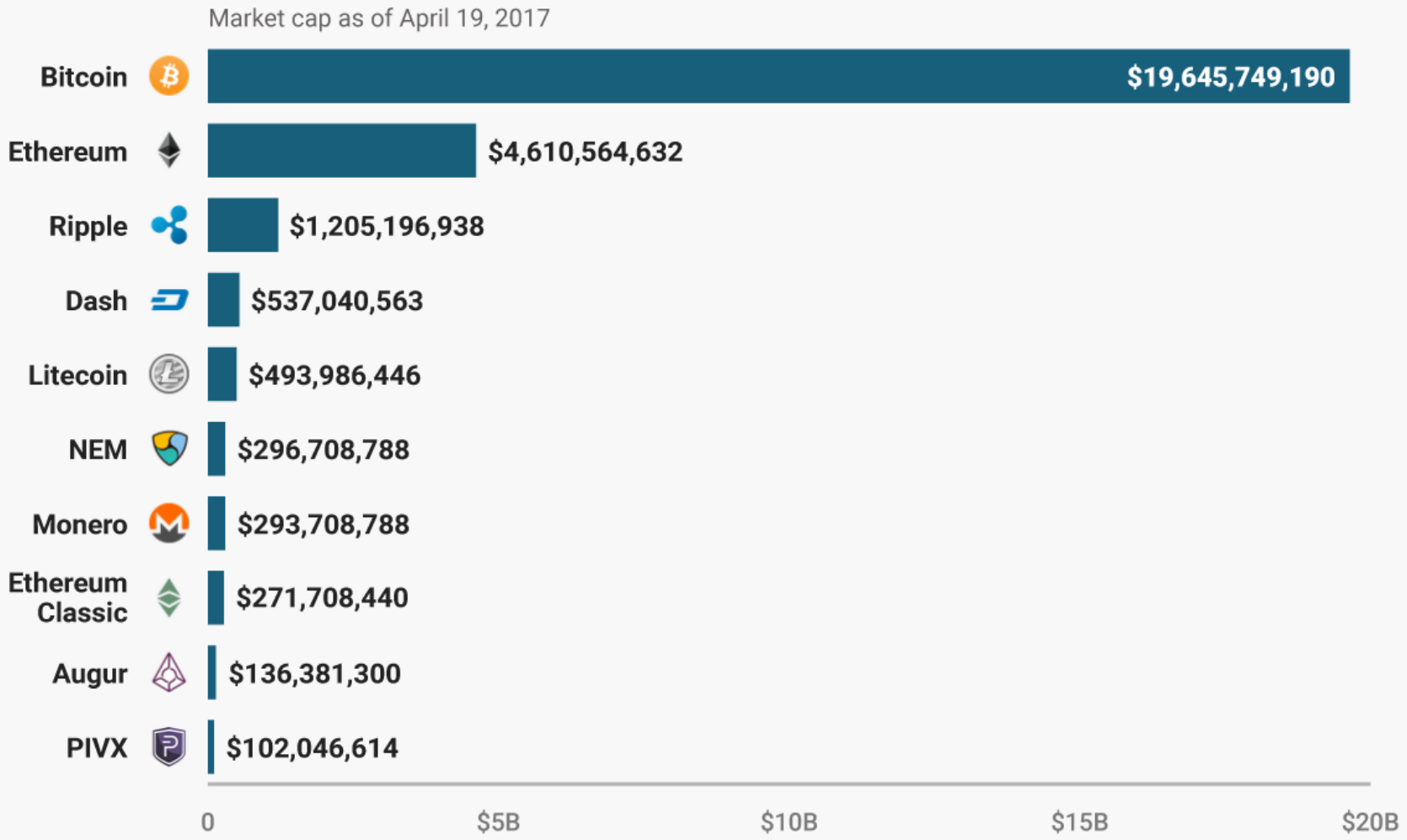


decentralised



distributed

10 CRYPTOCURRENCIES HAVE A MARKET CAP OVER $100M



SOURCE: CoinMarketCap.com

BUSINESS INSIDER

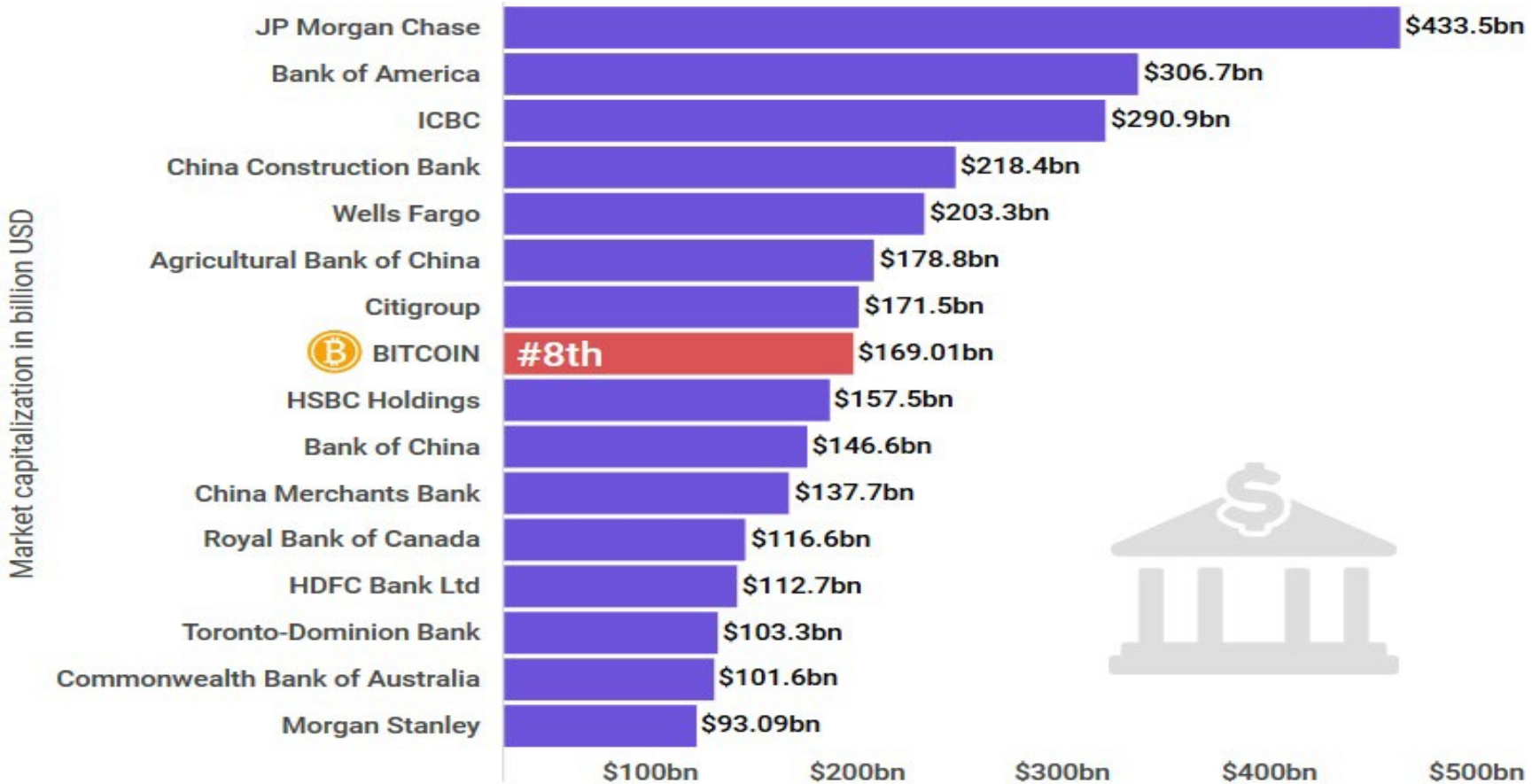

Top 15 Cryptocurrency by Market Capitalization
0$
500,000,000,000$
1,000,000,000,000$
Bitcoin (BTC)
970,915,801,747$
Ethereum (ETH)
462,550,279,037$
Cardano (ADA)
92,947,172,008$
Binance Coin (BNB)
84,507,362,328$
Tether (USDT)
66,831,148,664$
XRP (XRP)
60,564,297,138$
Dogecoin (DOGE)
41,061,110,734$
Solana (XLM)
41,623,366,678$
Polkadot (DOT)
34,012,230,854$
USD Coin (USDC)
27,829,570,616$
Uniswap (UNI)
17,881,248,085$
Litecoin (LTC)
15,368,765,324$
Chainlink (LINK)
15,052,157,312$

15 leading banks worldwide vs. Bitcoin

by market capitalization, as of July 2020, in billion USD

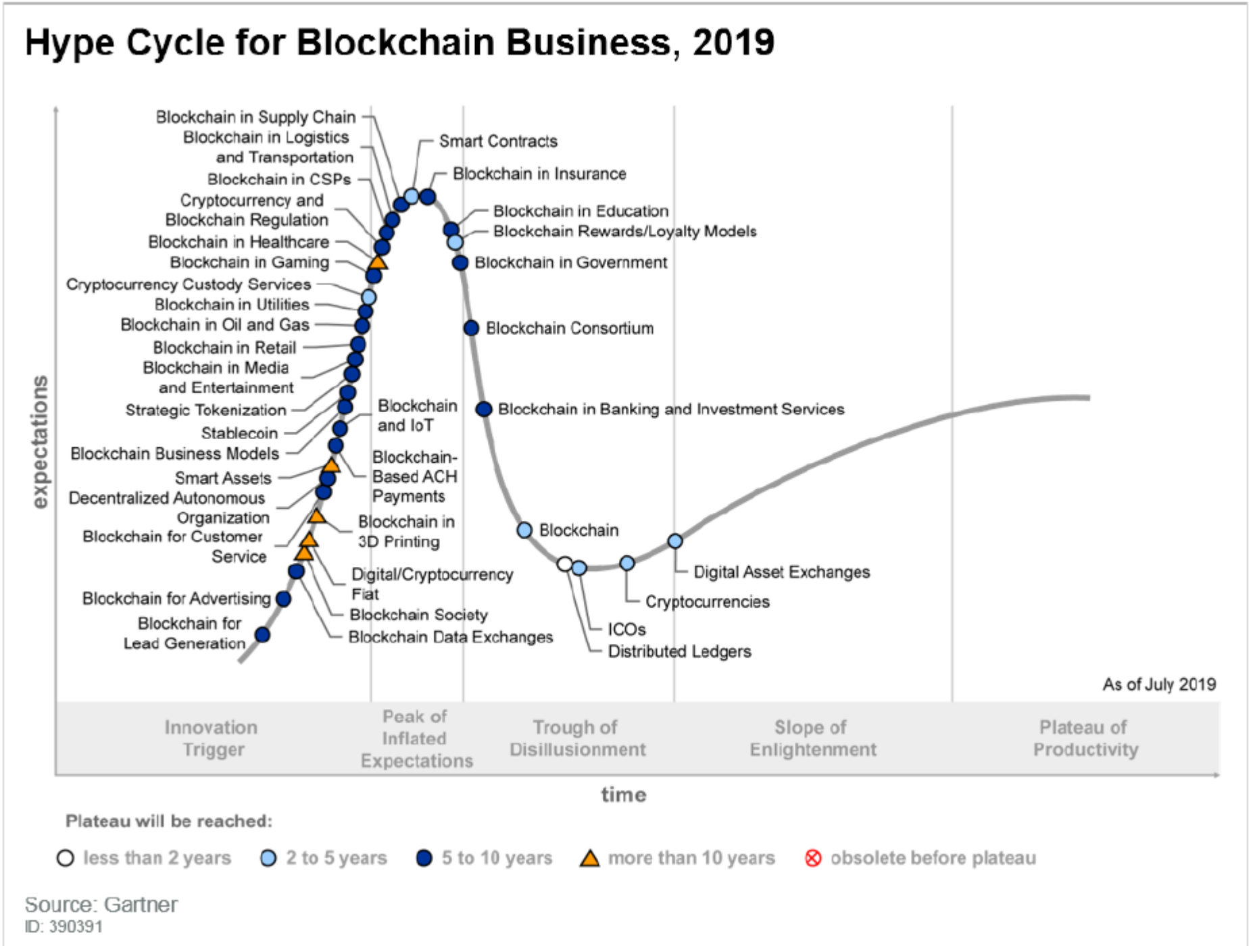
Details: Worldwide; data released in July 2020 (survey as of January 21, 2020).

Data: Coinmarketcap.com, Statista

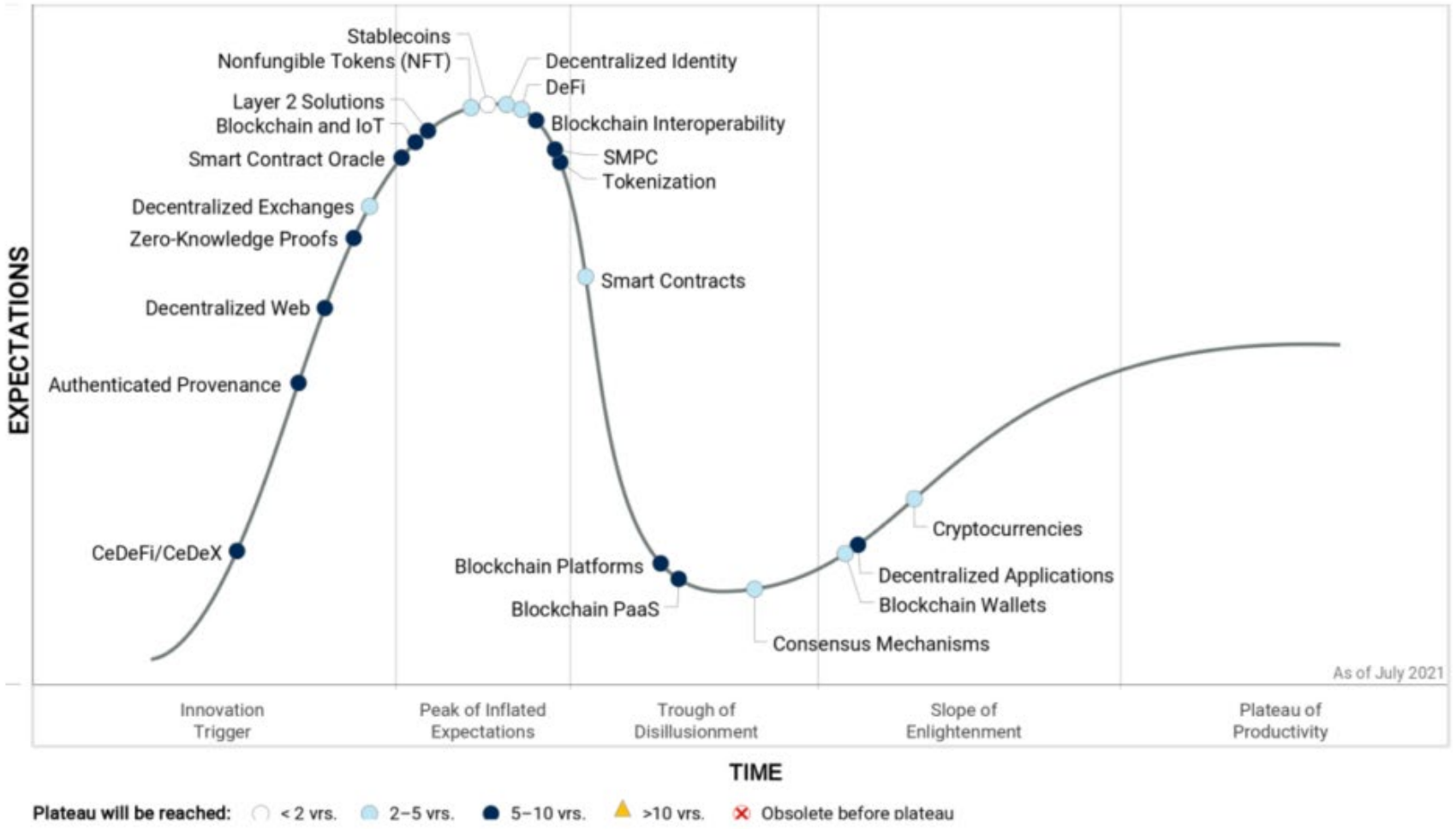


BUYSHARES

The 2019 Gartner, Inc. Hype Cycle for Blockchain Business shows that the business impact of blockchain will be transformational across most industries within five to 10 years.

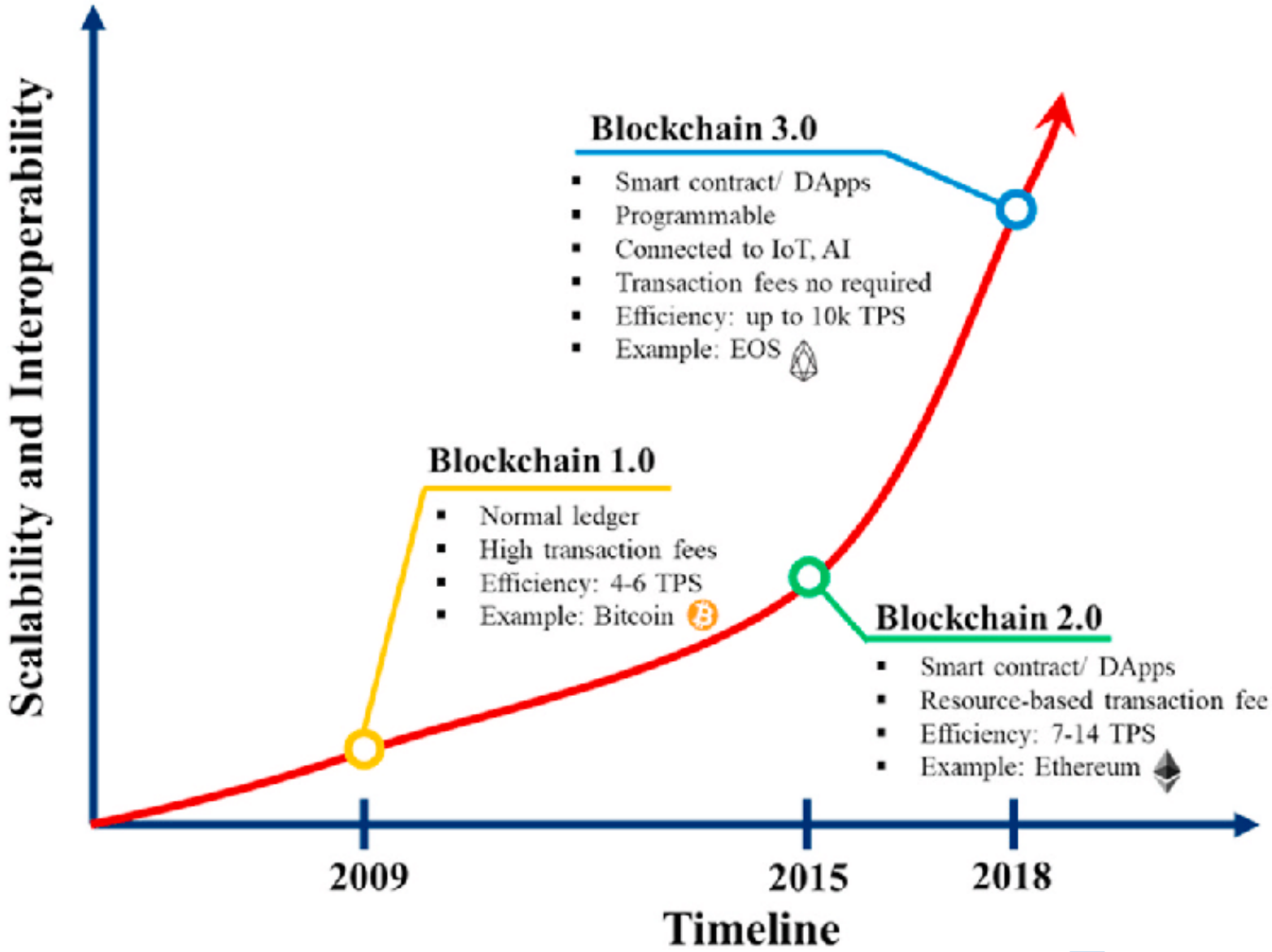


Hype Cycle for Blockchain, 2021



Source: Gartner (July 2021)

747513


Scalability and Interoperability
Blockchain 3.0
Smart contract/ DApps
Programmable
Connected to IoT, AI
Transaction fees no required
Efficiency: up to 10k TPS
Example: EOS
Blockchain 1.0
Normal ledger
High transaction fees
Efficiency: 4-6 TPS
Example: Bitcoin
Blockchain 2.0
Smart contract/ DApps
Resource-based transaction fee
Efficiency: 7-14 TPS
Example: Ethereum
2009
2015
2018
Timeline

Blockchain 2021 Drivers- I

- Mainstream adoption of Bitcoin, including El Salvador's adoption of Bitcoin as legal tender in June 2021.
- Payment network, banking and social network adoption of distributed ledger technologies (DLTs) for money movement, with the expected deployment of central bank digital currencies (CBDCs) being a key influencer.
- Decentralized finance (DeFi) applications offer substantially greater financial rewards than traditional finance. Centralized firms like hedge funds already take advantage of this.
- Tokenization of assets, including explosive growth of NFTs and DeFi tokens, and the promise of tokens linked to physical assets in the future.

Blockchain 2021 Drivers- II

- Blockchains such as Binance, Cardano, and Solana offering viable cost-effective alternatives to Ethereum chain transactions.
- Monumental progress in blockchain interoperability, including gateways and abstraction middleware, already used today by DeFi applications.
- Blockchain migration from the proof-of-work (POW) consensus method (still used for Bitcoin) to more energy-efficient consensus methods such as proof of stake (PoS). The ongoing upgrade of Ethereum leads this trend.

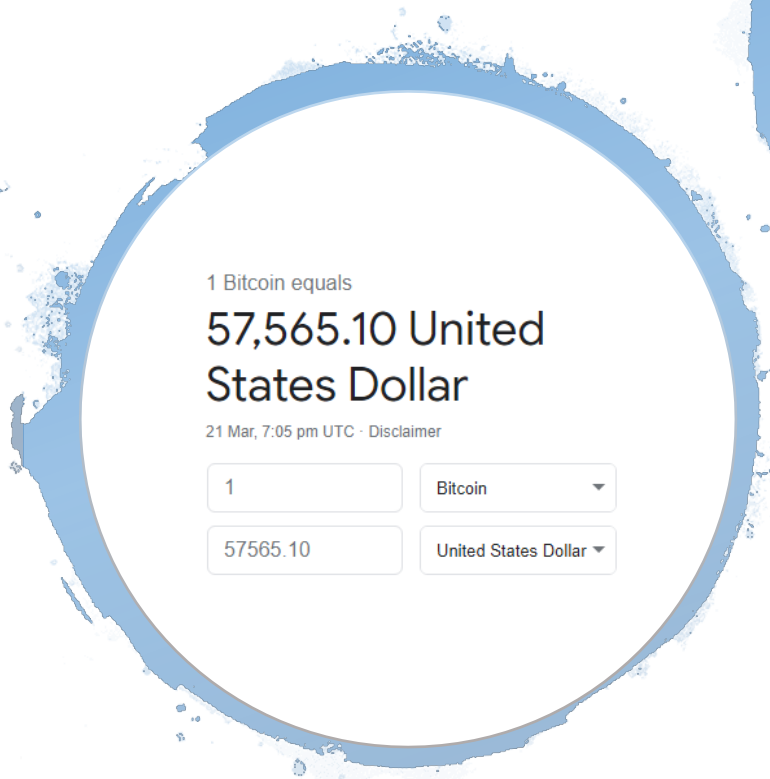
Blockchain 2021 challenges

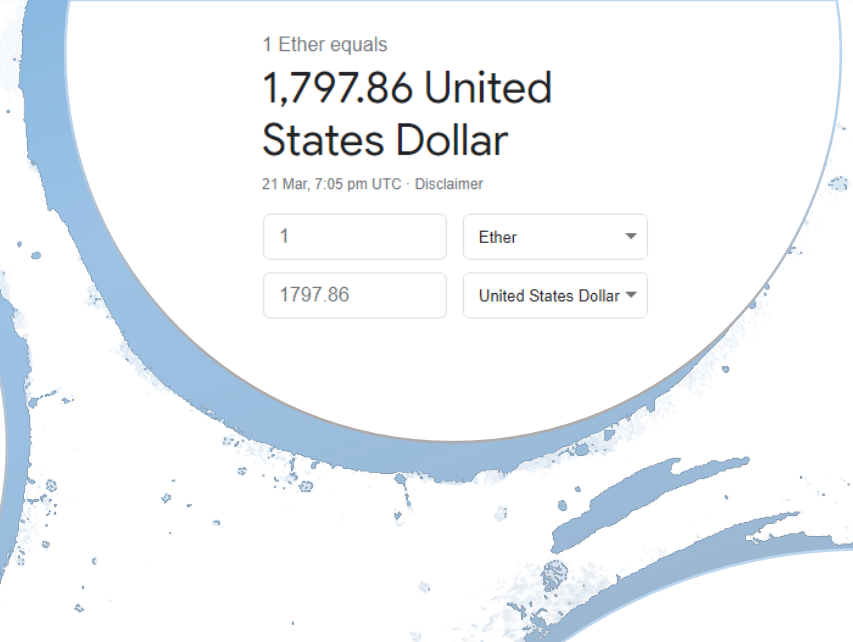
- Adoption of permissioned blockchains is moving much more slowly. Some use cases — especially around supply chain and authenticated provenance — are benefiting from ledger technology. However, most users are stuck trying to align use cases to the technology.
- Global regulations and accounting standards need clarification before most enterprises adopt cryptocurrency
- China continues to clamp down on crypto activities as they work on making their own CBDC the world's dominant currency.

.

Blockchain 2021

Awareness of decentralized public blockchain and private blockchain is rapidly increasing specially in supply chain sector, but the applications & adoptions are still not motivated enough because of the growing threats in absence of legal framework.



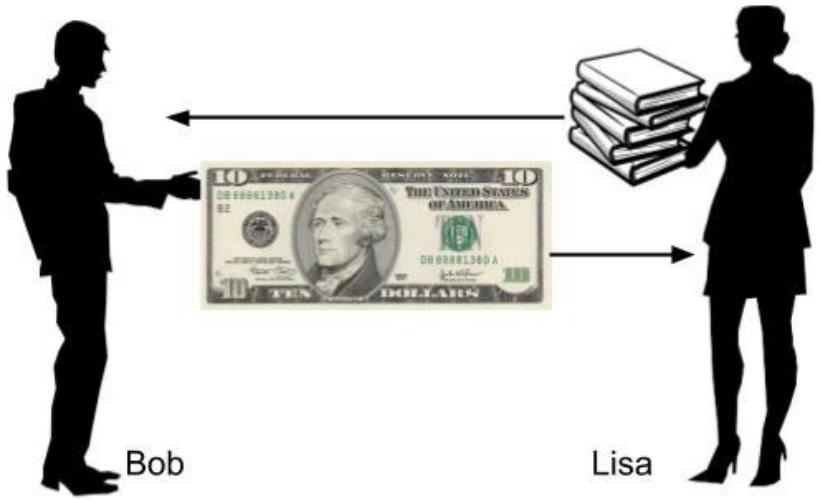


BitCoin value yesterday 21st march 20

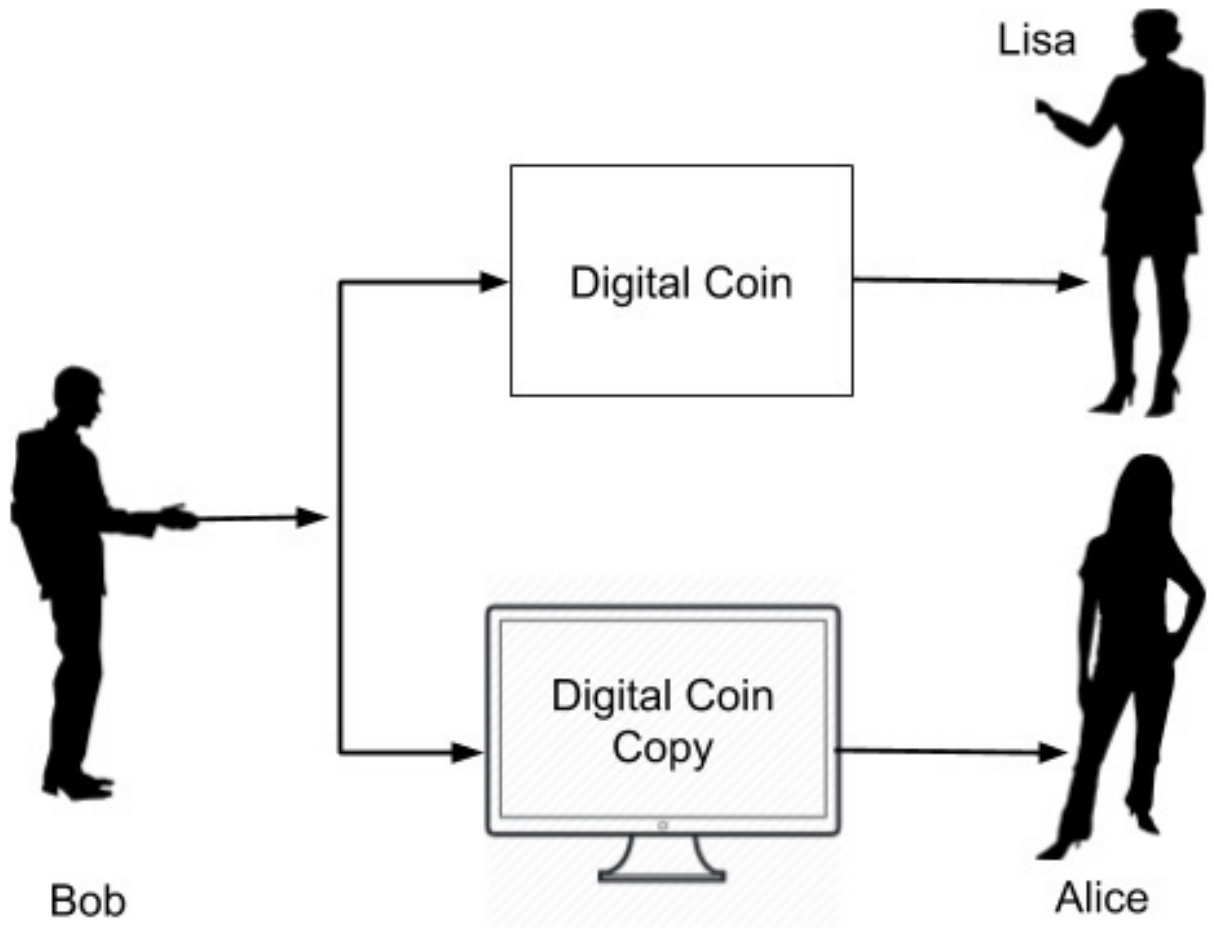
BlockChain Technology

- A blockchain 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.
- Blockchain has been in a lot of buzz these days. And that is mainly because it is backbone of the very famous cryptocurrency in the world - the Bitcoin. Many Governments and leading Banks have decided to bring many of their conventional transactions based on Blockchain concept.
- The applications and potential of this framework is huge and is considered to be changing the way transactions are made in various domains.

- Ref: Tutorials Point https://www.tutorialspoint.com/blockchain/index.htm



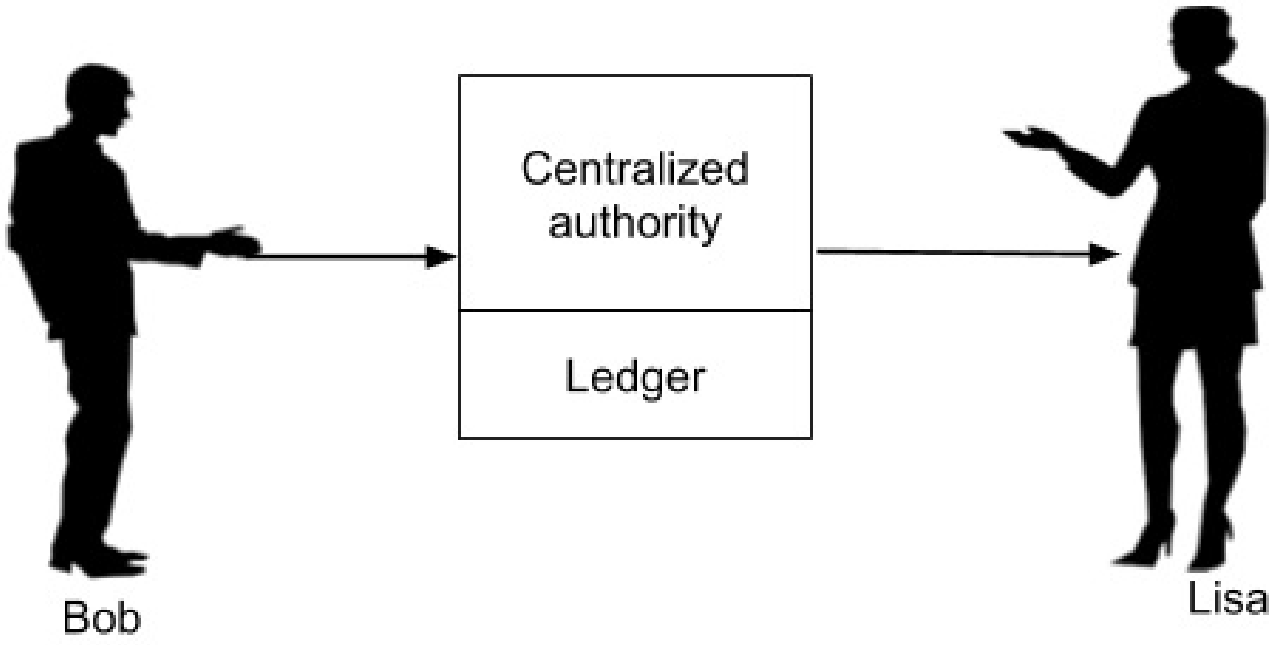
Bob and Lisa transaction ?


Lisa
Digital Coin
Digital Coin
Copy
Bob
Alice

Double Spending

- As the format for money exchange is in the digital format, it is essentially a binary physical file stored somewhere on Bob's device.
- After Bob gives this file (digital money) to Lisa, he can also a give a copy of the file to Alice.
- Both now think that they have received the money without having any means of authenticating the digital coin and would thus deliver their respective goods to Bob.
- This is called **double-spending** where the sender spends the same money at more than one place for obtaining services or goods from multiple vendors.

To solve this problem of double-spending, one would employ a centralized authority to monitor all the transactions.



Centralized Authority?

- The introduction of centralized authority though it solves the double-spending problem, introduces another major issue - the cost of creating and maintaining the centralized authority itself.
- As the banks need money for their operations, they start cutting commissions on each currency transaction they do for their clients. This sometimes can become very expensive, especially in overseas transfer of money where multiple agents (banks) may be involved in the entire deal.
- All the above issues are solved by the introduction of digital currency, called Bitcoin.

BitCoin Technology

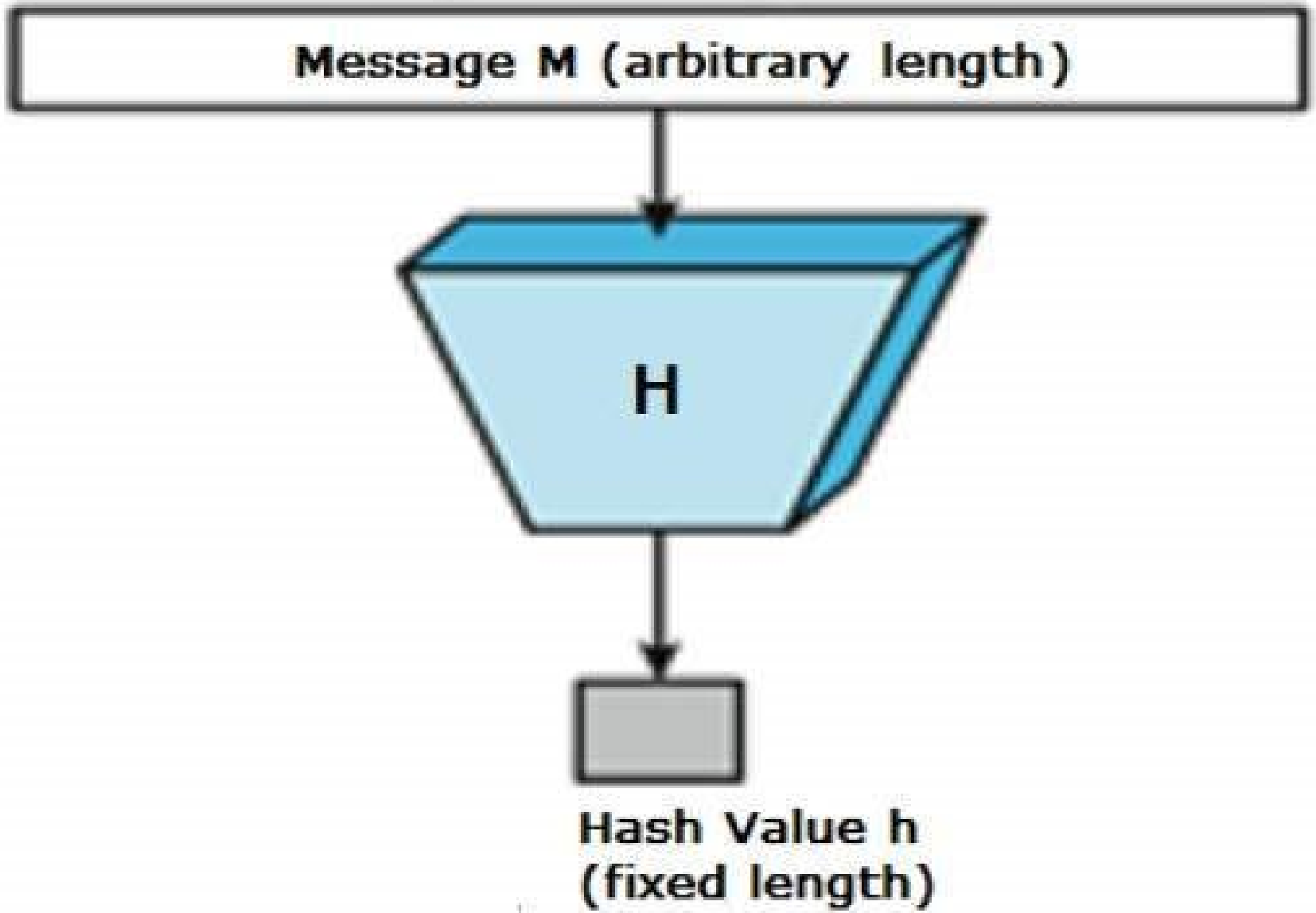
- The Bitcoin was introduced in this world by Satoshi Nakamoto through a research-style white paper entitled Bitcoin: A Peer-to-Peer Electronic Cash System in the year 2008.
- The Bitcoin not only solved the double-spending problem, but also offered many more advantages, One such advantage worth mentioning here is the **anonymity in the transactions**.
- Satoshi who created the system and did transact few coins on this system is totally anonymous to the entire world.
- Just imagine, in this world of social media, when the privacy of each individual is at stake, the world is not able to trace out so far who is Satoshi?
- In fact, we do not know whether Satoshi is an individual or a group of people. Googling it out also revealed the fact that the bitcoins Satoshi Nakamoto holds is worth about 34.9 billion - that money now remains unclaimed in the Bitcoin system.

BitCoin

- As you saw earlier, the bank maintains a ledger recording each transaction. This ledger is privately held and maintained by the bank.
- Satoshi proposed that let this ledger be public and maintained by the community.
- Since, this ledger is public, it has to be tamper-proof so that nobody can modify its entries.
- As each entry in the ledger is publicly visible, we will have to figure out how to maintain the anonymity - obviously you would not like everybody in the world to know that you paid one million dollars.

Intro to Cryptography and Cryptocurrencies

- Cryptographic Hash Functions
- Hash Pointers and Data Structures
  - Block Chains
  - Merkle Trees
- Digital Signatures
- Public Keys and Identities
- Let's design us some Digital Cash!


Message M (arbitrary length)
H
Hash Value h
(fixed length)

Cryptographic Hash Function

Hash Function: Mathematical Function with following 3 properties:

- The input can be any string of any size.
- It produces a fixed-size output. (say, 256-bit long)
- Is efficiently computable. (say, $O(n)$ for n-bit string)

Such general hash function can be used to build hash tables, but they are not of much use in cryptocurrencies. What we need are **cryptographic** hash functions.

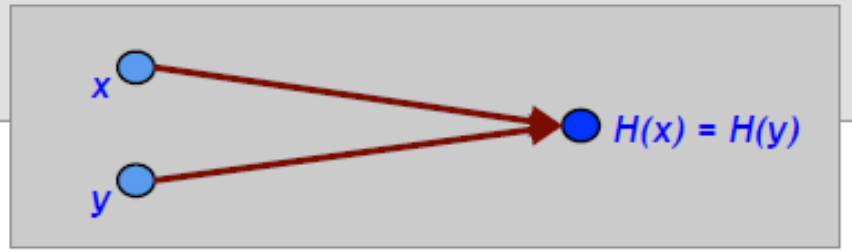
Cryptographic Hash Functions

A Hash Function is **cryptographically secure** if it satisfies the following 3 **security properties**:

- Property 1: Collision Resistance
- Property 2: Hiding
- Property 3: "Puzzle Friendliness"

Crypto Hash Property 1: Collision Resistance

Collision Resistance: A hash function *H* is said to be **collision resistant** if it is infeasible to find two values, *x* and *y*, such that *x != y*, yet *H(x) = H(y)*.



In other words: If we have *x* and *H(x)*, we can "never" find an *y* with a matching *H(y)*.

Collision Resistance

Application: Hash as a **Message Digest**

If we know that $H(x) = H(y)$, it is safe to assume that $x = y$.

Example: To recognize a file that we saw before, just remember its hash.

This works because hash is small.

Crypto Hash Property 2: Hiding

We want something like this:

Given *H(x)*, it is infeasible to find *x*.

Example:

H("heads")

H("tails")

easy to find *x*!

The value for *x* is easy to find because the distribution is not "spread out" (only two values!)

Crypto Hash Property 3: "Puzzle Friendliness"

Puzzle Friendliness: A hash function H is said to be **puzzle friendly** if for every possible n-bit output value y, if k is chosen from a distribution with high min-entropy, then it is infeasible to find x such that $H(k \,||\, x) = y$, in time significantly less than 2^n.

If a hash function is puzzle friendly, then there is no solving strategy for this type of puzzle that is much better than trying random values of x.

Bitcoin mining is just such a computational puzzle.

Hash Pointers

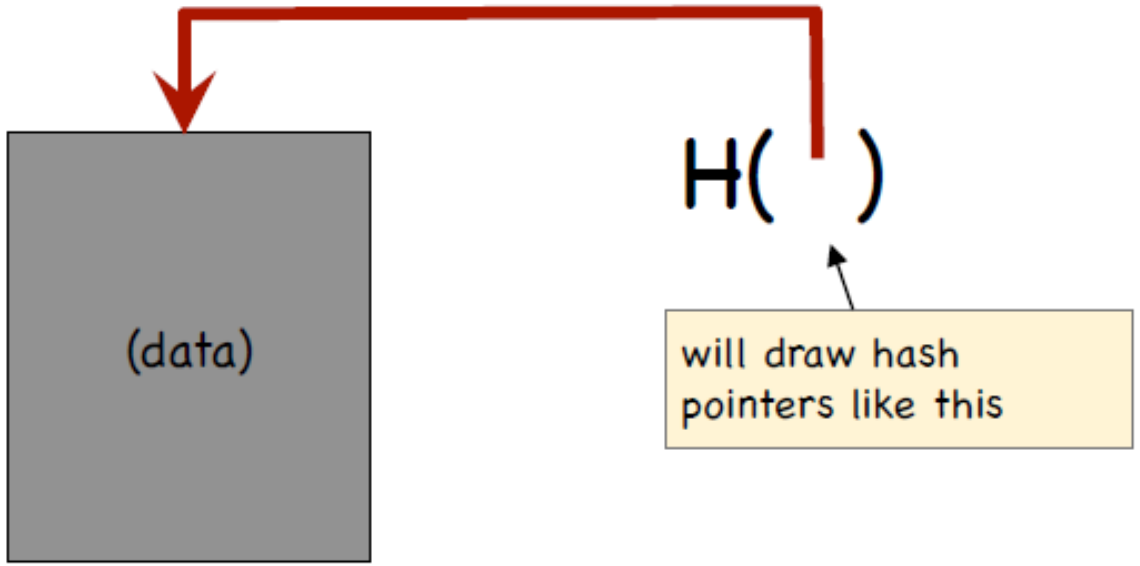
Hash Pointer is:

- pointer to where some info is stored, and
- (cryptographic) hash of the info

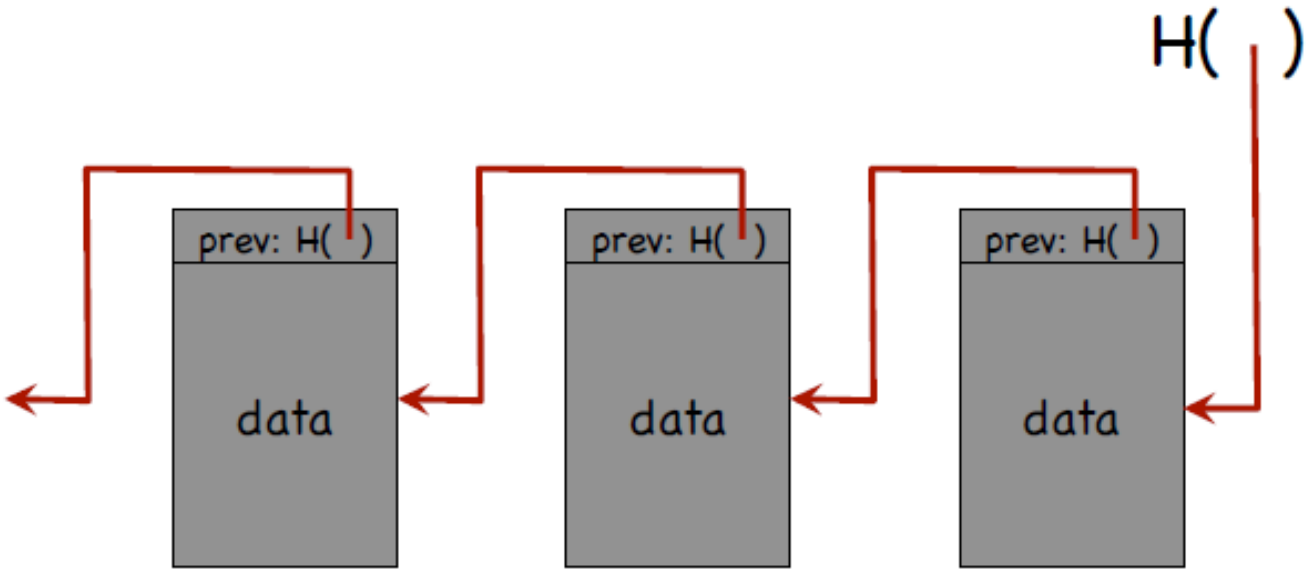
Given a Hash Pointer, we can

- ask to get the info back, and
- verify that it hasn't changed

Hash Pointers



Linked List with Hash Pointers: "Block Chain"



use case: tamper-evident log

Writing board 4

Digital Signatures

Q: What do we want from signatures?

Only you can sign, but anyone can verify.

Signature is tied to a particular document, i.e., cannot be cut-and-pasted to another document.

Digital Signature Scheme

Digital Signature Scheme consists of 3 algorithms:

- (sk,pk) := generateKeys(keysize) generates a key pair
  - *sk* is secret key, used to sign messages
  - *pk* is public verification key, given to anybody
- sig := sign(sk, msg) outputs signature for *msg* with key *sk*.
- verify(pk,msg,sig) returns true if signature is valid and false otherwise.

Signatures, Public Keys, and Identities

If you see a signature *sig* such that

verify(pk, msg, sig)==true,

think of it as

pk says, "*[msg]*".

Why?

Because to "speak for" *pk*, you must know the matching secret key *sk*.

How to Create a new Identity

Create a new, random key-pair *(sk, pk)*

- *pk* is the public "name" you can use
  [usually better to use *Hash(pk)*]
- *sk* lets you "speak for" the identity

You control the identity,
because only you know *sk*.

If *pk* "looks random", nobody needs to know who you are.

Decentralized Identity Management

By creating a key-pair,
anybody can make a new identity at any time.

Make as many as you want!

No central point of coordination.

These identities are called addresses in Bitcoin.

Identities and Privacy

Addresses are not directly connected to real-world identity.

But observer can link together an address' activity over time, and make inferences about real identity.

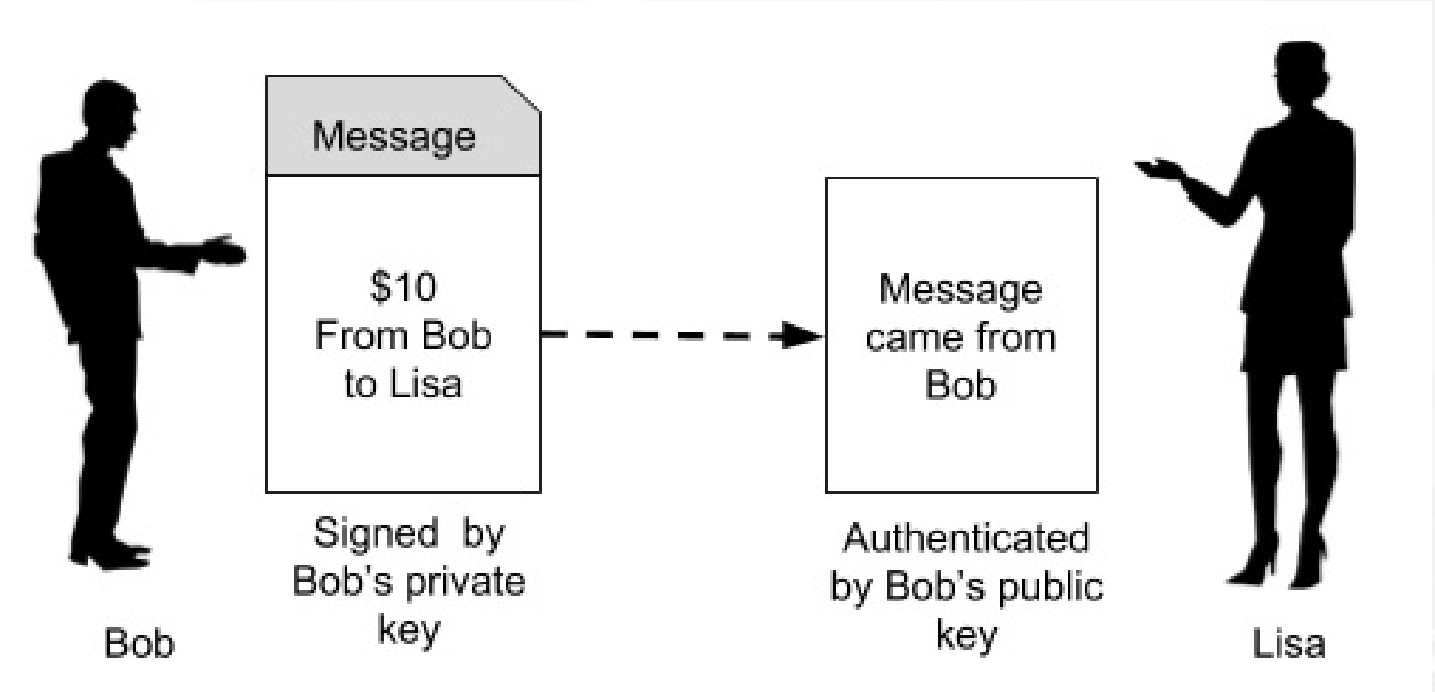
We will talk later about privacy in Bitcoin . . .

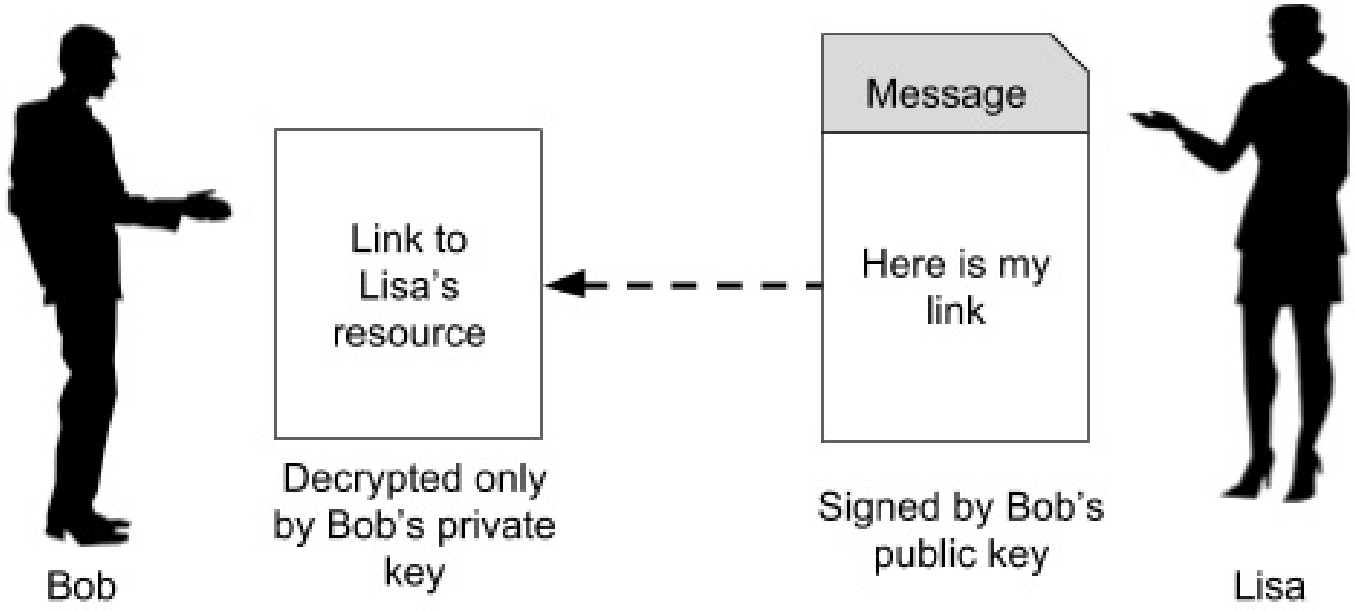
Role of PKI in BitCoins

- In case of Bitcoin, if you ever lose the private key to your Bitcoin wallet, the entire contents of your wallets would be instantly vulnerable to theft and before you know it, all your money (the contents of your wallet) would be gone with no mechanism in the system to trace out who stole it
- The PKI accomplish two functions - authentication and the message privacy through encryption/decryption mechanism

Authentication

- Now, Bob says that he is sending $10 to Lisa. So he creates a message (a plain-text message) containing Bob's (sender) public key, Lisa's (receiver) public key, and the amount ($10).
- The purpose of this remittance such as "I want to buy pumpkin from you" is also added into the message.
- The entire message is now signed using Bob's private key.
- When Lisa receives this message, she will use the signature verification algorithm of PKI and Bob's public key to ensure that the message indeed originated from Bob.





Message Privacy

The Lisa creates a message such as “Here is the link to my ebook which you had requested”, signs it with Bob’s public key that she has received in Bob’s request message and also encrypts the message using some secret key which is shared between the two during HTTPS handshake.

Writing board 5

Vanilla Cryptocurrency Ver. 0.0

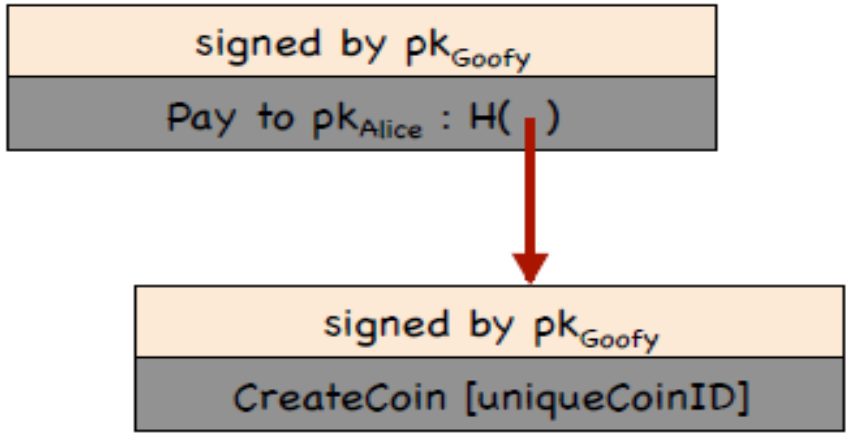
GoofyCoin

Goofy can create new Coins

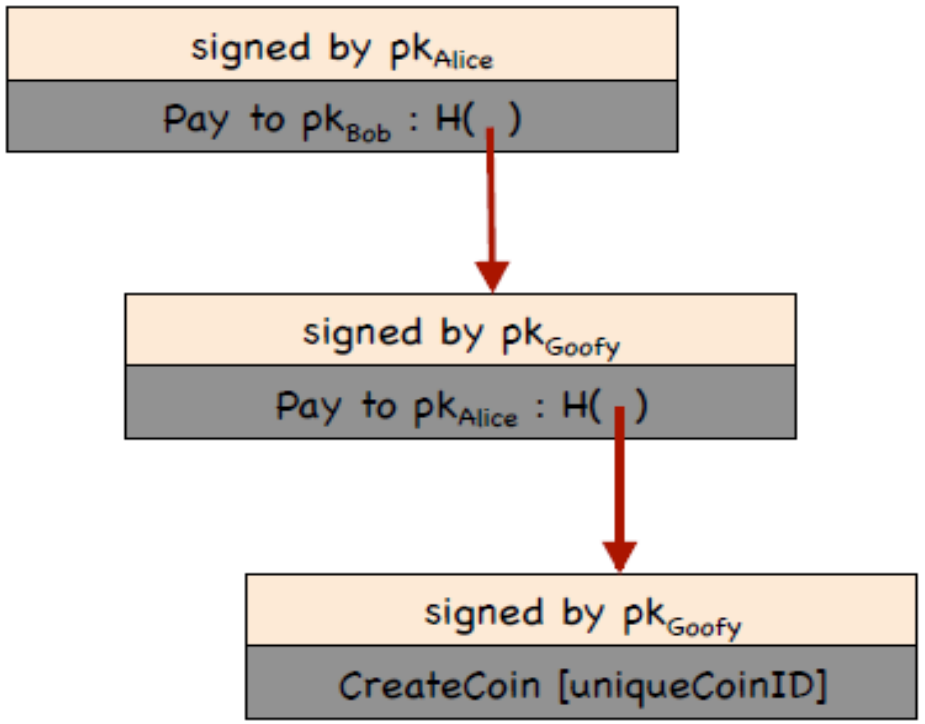
signed by pk_{Goofy}

CreateCoin [uniqueCoinID]

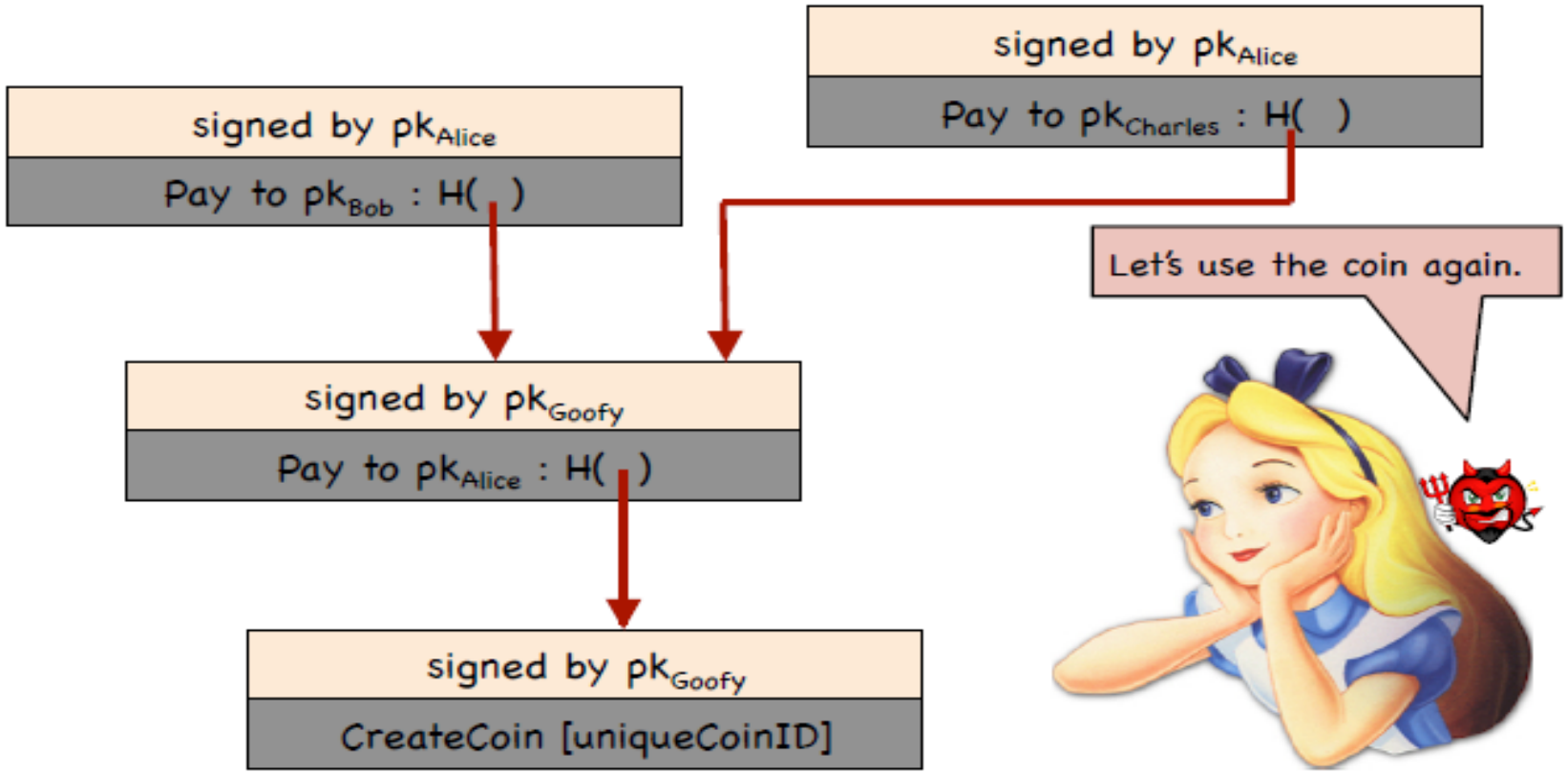
Goofy can spend the Coins



The Recipient can pass on the Coin again



The Recipient can also double-spend the coin!



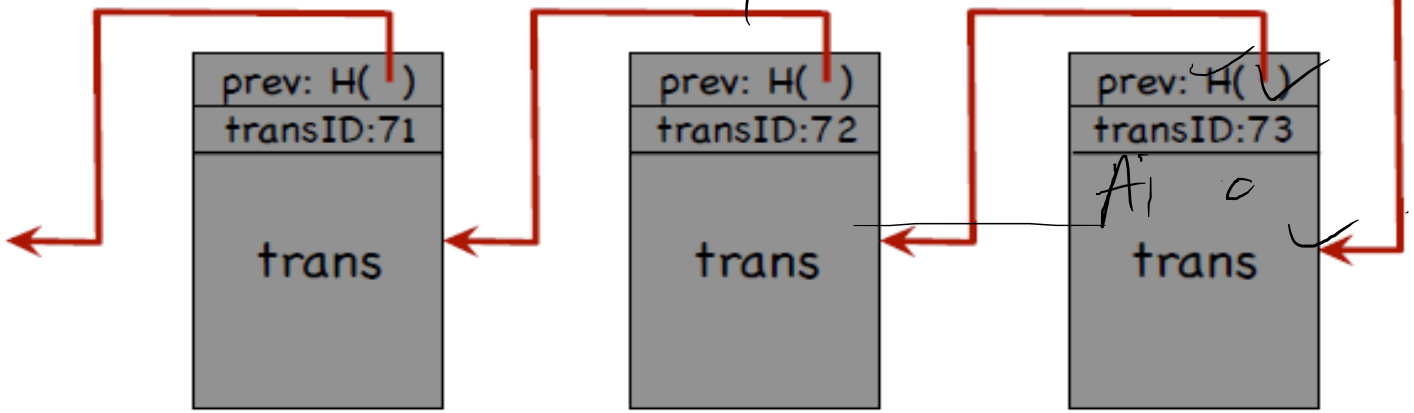
Vanilla Cryptocurrency Ver. 1.0

ScroogeCoin

Record Transactions in central Block Chain

Scrooge publishes a history of all transactions
(a block chain, signed by Scrooge)

H( )



optimization: put multiple transactions in the same block

Creating new Coins in ScroogeCoin

`CreateCoins` transaction creates new coins

Valid, because I said so!

transID: 73 type:CreateCoins		
coins created		
num	*value*	*recipient*
0	3.2	0x...
1	1.4	0x...
2	7.1	0x...

coinID 73(0)

coinID 73(1)

coinID 73(2)

The Problem with ScroogeCoin

Crucial question:

Can we descroogify the currency, and operate without any central, trusted party?

Writing board 6

Bank Frauds

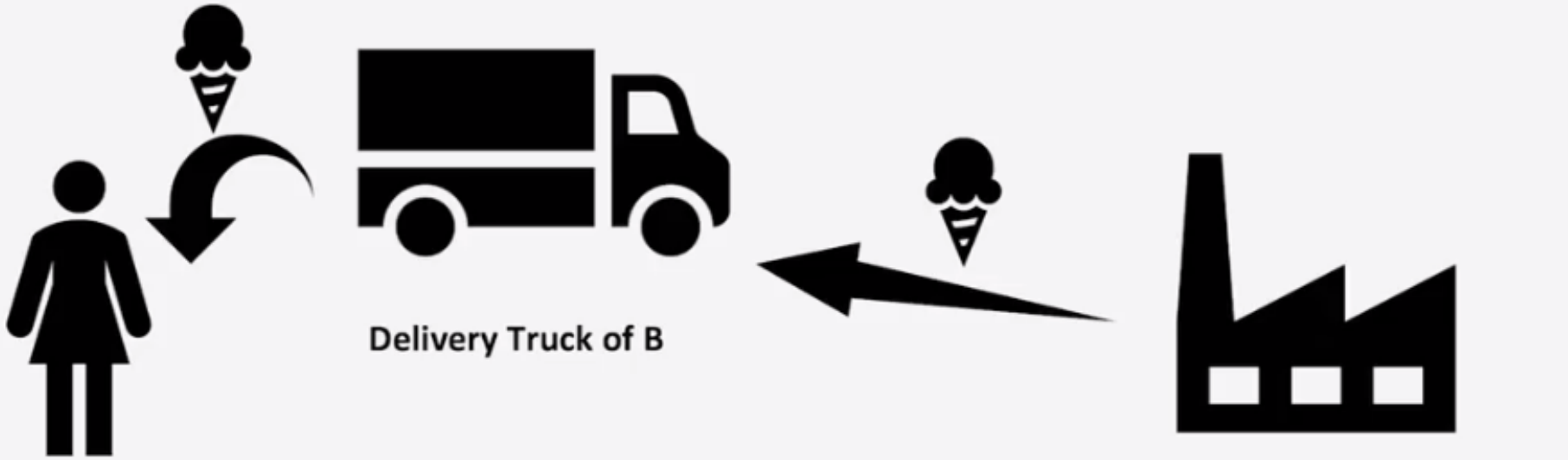
- You find a check was used to pay someone but you never wrote the check
  - Someone forged your check and/or signature
- You did sign a check for x amount, but the amount field was modified
  - How do you prove to the bank that an extra 0 was not there in your signing time?
- The monthly statement says that you did a transaction but you did not recall or the amount of a transaction is different from what you had done
  - Someone got your password, and possibly redirected OTP to another SIM (SIM Fraud)
  - Bank employees themselves might have done something
- How do you argue to the bank? (Non-repudiation)
- How do you argue that the amount was modified? (Integrity)
- Finally, do you tally your transactions when you receive your monthly statement?
  - Most people do not

Land Record

- Have you watched “Khosla ka Ghosla”?
- You buy a piece of land
- Someone else claims to own the land
- But the one who sold you the land showed you paper work
- Land registry office earlier said that the owner was rightful
- Now they say that they made a mistake – it was owned by the other person
- You already paid for the land – to the first person
- First person goes missing

  How does any one prove who changed the land record?
  - The government employees?

Back to the supply Chain Story (Herlihy)

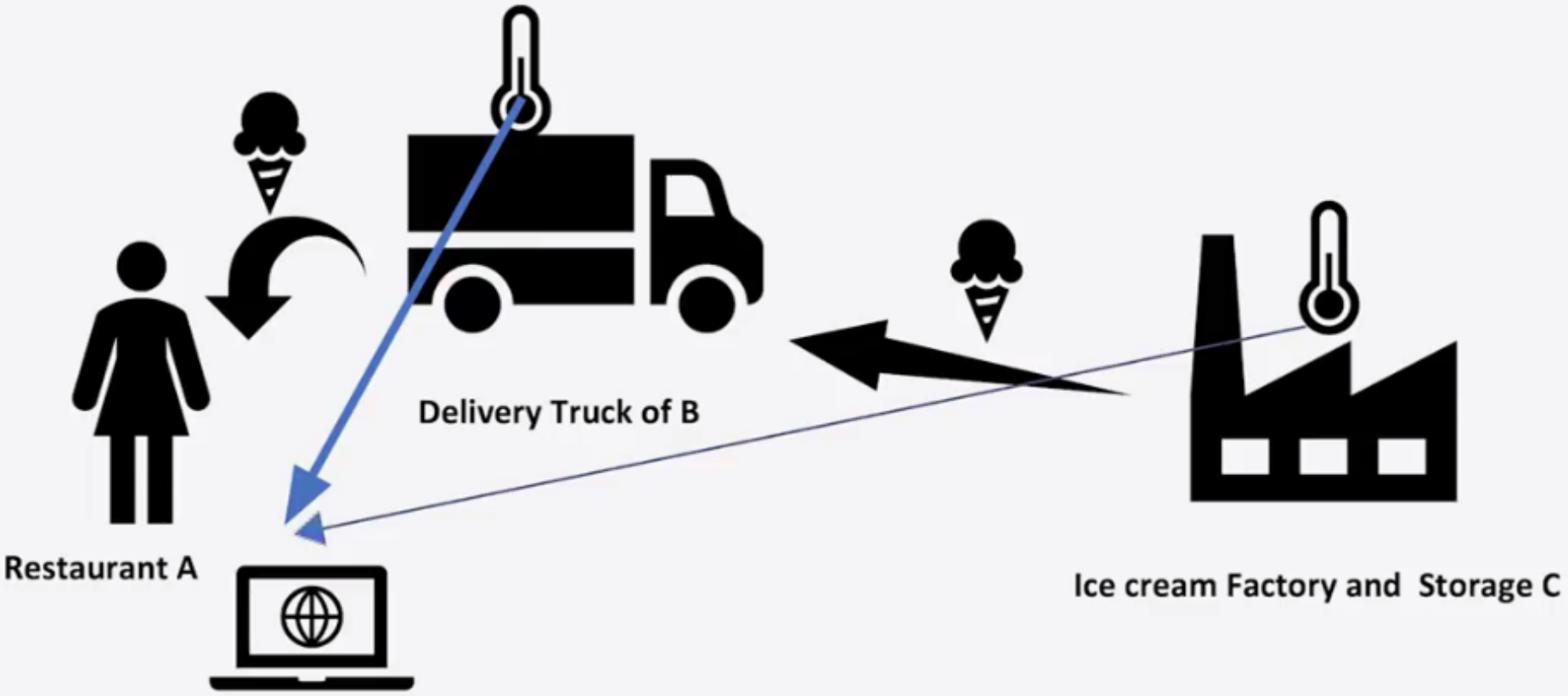


Ice Cream Supply Chain to Restaurant A from Factory C via Supplier B

Supply chain and provenance

- Your buy ice cream for your restaurant from supplier B
- Supplier B actually transports ice cream made in Company C's factory
- Upon delivery, you have been finding that your ice cream is already melted
- Who is responsible?
  - Supplier B is keeping it too long on the delivery truck?
  - Supplier B's storage facility has a temperature problem?
  - Supplier C says it's supplier B's fault as when picked up – ice cream was frozen
  - Supplier B says that when received, the temperature was too high, so C must have stored it or made it wrong
  - How do you find the truth?
    - Put temperature sensors in B's truck and storage, C's factory and storage, and sensor data is digitally signed by the entity where the sensor is placed and put in a log
    - You check the log – but B and C both have hacked the log and deleted some entries?
  - What to do?

Use IoT to create non-repudiation



IoT sensors sends real-time data to the server at Restaurant A to periodically show the factory and the truck temperatures to Restaurant A

What can go wrong?

- IoT sensor data may be intercepted by a middle man and changed before it reaches the server (**data integrity**)
- IoT sensors may be stopped and old readings may be replayed (**replay attack**)
- What the server gets purportedly from factory C, may be manufactured by supplier B (**Authenticity**)
- If restaurant A claims that C's temperature reading shows that ice cream was melting in the storage, C can say that message you received is not from me – there was an MITM attack (**repudiation**)

- So restaurant A will not be able to pinpoint any one in the supply chain with full confidence!!

What can be done?

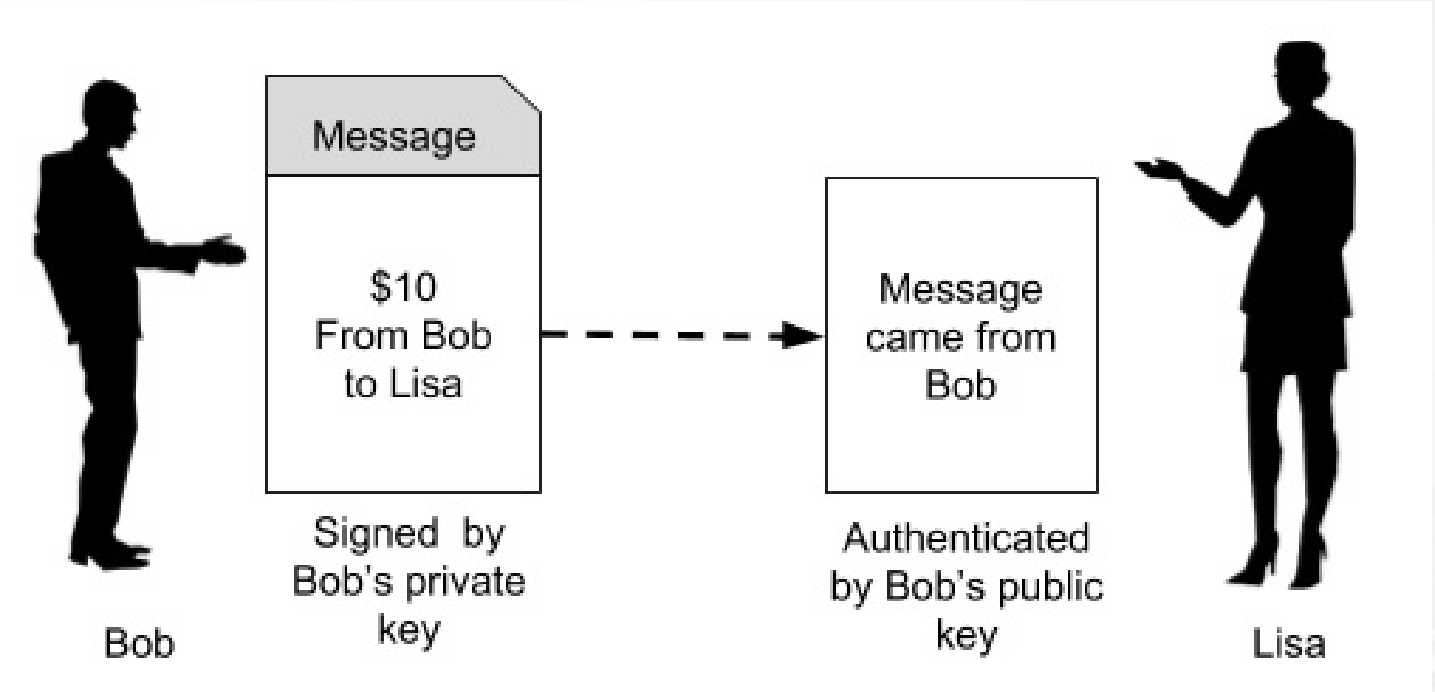
- Use a message integrity proof (Hashing)
- Use digital signature of the individual IoT devices (Authenticity and non-repudiation)
  - assuming the digital signatures cannot be forged
  - private keys are kept safe
- Use authentic time stamping with the IoT data before hashing for integrity (avoid replay attacks)
- So now factory A can pinpoint with some basic security assumptions about this infrastructure

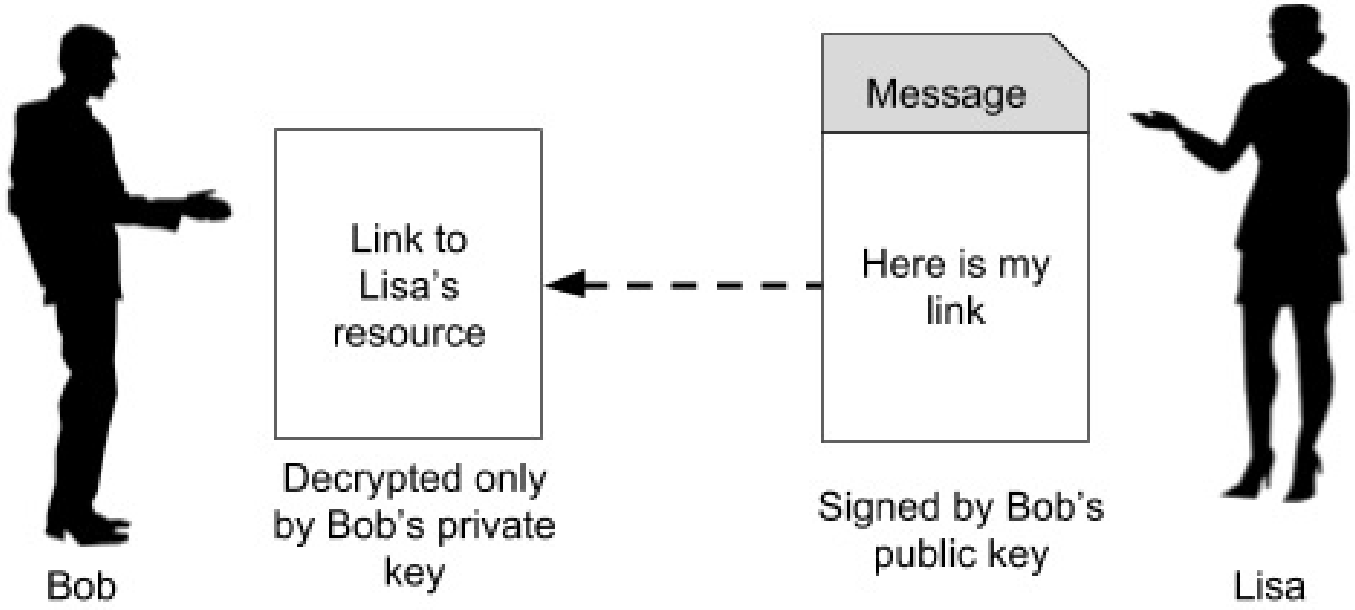
Role of PKI in BitCoins

- In case of Bitcoin, if you ever lose the private key to your Bitcoin wallet, the entire contents of your wallets would be instantly vulnerable to theft and before you know it, all your money (the contents of your wallet) would be gone with no mechanism in the system to trace out who stole it
- The PKI accomplish two functions - authentication and the message privacy through encryption/decryption mechanism

Authentication

- Now, Bob says that he is sending $10 to Lisa. So he creates a message (a plain-text message) containing Bob's (sender) public key, Lisa's (receiver) public key, and the amount ($10).
- The purpose of this remittance such as "I want to buy pumpkin from you" is also added into the message.
- The entire message is now signed using Bob's private key.
- When Lisa receives this message, she will use the signature verification algorithm of PKI and Bob's public key to ensure that the message indeed originated from Bob.



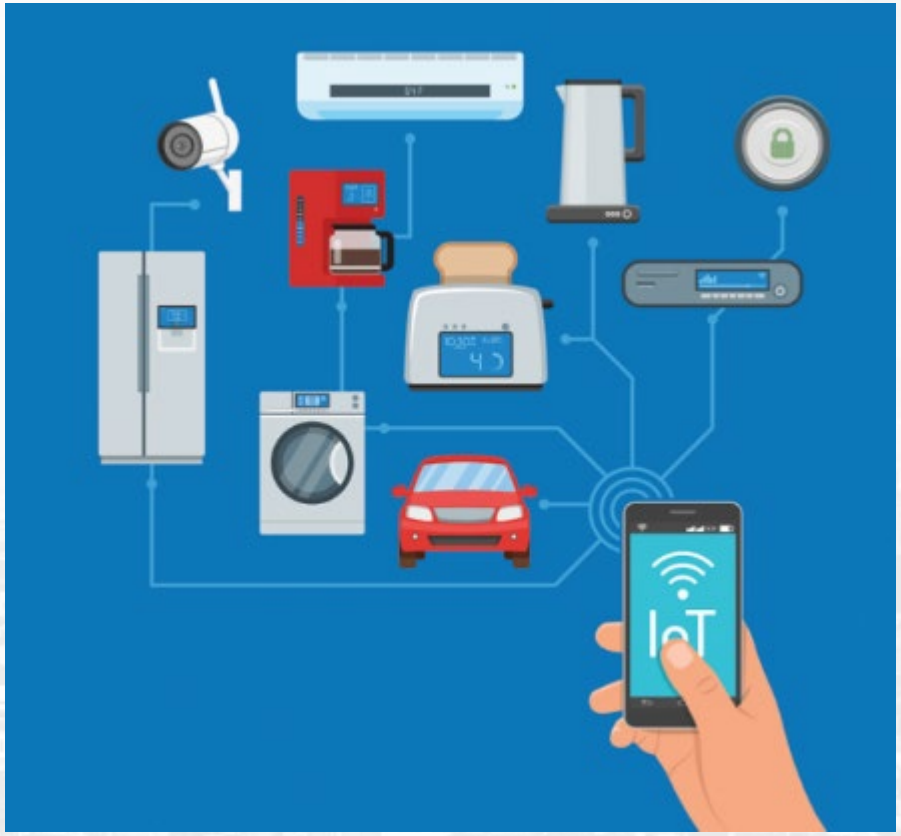


Message Privacy

The Lisa creates a message such as “Here is the link to my ebook which you had requested”, signs it with Bob’s public key that she has received in Bob’s request message and also encrypts the message using some secret key which is shared between the two during HTTPS handshake.

Block Applications

- Secure sharing of medical data
- Real estate processing platform
- Music royalties tracking
- Cross-border payments
- Real-time IoT operating systems
- Personal identity security
- Anti-money laundering tracking system
- Supply chain and logistics monitoring
- Voting mechanism
- Advertising insights
- Original content creation
- Cryptocurrency exchange



Blockchain Features / Advantages

- **Resilience:** Blockchains is often replicated architecture. The chain is still operated by most nodes in the event of a massive attack against the system.
- **Time reduction:** In the financial industry, blockchain can play a vital role by allowing the quicker settlement of trades as it does not need a lengthy process of verification, settlement, and clearance because a single version of agreed-upon data of the share ledger is available between all stack holders.
- **Reliability:** Blockchain certifies and verifies the identities of the interested parties. This removes double records, reducing rates and accelerates transactions.
- **Unchangeable transactions:** By registering transactions in chronological order, Blockchain certifies the unalterability, of all operations which means when any new block has been added to the chain of ledgers, it cannot be removed or modified.

Immutable

Blockchain Features / Advantages

- **Fraud prevention:** The concepts of shared information and consensus prevent possible losses due to fraud or embezzlement. In logistics-based industries, blockchain as a monitoring mechanism act to reduce costs.
- **Security:** Attacking a traditional database is the bringing down of a specific target. With the help of Distributed Ledger Technology, each party holds a copy of the original chain, so the system remains operative, even the large number of other nodes fall.
- **Transparency:** Changes to public blockchains are publicly viewable to everyone. This offers greater transparency, and all transactions are immutable.
- **Collaboration** – Allows parties to transact directly with each other without the need for mediating third parties.
- **Decentralized:** There are standards rules on how every node exchanges the blockchain information. This method ensures that all transactions are validated, and all valid transactions are added one by one.

- **Blockchain 1.0: Currency**

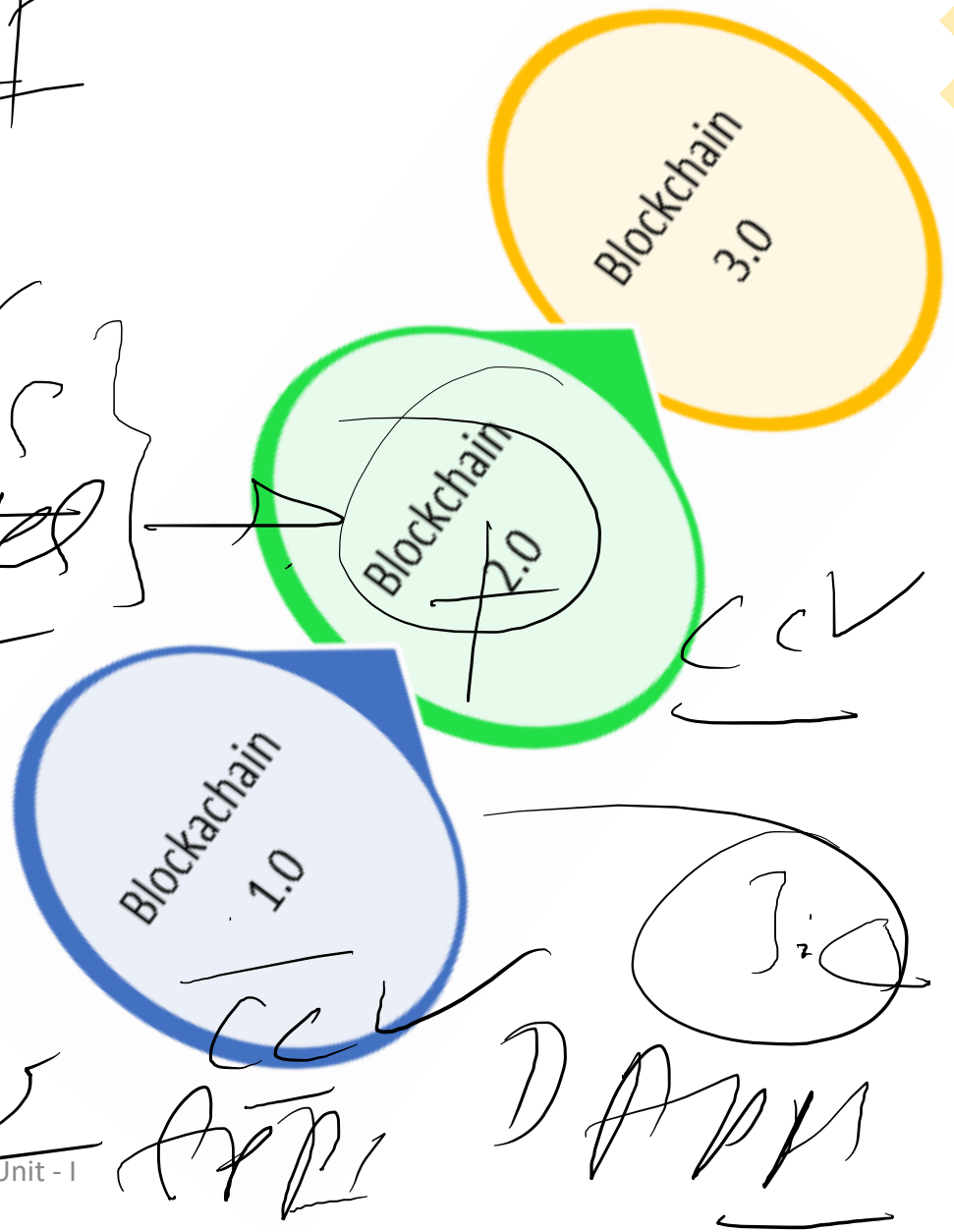
The implementation of DLT (distributed ledger technology) led to its first and obvious application: cryptocurrencies. This allows financial transactions based on blockchain technology. It is used in currency and payments. Bitcoin is the most prominent example in this segment.

- **Blockchain 2.0: Smart Contracts**

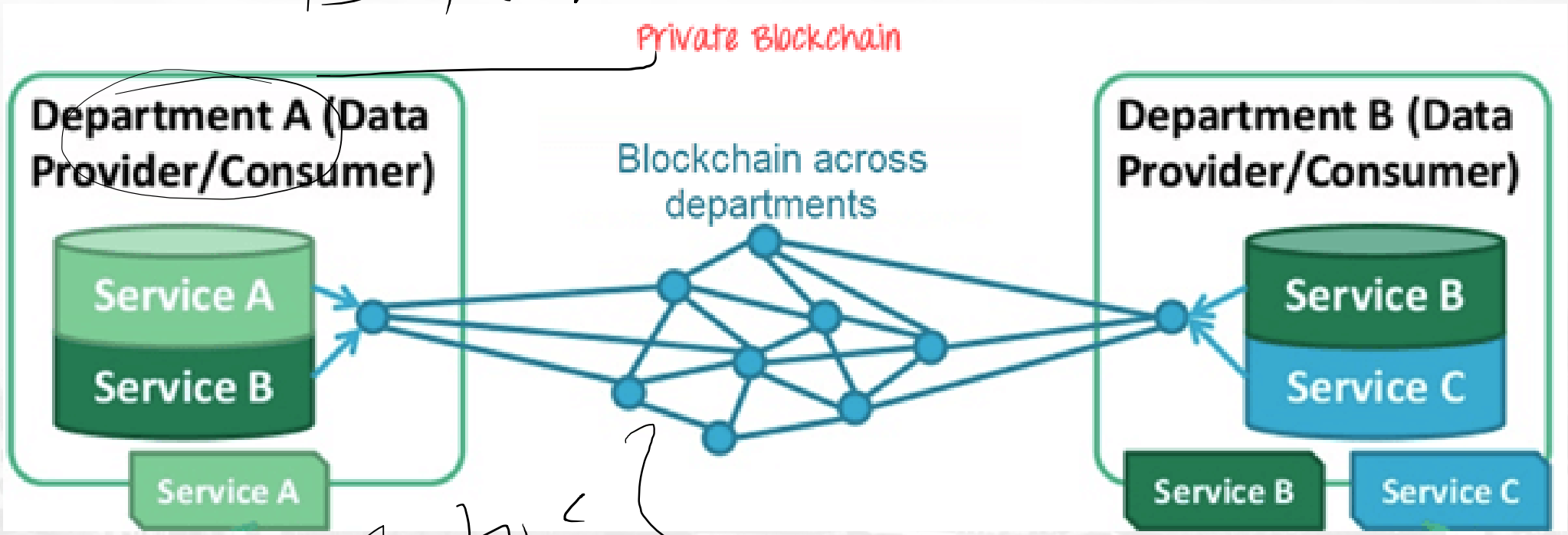
The new key concepts are Smart Contracts, small computer programs that "live" in the blockchain. They are free computer programs that execute automatically, and check conditions defined earlier like facilitation, verification or enforcement. It is used as a replacement for traditional contracts.

- **Blockchain 3.0: DApps:**

DApps is an abbreviation of decentralized application. It has their backend code running on a decentralized peer-to-peer network. A DApp can have frontend Blockchain example code and user interfaces written in any language that can make a call to its backend, like a traditional Apps.



Block Chain Types



Types of Blochains

- **Public:**

In this type of blockchains, ledgers are visible to everyone on the internet. It allows anyone to verify and add a block of transactions to the blockchain. Public networks have incentives for people to join and free for use. Anyone can use a public blockchain network.

- **Private:**

The private blockchain is within a single organization. It allows only specific people of the organization to verify and add transaction blocks. However, everyone on the internet is generally allowed to view.

- **Consortium:**

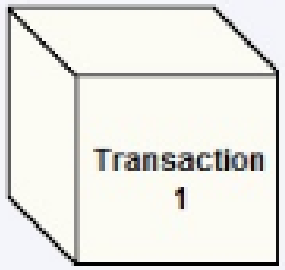
In this Blockchain variant, only a group of organizations can verify and add transactions. Here, the ledger can be open or restricted to select groups. Consortium blockchain is used cross-organizations. It is only controlled by pre-authorized nodes.

Limitations of Blockchain technology

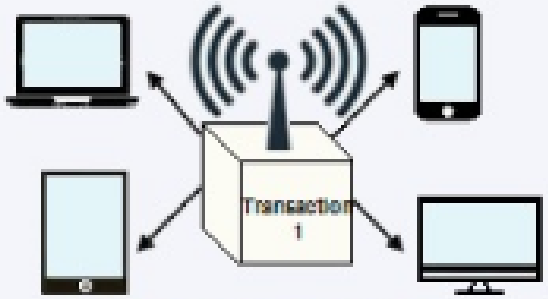
- **Higher costs:** Nodes seek higher rewards for completing Transactions in a business which work on the principle of Supply and Demand
- **Slower transactions:** Nodes prioritize transactions with higher rewards, backlogs of transactions build up
- **Smaller ledger:** It not possible to a full copy of the Blockchain, potentially which can affect immutability, consensus, etc.
- **Transaction costs, network speed:** The transactions cost of Bitcoin is quite high after being touted as 'nearly free' for the first few years.
- **Risk of error:** There is always a risk of error, as long as the human factor is involved. In case a blockchain serves as a database, all the incoming data has to be of high quality. However, human involvement can quickly resolve the error.
- **Wasteful:** Every node that runs the blockchain has to maintain consensus across the blockchain. This offers very low downtime and makes data stored on the blockchain forever unchangeable. However, all this is wasteful, because each node repeats a task to reach consensus.

Blockchain Process

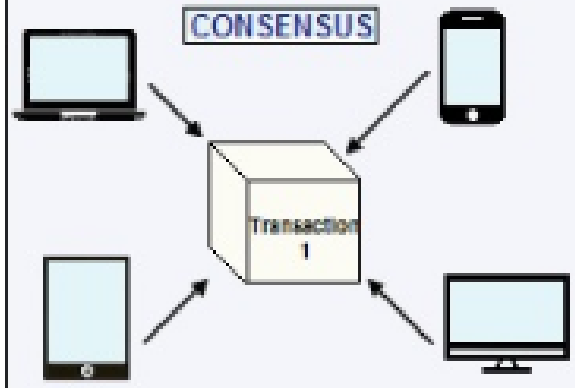
1. Ivy buys something from Joe & initiated payment.



2. A block is created with Ivy's transaction.

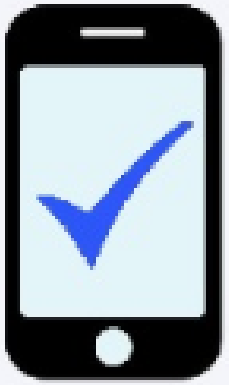


3. The transaction and block are broadcasted to everyone on its network.



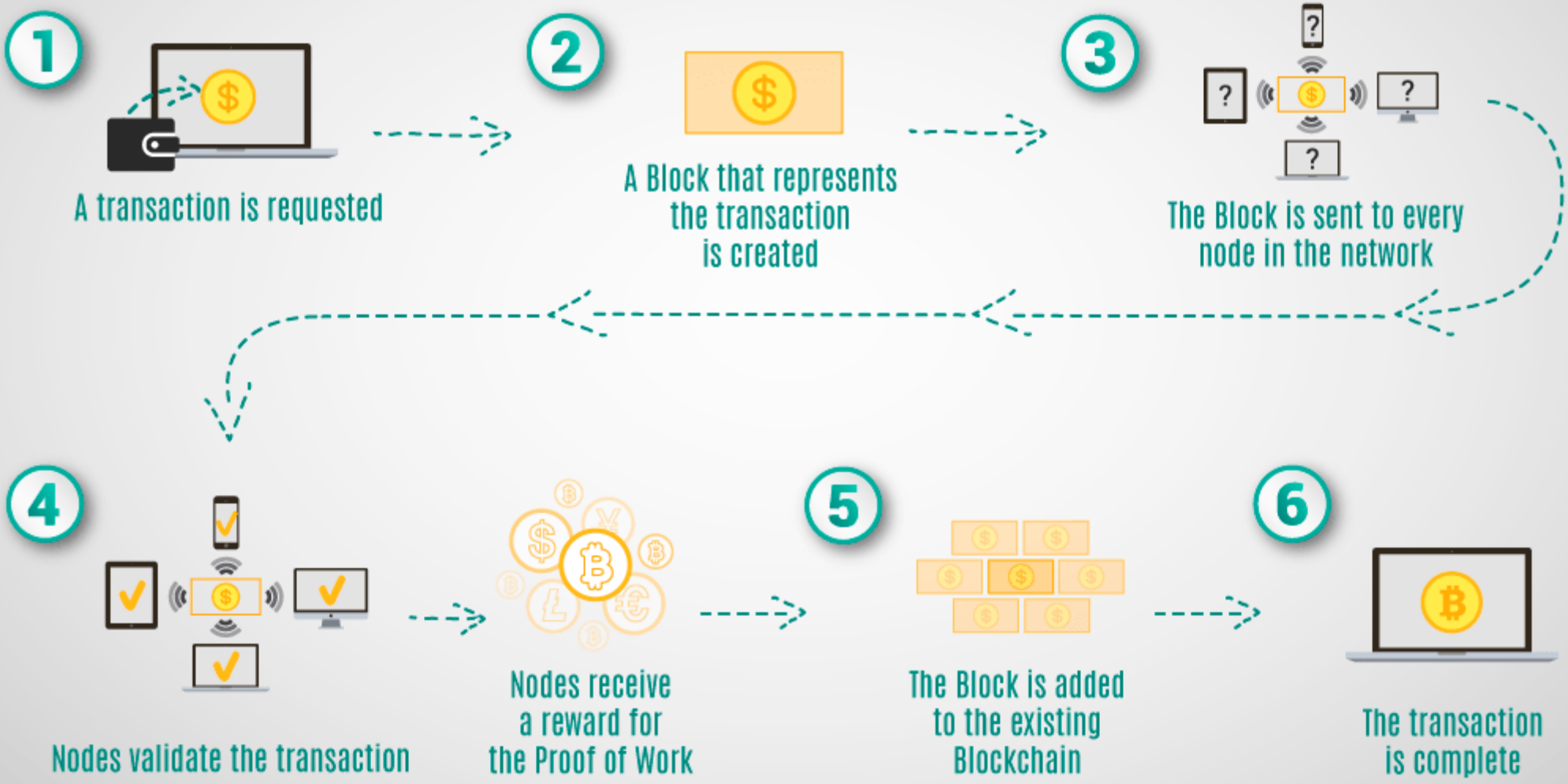
4. The transaction is verified by everybody on its network.

5. The verified block is time-stamped & chained to the previous block in the chain.



6. Blockchain is updated. Joe receives payment from Ivy.

HOW BLOCKCHAIN WORKS



HOW DO BITCOINS WORK?

Miners create bitcoins by using computers to solve mathematical functions. he same process also verifies previous transactions

Bitcoin exchanges will trade between conventional currencies and bitcoin.offering a way into the market for non-miners, as well as way to cash out

Users download a bitcoin 'wallet' that works a little like an email adress, proiding a way to store and receie currency. Bitcoins can be transferred from one wallet to another using a web browser or a pone app

Business create a wallet in the wame way as an individual user, typically using a website button to enable a bitcoin payment for inthe flesh enterprises, QR codes can be used to let customers pay quickly and easily

Merkle Trees in BlockChain

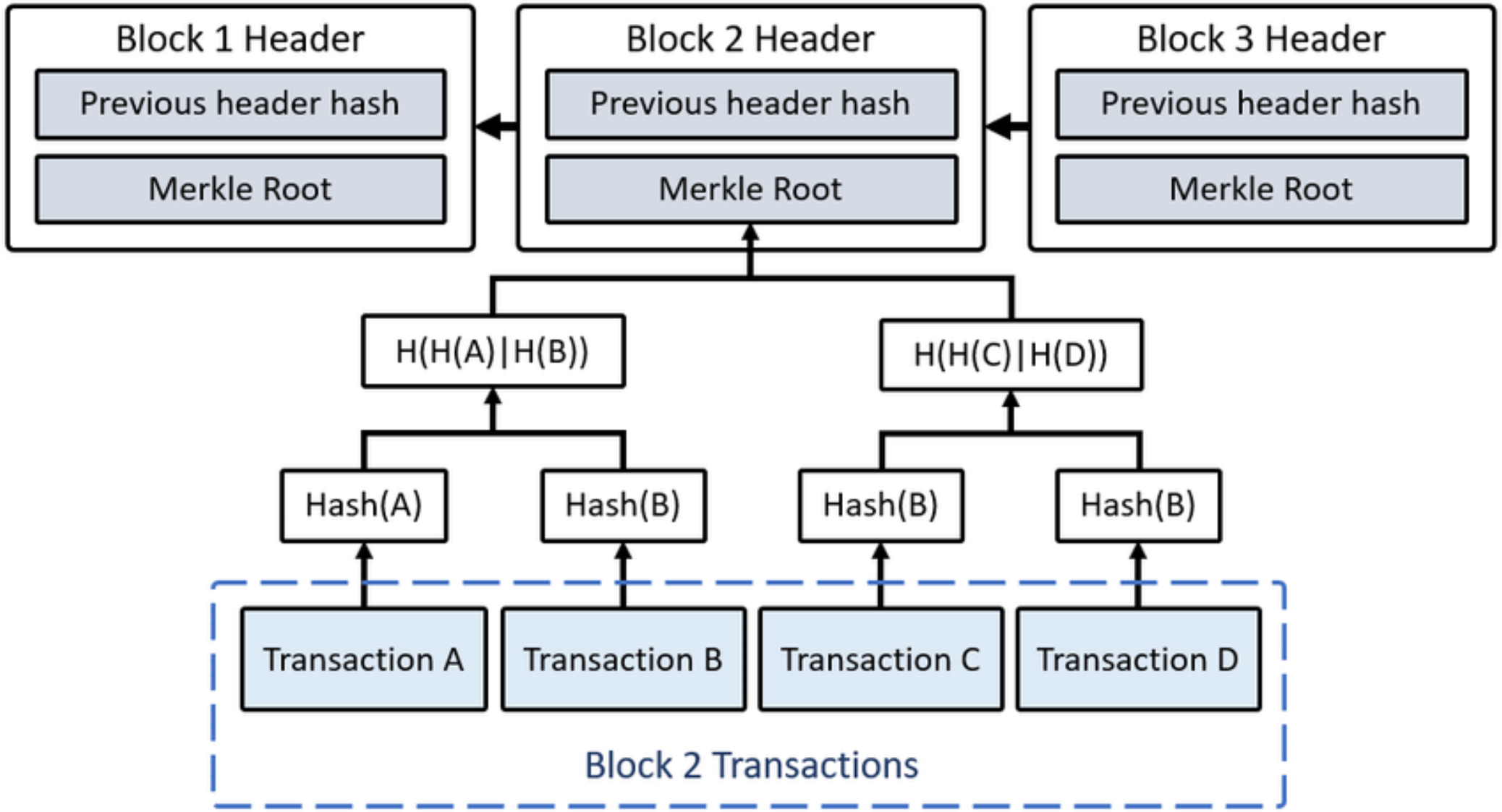
- Merkle tree is a fundamental part of blockchain technology.
- It is a mathematical **data structure** composed of hashes of different blocks of data, and which serves as a summary of all the transactions in a block.
- It also allows for efficient and secure verification of content in a large body of data.
- It also helps to verify the consistency and content of the data. Both Bitcoin and Ethereum use Merkle Trees structure.
- Merkle Tree is also known as **Hash Tree**.
- The concept of Merkle Tree is named after **Ralph Merkle**, who patented the idea in **1979**.
- Fundamentally, it is a data structure tree in which every **leaf node** labelled with the hash of a data block, and the **non-leaf node** labelled with the cryptographic hash of the labels of its child nodes. The leaf nodes are the lowest node in the tree.

Merkle Trees in Block chain

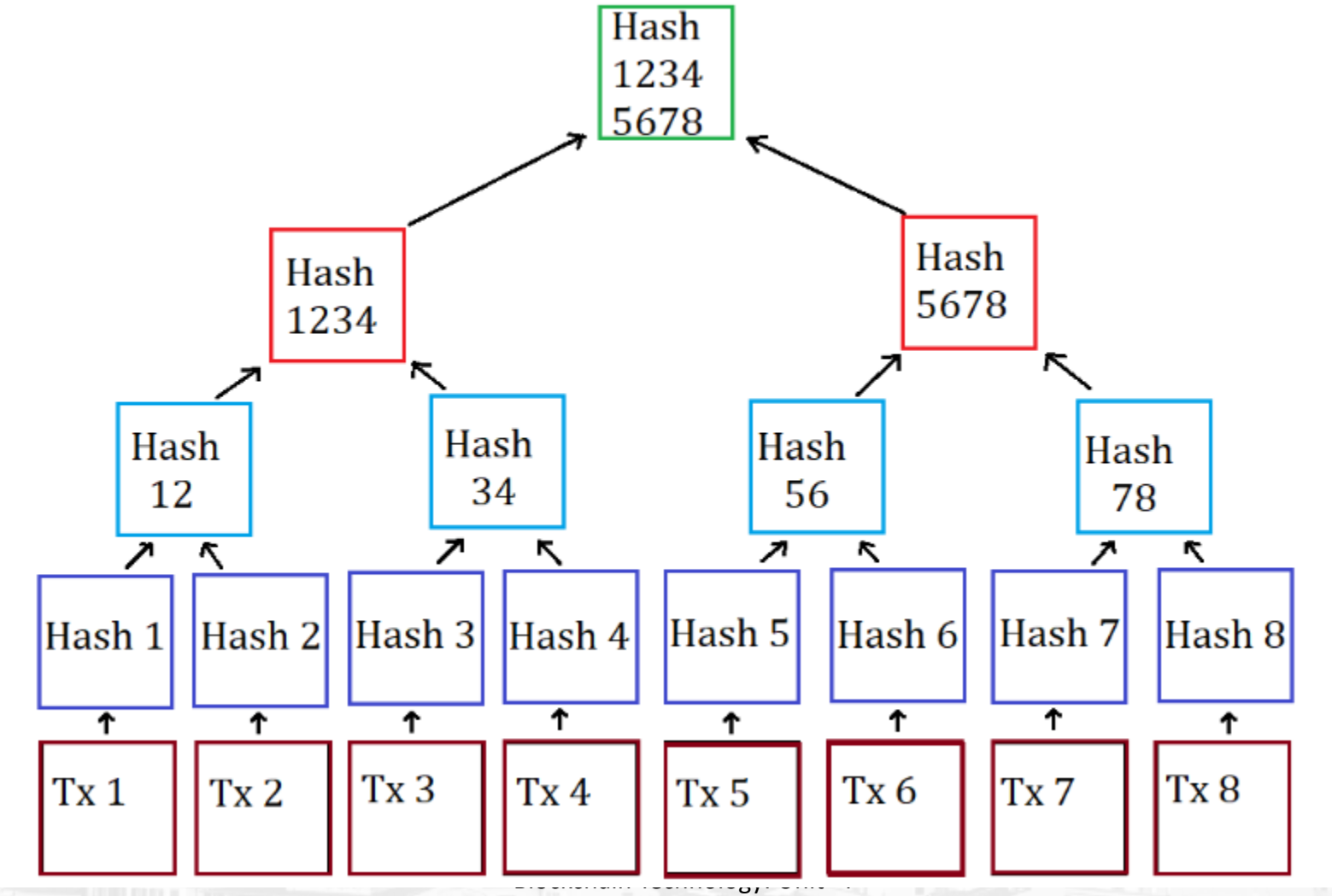
- Merkle trees are created by repeatedly calculating hashing pairs of nodes until there is only one hash left.
- This hash is called the Merkle Root, or the Root Hash. The Merkle Trees are constructed in a bottom-up approach.
- The Merkle Tree maintains the integrity of the data. If any single detail of transactions or order of the transaction's changes, then these changes reflected in the hash of that transaction.
- This change would cascade up the Merkle Tree to the Merkle Root, changing the value of the Merkle root and thus invalidating the block. So everyone can see that Merkle tree allows for a quick and simple test of whether a specific transaction is included in the set or not.

Merkle trees have three benefits:

- It provides a means to maintain the integrity and validity of data.
- It helps in saving the memory or disk space as the proofs, computationally easy and fast.
- Their proofs and management require tiny amounts of information to be transmitted across networks.


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

Merkle Trees in Block chain



Visualization

- https://blog.iden3.io/merkle-trees-visual-introduction.html

Blockchain Council

- Blockchain Council provides certification for blockchain, which is specially designed for the people who want to make a career in the blockchain domain.
- This certification requires in-depth knowledge of the core concept of blockchain.
- It focuses on Corda, Smart Contracts, Hyperledger, Quorum applications.
- Blockchain Council certification can be helpful to work in industries like digital marketing, healthcare, supply chain, etc.

Blockchain Council certifications

- A Certified Blockchain Expert
- Certified Corda Expert
- Certified Corda Architect
- Certified Blockchain Developer
- Certified BlockChain Security Professional
- Certified Smart Contract Developer
- Certified Bitcoin Expert
- Certified Ethereum Expert

Myth	Reality
It solves every problem	No, it is just a database
Trustless Technology	It can shift trust and also spread trust
Secure	It focuses integrity and not confidentiality
Smart contracts are always legal	It only executes parts of some legal contracts
Immutable	It only offers probabilistic immutability
Need to waste electricity	Emerging blockchains are efficient
It is inherently unscalable	Emerging blockchains are scalable

Real Case studies of Block chain

1.Dubai: The Smart City

In the year 2016, smart Dubai office introduced Blockchain strategy. Using this technology entrepreneurs and developers will be able to connect with investor and leading companies. The objective is to implement blockchain base system which favors the development of various kind of industries to make Dubai 'the happiest city in the world.'

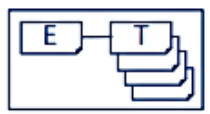
2. Blockchain for Humanitarian Aid

In January 2017 the united nations world food program started a project called humanitarian aid. The project was developed in rural areas of the Sindh region of Pakistan. By using the Blockchain technology, beneficiaries received money, food and all type of transactions are registered on a blockchain to ensure security and transparency of this process.

Block Chain vs DDatabase

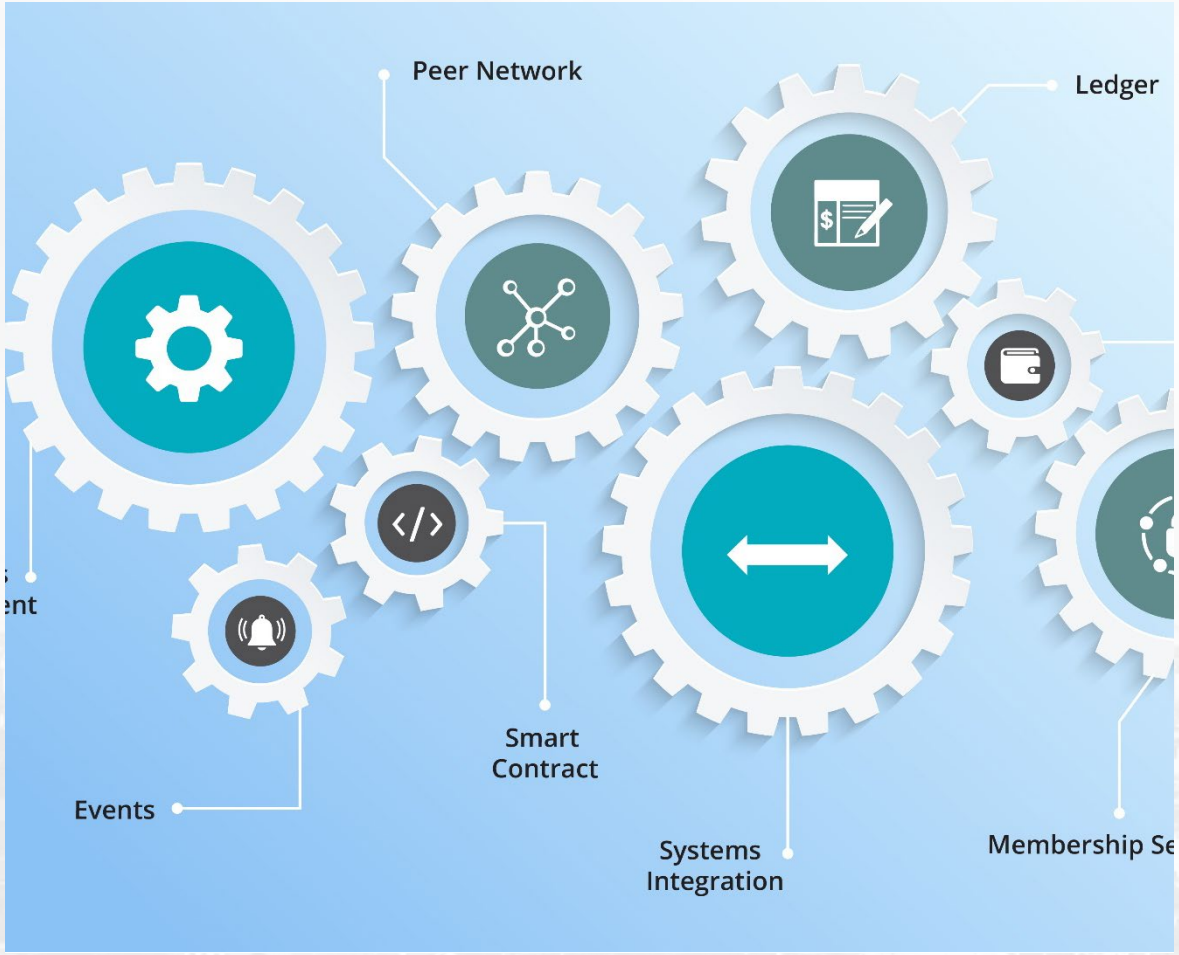
Parameters	Blockchain	Shared Database
Operations	Insert	Create/ Read/ Update and Delete
Replication	Full replication on every peer	Master-slave Multi-master
Consensus	Most of the peers agree on the outcome of transactions.	Distributed transactions which held in two phases commit and Paxos.
Validation	Global rules enforced on the whole blockchain system.	Offers only local integrity constraints
Disintermediation	It is allowed with blockchain.	Not allowed.
Confidentiality	Fully confidential	Not totally confidential
Robustness	Fully robust technology.	Not entirely robust.

Blockchain Components

Ledger		contains the current world state of the ledger and a Blockchain of transaction invocations
Smart Contract		encapsulates business network transactions in code. transaction invocations result in gets and sets of ledger state
Consensus Network		a collection of network data and processing peers forming a Blockchain network. Responsible for maintaining a consistently replicated ledger
Membership		manages identity and transaction certificates, as well as other aspects of permissioned access
Events		creates notifications of significant operations on the Blockchain (e.g. a new block), as well as notifications related to smart contracts. Does not include event distribution.
Systems Management		provides the ability to create, change and monitor Blockchain components
Wallet		securely manages a user's security credentials
Systems Integration		responsible for integrating Blockchain bi-directionally with external systems. Not part of Blockchain, but used with it.

https://www.beingcrypto.com/

Blockchain Components



The blockchain is built of several different types of components, each with a specific role to play within the blockchain's operation:

- **Ledger**: A distributed, immutable historical record
- **Peer Network**: Stores, updates, and maintains the ledger
- **Membership Services**: User authentication, authorization, and identity management
- **Smart Contract**: Program that runs on the blockchain
- **Wallet**: Stores users' credentials
- **Events**: Notifications of updates and actions on the blockchain
- **Systems Management**: Component creation, modification, and monitoring
- **Systems Integration**: Integration of blockchain with external systems.

Block Components

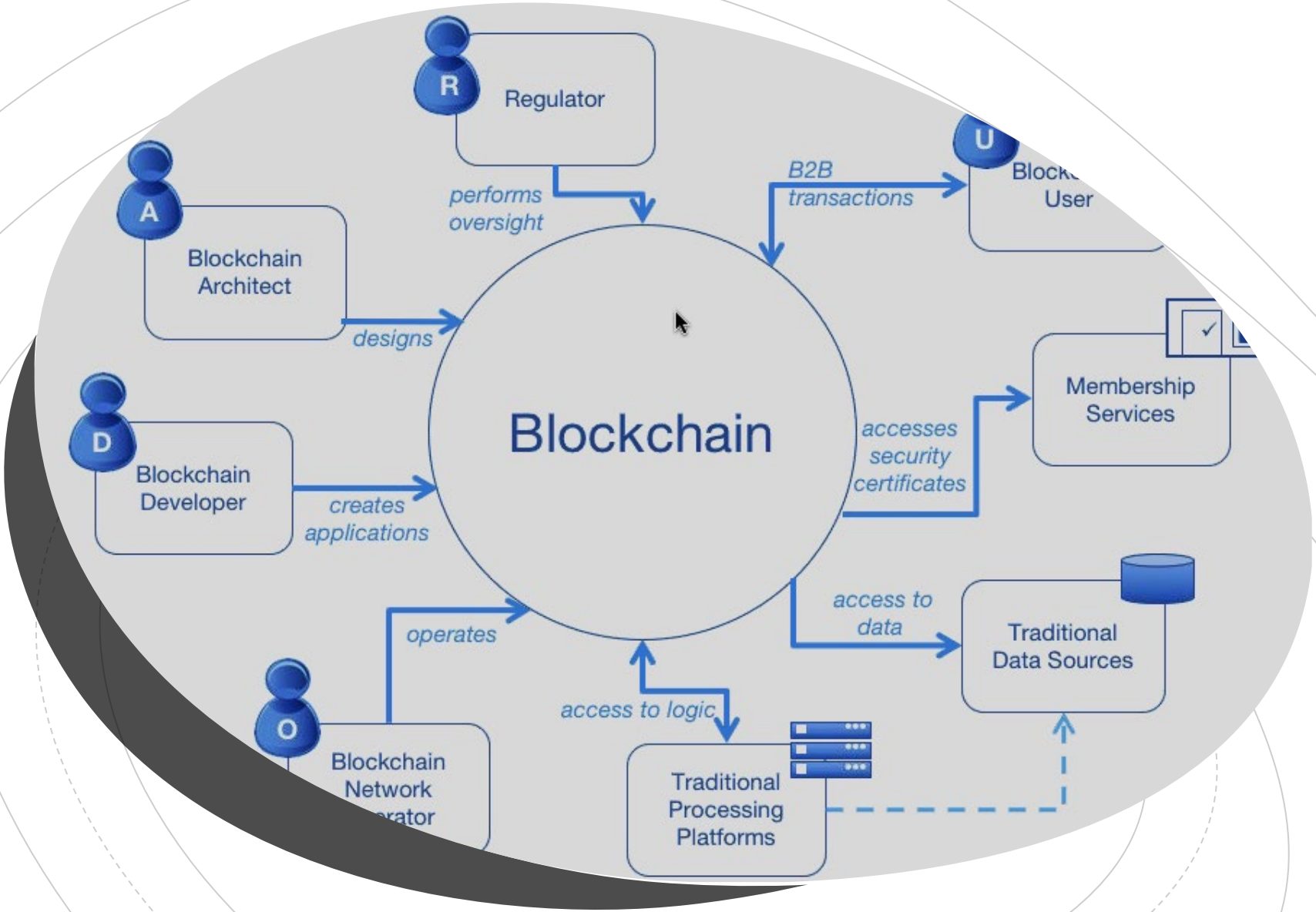
- **Ledger: A distributed, immutable historical record**
  The goal of the blockchain is to create a distributed, immutable record of the history of the blockchain called the ledger.
- **Peer Network: Stores, updates, and maintains the ledger**
  The ledger is stored, updated, and maintained by a peer network. Each node in this network maintains its own copy of the ledger. It is the job of the network as a whole to come to a consensus on the contents of each update to the ledger. This ensures that each individual copy of the ledger is identical without requiring a centralized "official" copy of the ledger.
- **Membership Services: User authentication, authorization, and identity management**
  On some blockchains, anyone can join the peer network and all network members have equal powers and authority. Permissioned blockchains require authorization to join and Membership Services authenticates, authorizes, and manages the identity of users on the blockchain.

Block Components

- **Smart Contract: Program that runs on the blockchain**
  The original blockchains were designed to simply allow financial transactions to be performed and stored in the historical ledger, and had limited configurability. Since then, blockchains have evolved so that some have become fully functional distributed computers. Smart contracts are programs that run on the blockchain. Users can interact with smart contracts in a similar way that they interact with programs on a standard computer.
- **Wallet: Stores users credentials**
  In blockchain, the user's wallet stores their credentials and tracks digital assets associated with the user's address. The wallet tracks user credentials and any other information that may be associated with their account.
- **Events: Notifications of updates and actions on the blockchain**
  The blockchain’s ledger and the state of the peer network are updated by events. Examples of events include the creation and dispersion of a new transaction across the peer network and the addition of a new block to the blockchain. Events may also include notifications from smart contracts on blockchains that support such contracts.

Block Components

- **Systems Management: Component creation, modification, and monitoring**
  The blockchain is designed to be a long-lived system in a field that is constantly evolving. Systems management provides the capability of creating, modifying, and monitoring blockchain components to meet the needs of its users.
- **Systems Integration: Integration of blockchain with external systems**
  As blockchain has evolved and increased in functionality, it has become more common to integrate blockchains with other external systems, commonly through the use of smart contracts. While this is not a specific component of the blockchain, systems integration is included to acknowledge this capability.



Block Chain Actors

Link to Png file

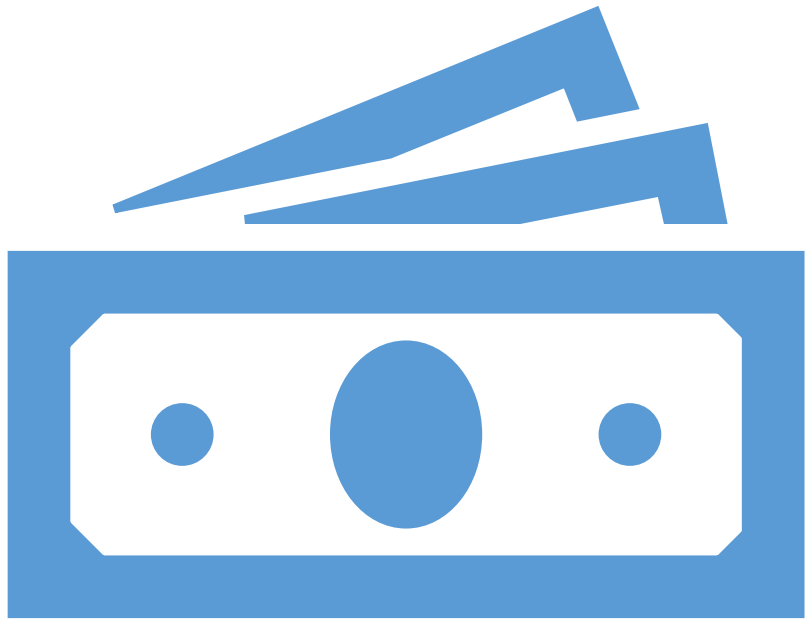
Comparison ETH vs Bitcoin

Comparison	Ethereum	Bitcoin
Founder	Vitalik Buterin	Satoshi Nakamoto
Release date	30th July 2015	9th Jan 2009
Release method	Presale	Genesis Block mined
Blockchain	Proof Of Work (Planning the switch to POS)	Proof of Work
Usage	Smart Contract Digital Currency	Digital Currency
Cryptocurrency used	Ether	Bitcoin
Algorithm used	Ethash	SHA - 256
Blocks Time	12-14 seconds	10 minutes
Mining	GPU	ASIC miners
Scalable	Yes	Not as of now.

Warren Buffet

- “Cryptocurrencies basically have no value and they don't produce anything… In terms of value: zero,” **Buffett** had told CNBC last year. “I don't have any **cryptocurrency** and I never will,” he had said. In 2019 as well, **Buffett** had called **bitcoin** a 'gambling device’

- But that’s not all ….



Bitcoin Wallets

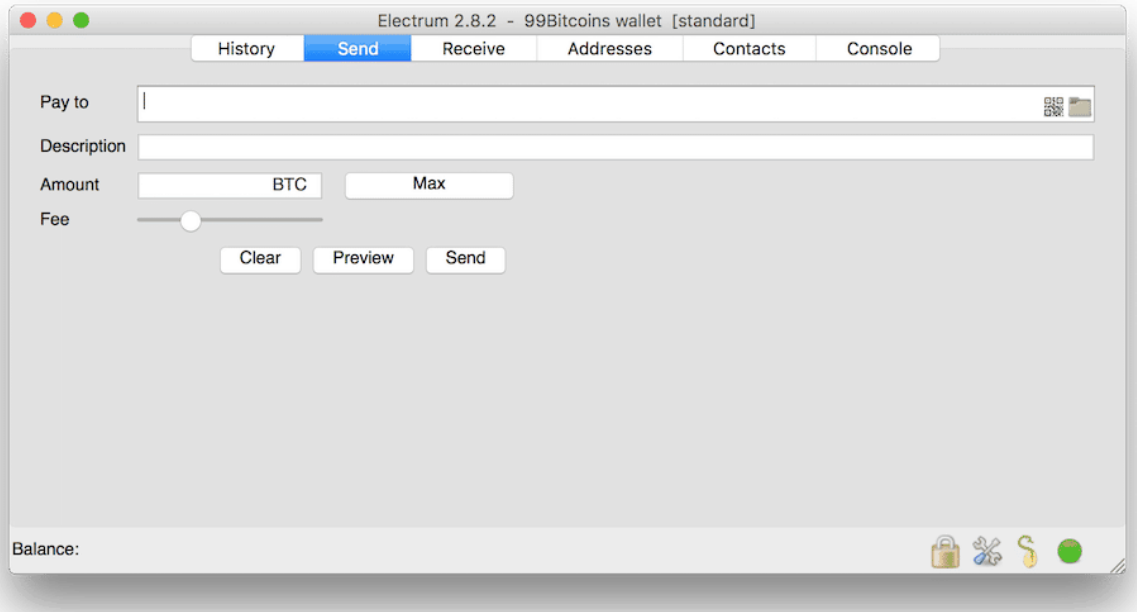
BitCoin Wallets

- Bitcoin wallets are one of the most actively developed applications in the bitcoin ecosystem.
- There is intense competition and while a new wallet is probably being developed right now, several wallets from last year are no longer actively maintained.
- Many wallets focus on specific platforms or specific uses, and some are more suitable for beginners while others are filled with features for advanced users

Wallets

Desktop Wallet

- A desktop wallet was the first type of bitcoin wallet created as a reference implementation and many users run desktop wallets for the features, autonomy and control they offer. Running on general-use operating systems such as Windows and Mac OS has certain security disadvantages however, as these platforms are often insecure and poorly configured.



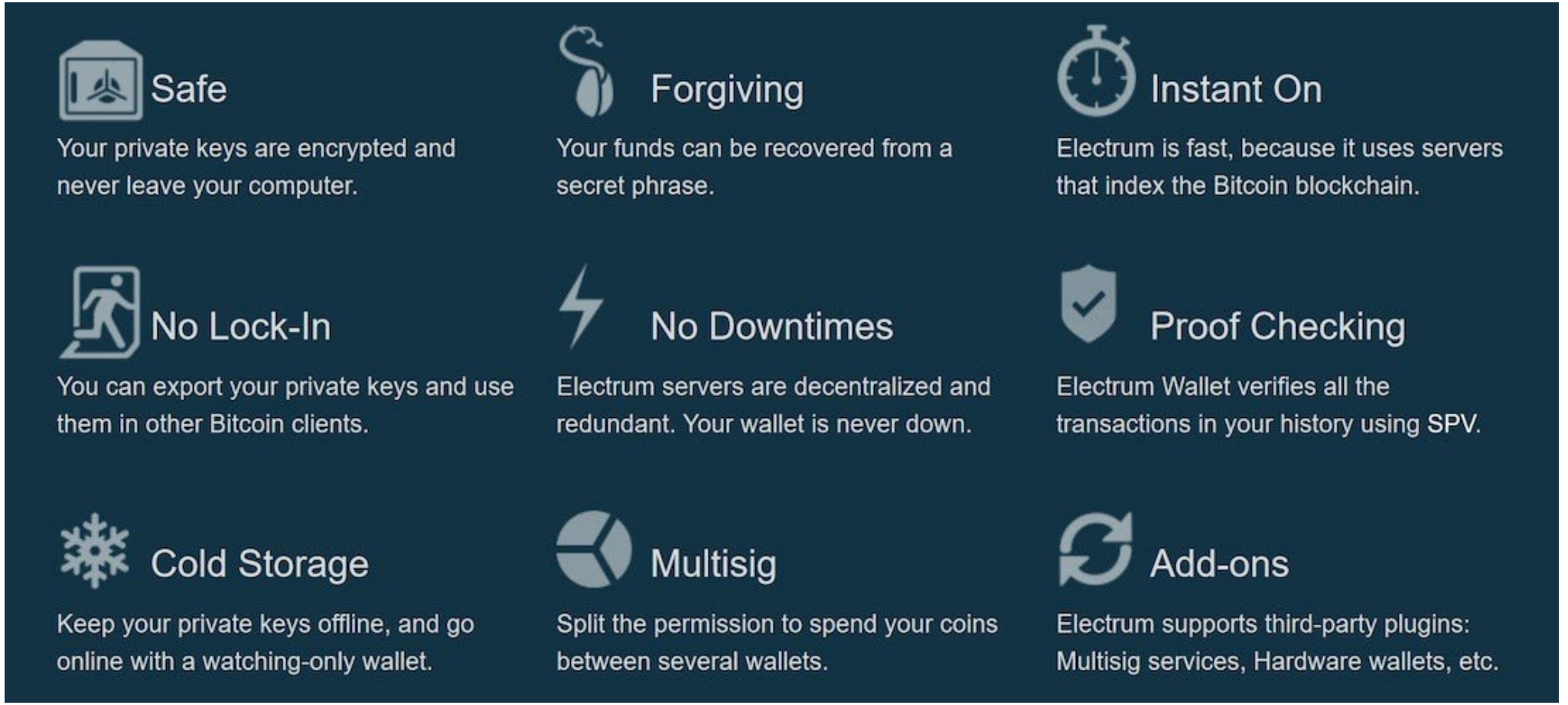
Desktop Wallets

- Popular Desktop wallets are Bitcoin Core, Bitcoin Knots, mSIGNA, Armory, etc.

Electrum desktop wallet

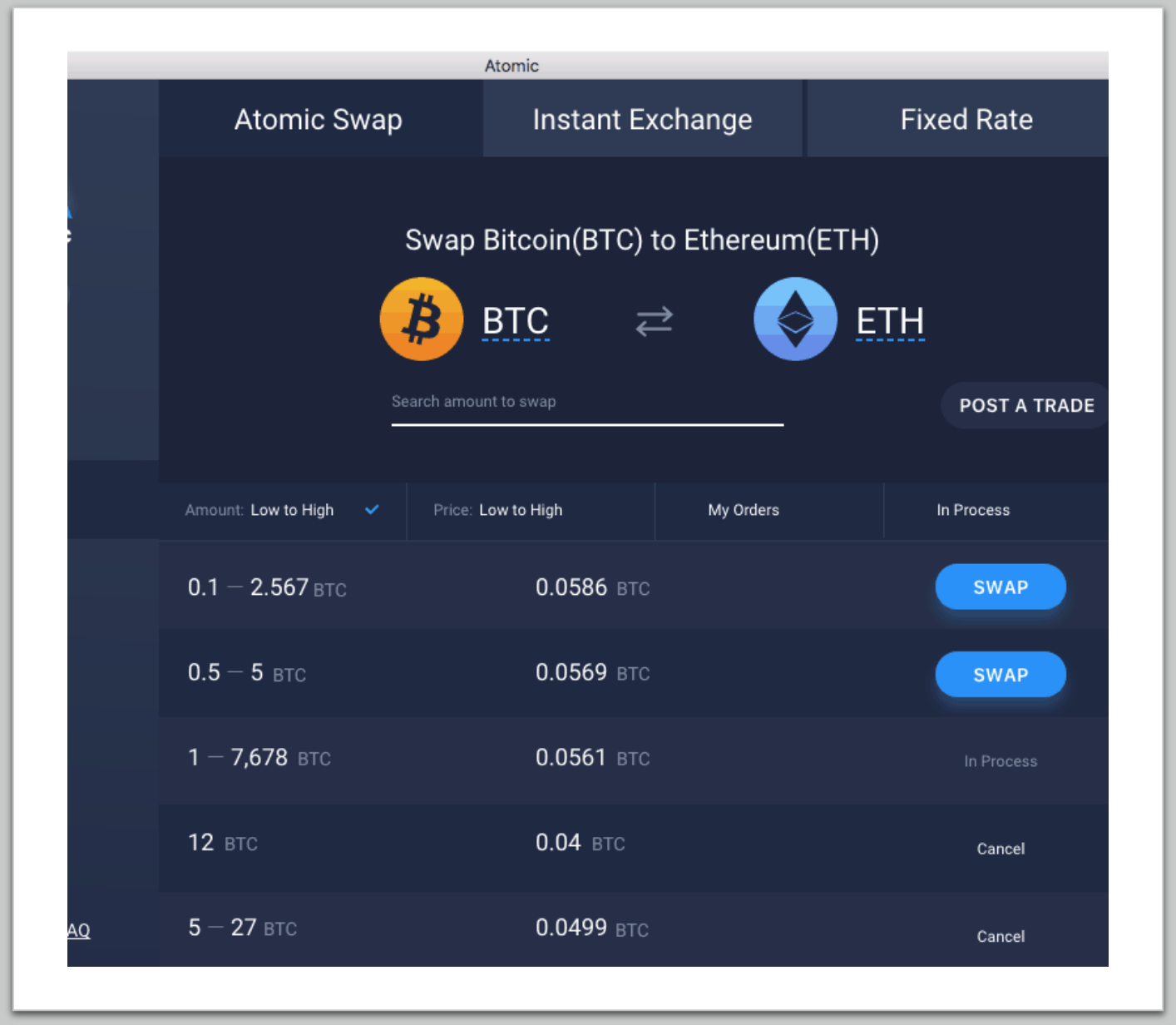
- Electrum is one of the most robust, effective and secure desktop wallets out there.
- Also, it’s open source, meaning many people have taken part in reviewing and composing the code. This reduces the chance of malicious code inside the software to practically zero.
- In times when the Bitcoin network is “crowded” and transaction fees can skyrocket, Electrum is one of the few wallets that allows you to replace the fee you’ve set to an already broadcasted transaction.
- This feature is very handy when you can’t get your transaction to confirm.
- Additional features include address tagging, fee adjustments, encrypting your wallet and signing/verifying messages

Electrum Wallet Benefits



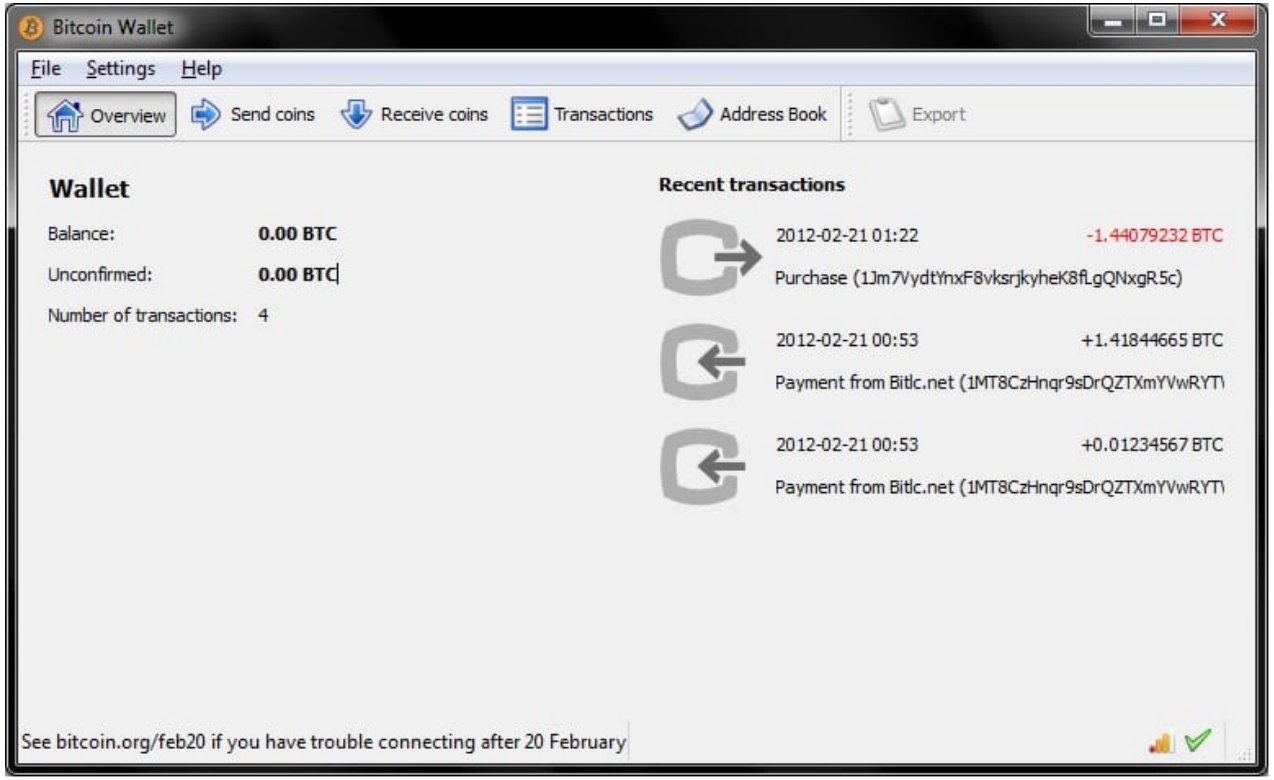
Atomic Wallet – The Multi-currency Option

- If you're looking for an easy to use desktop wallet to store not only Bitcoin you can take a look at Atomic Wallet. Atomic Wallet is a multi-currency wallet that allows you to store up to 500 different coins and tokens in a single interface.
- The wallet also allows you to use Atomic Swaps in order to exchange between certain cryptocurrencies directly from within the wallet without the need for an exchange



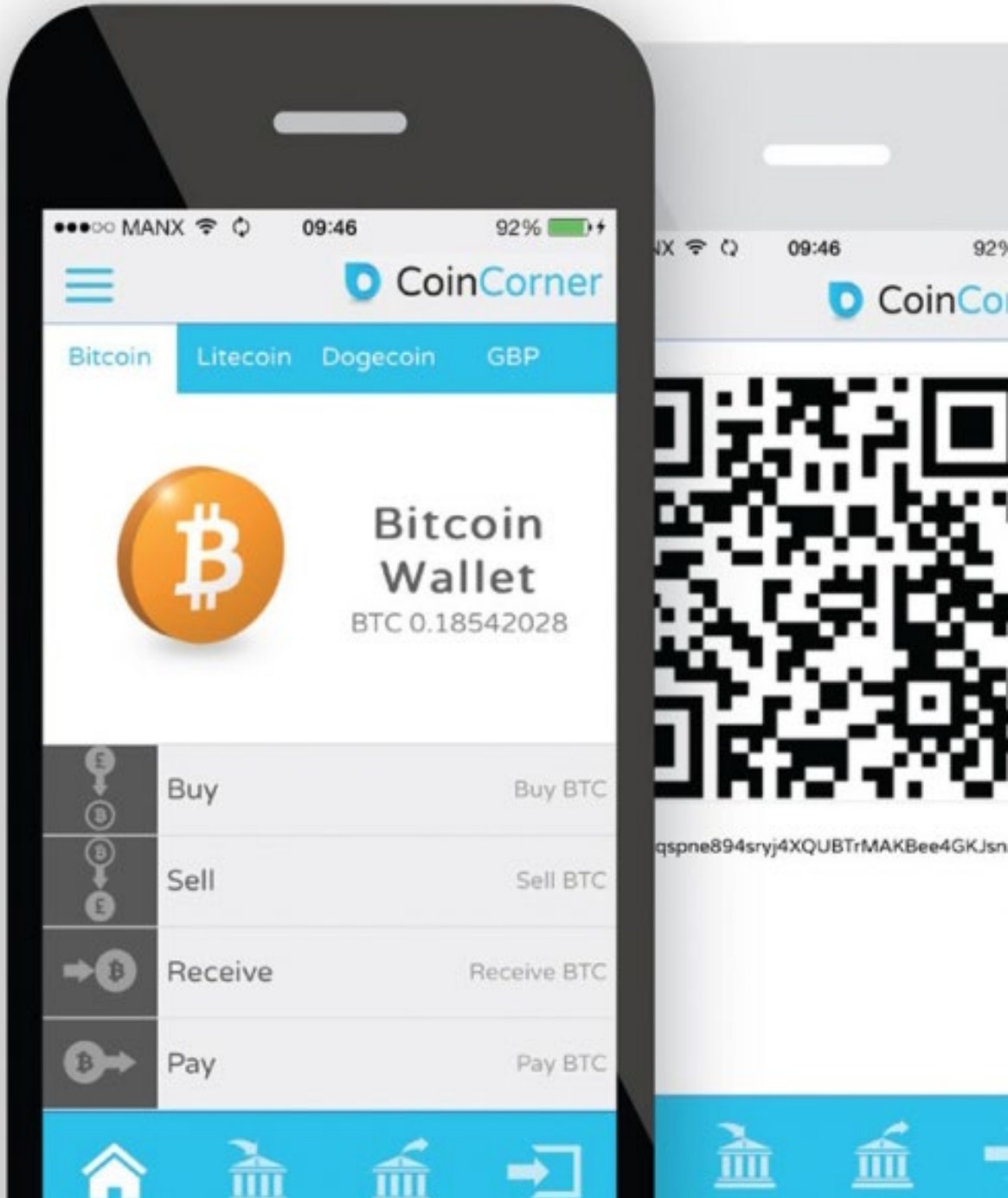
Bitcoin Core – A full Bitcoin node

- **All of the wallets I've covered so far are known as SPV wallets or lite wallets. This means that they don't have a full copy of the blockchain in order to verify transactions – they rely on other computers on the network to give them transaction information.**
- **Bitcoin Core is a full node Bitcoin wallet. This means that once you download the wallet, you will also download the whole blockchain to your computer.**
- **This can get really messy as the blockchain's size is a few hundred Gigabytes and can take some time to download.**
- **However, once the Blockchain is downloaded you can start independently verifying transactions on the network. You no longer need to trust anyone else in the system.**



Mobile Wallet

- A mobile wallet is the most common type of bitcoin wallet.
- Running on smartphone operating systems such as Apple iOS and Android, these wallets are often a great choice for new users.
- Many are designed for simplicity and ease-of-use, but there are also fully-featured mobile wallets for power users.



Mobile Wallets

- Popular Mobile wallets are Bitpay, BTC.com, Edge, Electrum, Mycelium, Bitcoin Wallet, etc.

Web Wallet

- Web wallets are accessed through a web browser and store the user's wallet on a server owned by a third party.
- This is similar to webmail in that it relies entirely on a third-party server.
- Some of these services operate using client-side code running in the user's browser, which keeps control of the bitcoin keys in the hands of the user.
- Most however present a compromise by taking control of the bitcoin keys from users in exchange for ease-of-use. It is inadvisable to store large amounts of bitcoin on third-party systems.
- You access it through a web browser or internet connected app. The private key for the coins (which is like the password to the wallet) is either held by a custodian (the person who owns the web wallet site) or it is encrypted behind a password of your choosing.
- Popular web wallets are Guarda, Coinbase, GreenAddress, Binance, etc.

Hardware Wallet

- **Hardware wallets are devices that operate a secure self-contained bitcoin wallet on special-purpose hardware.**
- **They are operated via USB with a desktop web browser or via near-field-communication (NFC) on a mobile device.**
- **By handling all bitcoin-related operations on the specialized hardware, these wallets are considered very secure and suitable for storing large amounts of bitcoin.**

Hardware Wallets

- Popular hardware wallets are BitBox, Keepkey, Trezor, Ledger Nano S, etc.

Paper Wallet

- The keys controlling bitcoin can also be printed for long term storage.
- These are known as paper wallets even though other materials (wood, metal, e.t.c.) can be used.
- Paper wallets offer a low-tech but highly secure means of storing bitcoin long term.
- Offline storage is also often referred to as *cold storage*.

Wallet Clients

- Another way to categorize bitcoin wallets is by their degree of autonomy and how they interact with the bitcoin network

- https://www.g2.com/categories/cryptocurrency-wallets

Full node clients

- A full client, or “full node,” is a client that stores the entire history of bitcoin transactions (every transaction by every user, ever), manages the users’ wallets, and can initiate transactions directly on the bitcoin network.
- A full node handles all aspects of the protocol and can independently validate the entire blockchain and any transaction.
- A full-node client consumes substantial computer resources (e.g. more than 60GB of disk, 2GB of RAM) but offers complete autonomy and independent transaction verification.

A full-node is a mining node.

- **A node:**
- Needs a complete, validated copy of the blockchain so that it can mine on the correct chain, earning bitcoins and contributing to the security of the network.
- Chooses the transactions it includes in its blocks.
- Relies on other mining nodes to accept its blocks as valid. Rejects any invalid blocks.
- Won’t update its software unless it is sure it will generate blocks valid to the rest of the network
- Will likely service requests for blockchain data and SPV clients (Simplified payment verification)

Satoshi's Vision

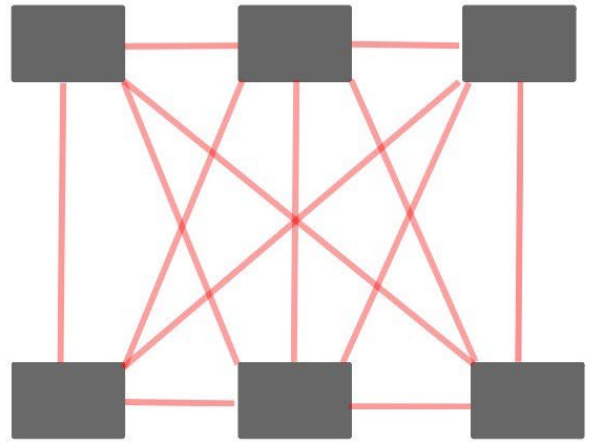
Nodes

Full-Nodes

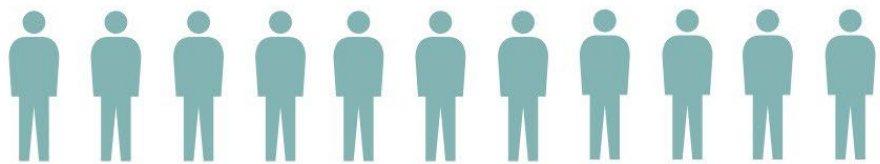
&

SPV-Nodes

Mining-Nodes (1000s)

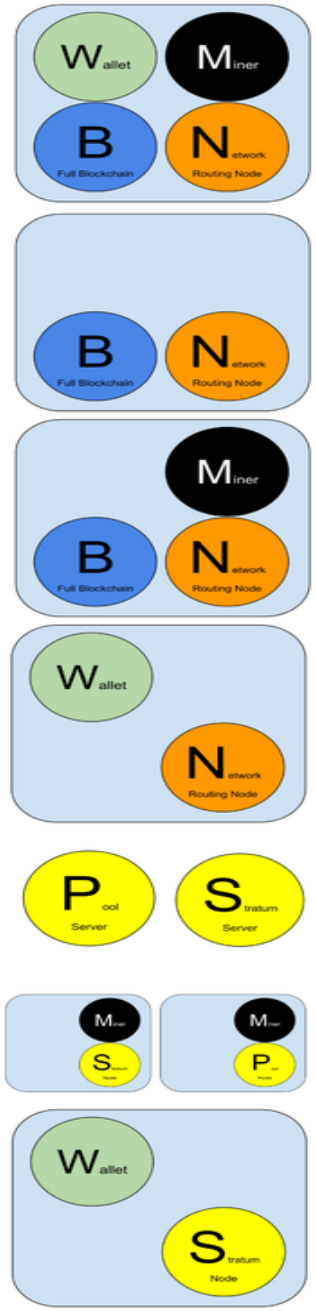


SPV Nodes (10,000s)



The mining-nodes provide fraud proofs to SPV users

Various types of nodes in Bitcoin / Block Chain



Reference Client (Bitcoin Core)

Contains a Wallet, Miner, full Blockchain database, and Network routing node on the bitcoin P2P network.

Full Block Chain Node

Contains a full Blockchain database, and Network routing node on the bitcoin P2P network.

Solo Miner

Contains a mining function with a full copy of the blockchain and a bitcoin P2P network routing node.

Lightweight (SPV) wallet

Contains a Wallet and a Network node on the bitcoin P2P protocol, without a blockchain.

Pool Protocol Servers

Gateway routers connecting the bitcoin P2P network to nodes running other protocols such as pool mining nodes or Stratum nodes.

Mining Nodes

Contain a mining function, without a blockchain, with the Stratum protocol node (S) or other pool (P) mining protocol node.

Lightweight (SPV) Stratum wallet

Contains a Wallet and a Network node on the Stratum protocol, without a blockchain.

Lightweight client

- A lightweight client, also known as a simple-payment-verification (SPV) client connects to bitcoin full nodes (mentioned above) for access to the bitcoin transaction information, but stores the user wallet locally and independently creates, validates and transmits transactions.
- Lightweight clients interact directly with the bitcoin network, without an intermediary.

Third-Party API client

- A third-party API client is one that interacts with bitcoin through a third-party system of application programming interfaces (APIs), rather than by connecting to the bitcoin network directly.
- The wallet may be stored by the user or by the third-party servers, but all transactions go through a third party.

Wallet summary

- Combining the categorizations below, many bitcoin wallets fall into a few groups, with the three most common being Desktop Full Client, Mobile Lightweight Wallet and Web Third-Party Wallet.
- The lines between different categories are often blurry, as many wallets run on multiple platforms and can interact with the network in different ways.

Finding the Current Price of Bitcoin

- **Bitcoin, like most other currencies, has a *floating exchange rate*. That means that the value of bitcoin vis-a-vis any other currency fluctuates according to supply and demand in the various markets where it is traded**
- **There are hundreds of applications and websites that can provide the current market rate. Here are some of the most popular:**
- ***Bitcoin Average***
- **A site that provides a simple view of the volume-weighted-average for each currency**
- ***Bitcoin Charts***
- **A market data listing service that shows the market rate of bitcoin across many exchanges around the globe, denominated in different local currencies**
- ***ZeroBlock***
- **A free Android and iOS application that can display a bitcoin price from different exchanges**

Wallet Selection Criteria

- **To select a reliable Bitcoin wallet, one should judge it based on the following criteria:**

- **Hot/Cold Wallet:** Whether a wallet is a hot(Online storage) or cold(offline storage).
- **Control private keys:** A wallet where you own and control your keys.
- **Backup & security features:** Here, you can seed backup keys and pin codes.
- **Developer community:** It is an active development community for maintenance.
- **Compatibility:** It can be compatible with different operating systems.
- **HD Wallet:** It is a wallet that generates new addresses itself.
- **KYC:** A wallet that doesn't require KYC.