TIBA

# Lecture 2
# Blockchain 1.0 Bitcoin

By Samuel Tang, TIBA

Fall 2020 @ Tsinghua University

TIBA

# Goal: How does Bitcoin work?

TIBA

## Content

- Bitcoin
  - Identity
  - Transaction
  - Network
  - Blockchain
- Value

TIBA

TIBA

# Bitcoin Identity

## Random strings as identity

- **Private key**
  - **your password – keep it safe!!**
  - a randomly generated 256-bit number
  - 256 bits in hexadecimal is 32 bytes
  - or 64 characters in the range 0-9 or A-F
    - 979D57805279E6B5B2596918EEE1FB20D1FE0E832C4C261FF821D74DA9427027
  - or WIF compress to 52 characters in base58
    - L2JRtP5NMRXoCgeHuxsrWqDnQVpmHcmWDYRQeFgbT8hqnAq7pYe1

Source: https://en.bitcoin.it/wiki/Private_key

TIBA

# Bitcoin Identity

Random strings as identity

- **Public key**
  - **your username**
  - generated from private key using ECDSA (Elliptic Curve Digital Signature Algorithm)
  - cannot find its private key given a public key (cannot find the password given a username)
  - 512 bits + some formatting bits, or 65 bytes
  - compressed to 257 bits or 33 bytes
  - 66 characters in the range 0-9 or A-F
    - 03efde69707965d902643449e0e2029d3b44333c29b9711e5f385fa531c0ea7d33

Source: https://bitcoin.stackexchange.com/questions/2013/why-does-the-length-of-a-bitcoin-key-vary

TIBA

# Bitcoin Identity

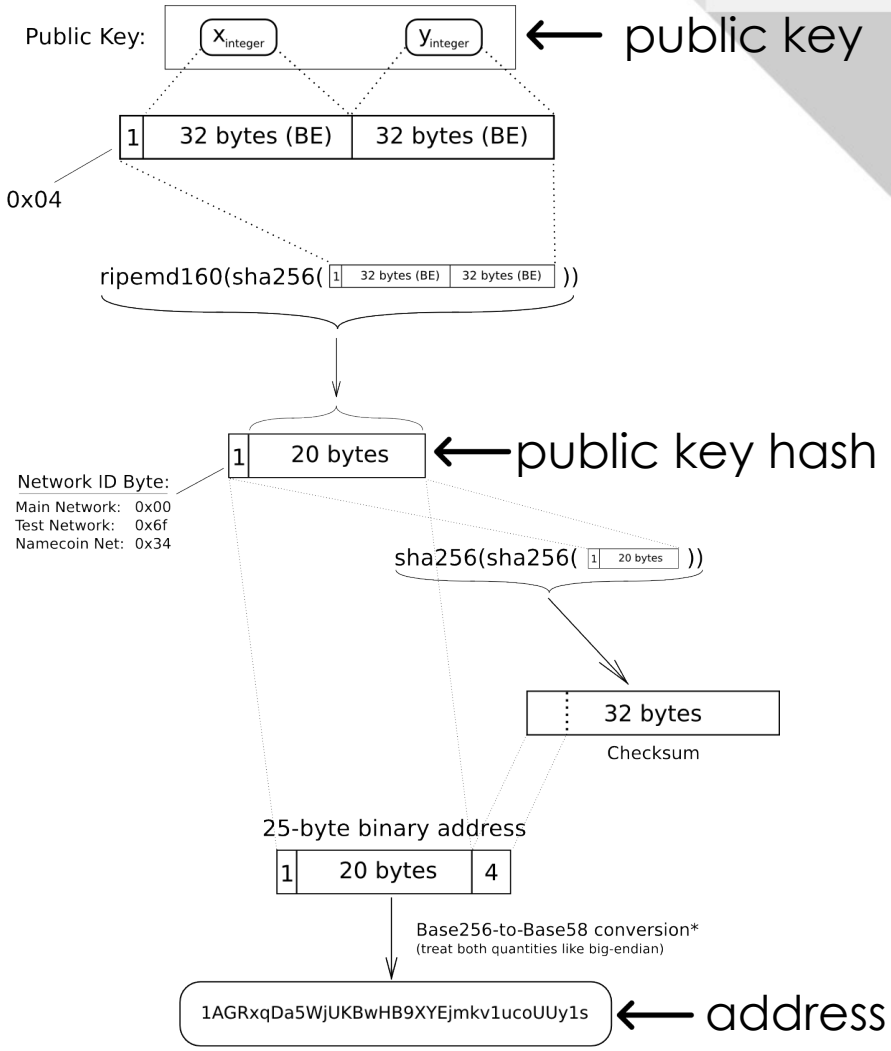
## Random strings as identity

- **Address**
  - **your user id**
  - generated from public key

(public key -> public key hash -> address)

- 20 bytes (160 bits)
- 1FxyjVSqEaVtPcSv9z4qQoHGCdoFtjmfyp

Elliptic-Curve Public Key to BTC Address conversion




*In a standard base conversion, the 0x00 byte on the left would be irrelevant (like writing '052' instead of just '52'), but in the BTC network the left-most zero chars are carried through the conversion. So for every 0x00 byte on the left end of the binary address, we will attach one '1' character to the Base58 address. This is why main-network addresses all start with '1'

etotheipi@gmail.com / 1Gffm7LKXcNFPrtxy6yF4JBoe5rVka4sn1

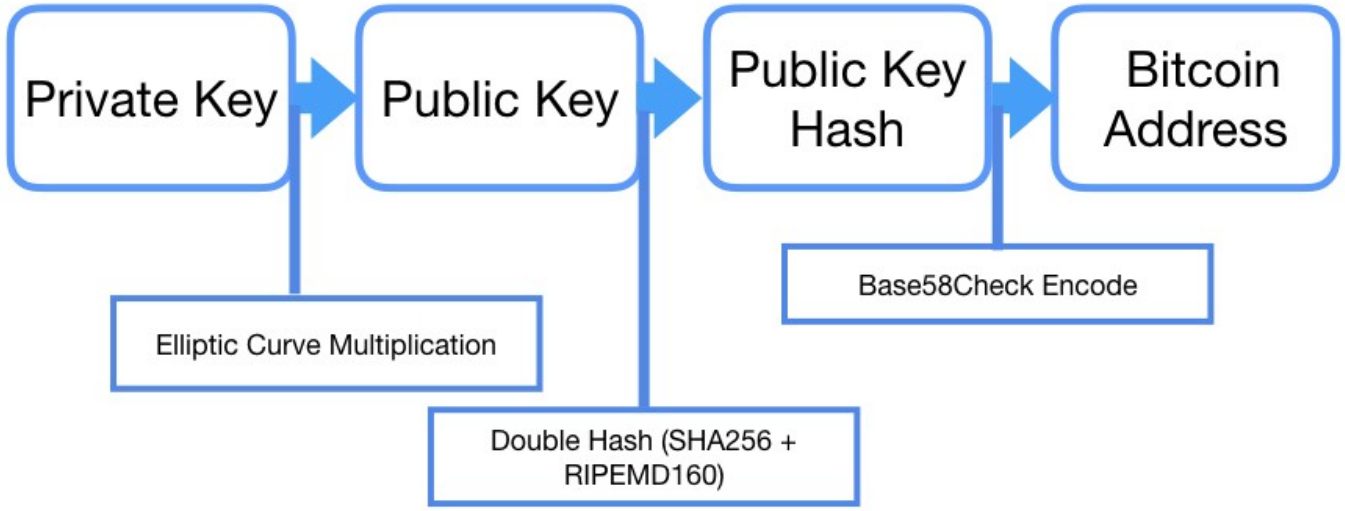
Source: https://en.bitcoin.it/wiki/Technical_background_of_version_1_Bitcoin_addresses

TIBA

# Bitcoin Identity

Random strings as identity

- Private key – password
  - to redeem
- Public key – username
  - to receive
- Address – user id
  - to be found




*wise advice: use a new address for each transaction or generate a new key pair each time

Source: https://medium.com/coinmonks/what-is-a-bitcoin-address-6c822c857004

TIBA

# Bitcoin Identity

## Random strings as identity

- What if I lose my private key?
- What if someone stole my private key?
- What if someone guesses my private key?
- OR What if someone randomly generated the same private key as mine?

TIBA

# Bitcoin Identity

## Random strings as identity

- What if I lose my private key?
  - Your bitcoin is gone forever!
- What if someone stole my private key?
  - They have complete access to your bitcoin!
- What if someone guesses my private key?
- OR What if someone randomly generated the same private key as mine?
  - Mathematically impossible :)

TIBA

# Bitcoin Identity

## Random strings as identity

- Number of address possible:
  - $2^{160}$(1,461,501,637,330,902,918,203,684,832,716,283,019,655,932,542,976)unique addresses
- In comparison, estimated $2^{63}$ grains of sand on planet Earth
- ~7.5 billion population (2017)
  - each person can have ~$2^{127}$ addresses

Source: UCBerkeley Blockchain at Berkeley Fundamental Decal

# Bitcoin Identity

## Keys Storage

- **Wallet** - holds (and generates) the private key(s) that allow you to access your bitcoin address
- hot storage – online
  - mobile wallet
  - web wallet
- cold storage – offline
  - paper wallet
  - hardware wallet
  - brain wallet

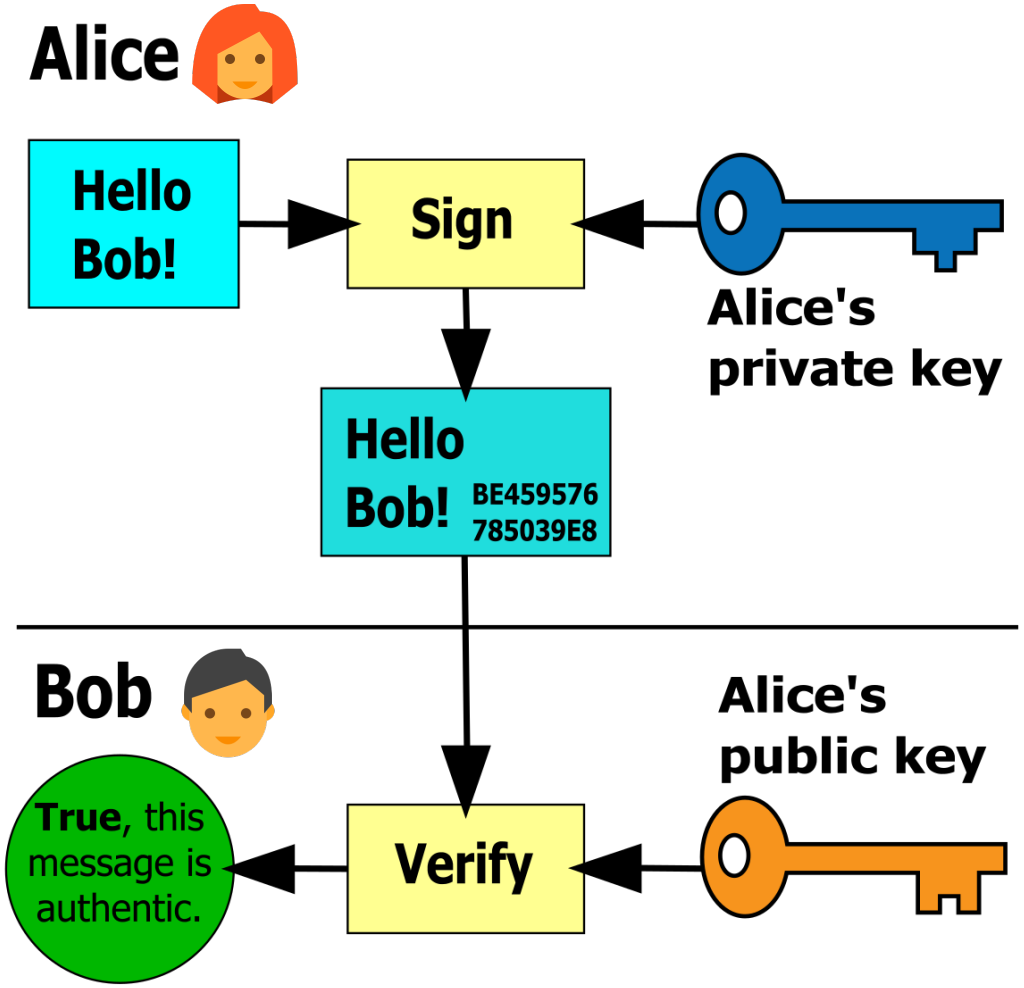

paper wallet

Source: https://www.coindesk.com/learn/bitcoin-101/how-to-store-your-bitcoins; https://www.bitaddress.org/

# Bitcoin Identity

## Proving Identity

- **Digital Signature**
  - to generate:
    private key + message
  - to verify:
    public key + message + digital signature
  - in **Bitcoin**:
    message == transaction




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

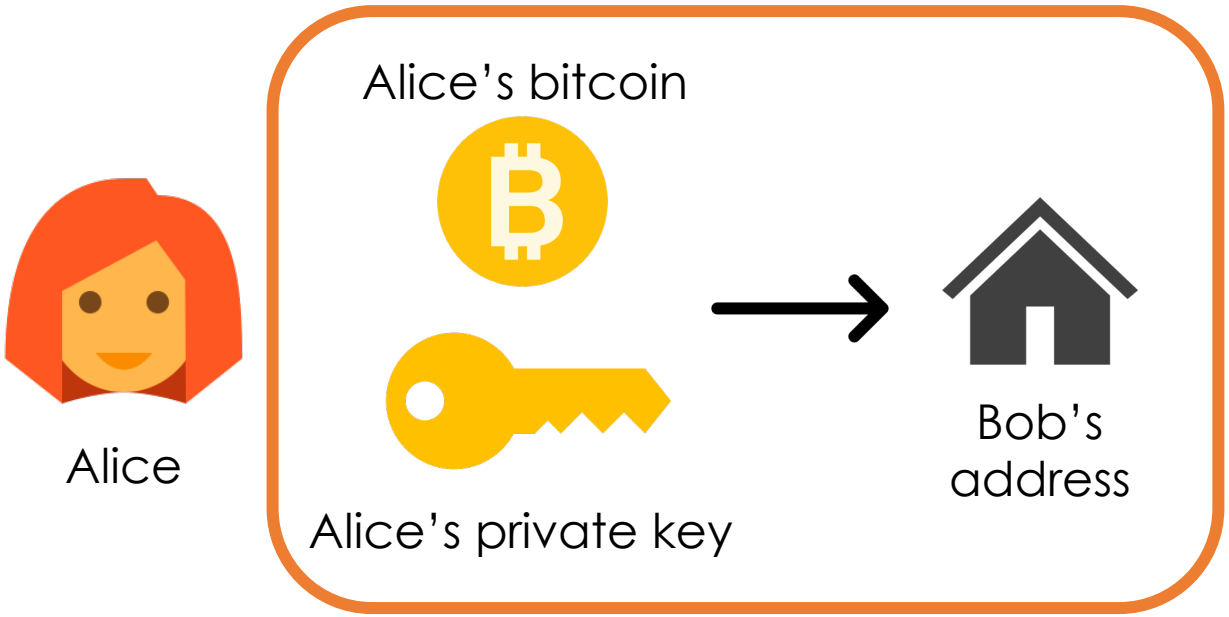
TIBA

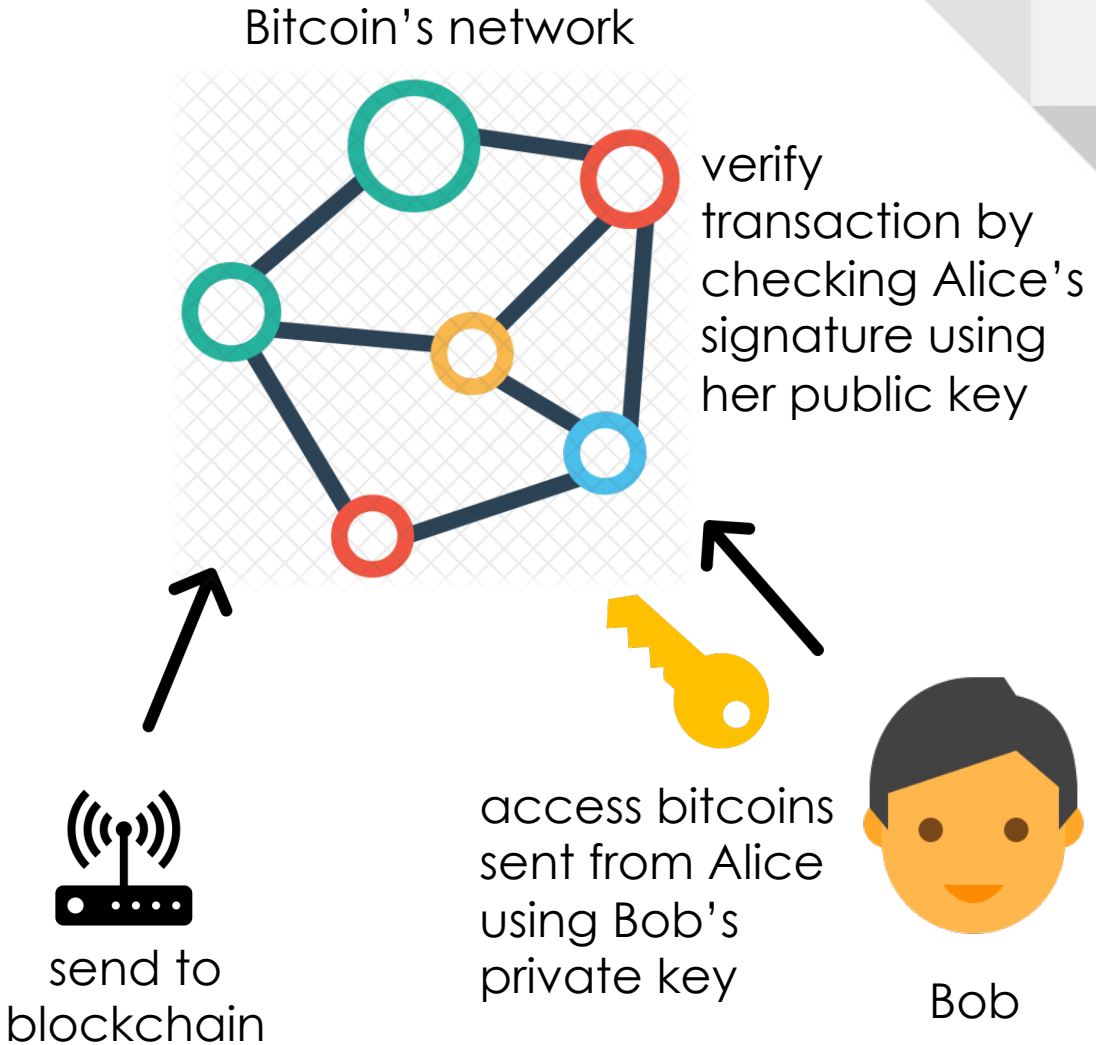
# Bitcoin Transaction

# Bitcoin Transaction

Example

- Alice sends a transaction to Bob



TIBA

# Bitcoin Transaction

## UTXOs

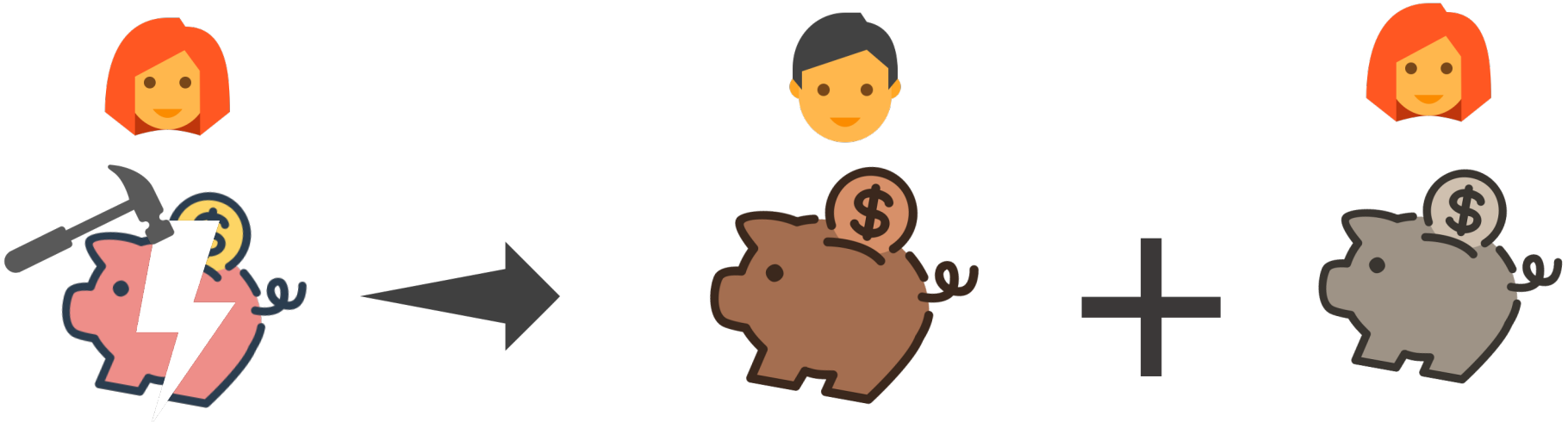
- **Double-spending problem** – spending the same money more than once
  - the ultimate enemy of digital money
- **Bitcoin**'s solution:
  **UTXOs** (Unspent Transaction Outputs)
  - piggy banks (spend all or none)
  - contained data: value(amount) and owner's address
- **Bitcoin** is **NOT** account/balance based

5 BTC
1FxyjVSqEaVtPcSv9z4qQoHGCdoFtjmfyp

# Bitcoin Transaction

## Behind the Scene – Spending UTXO

- example:  Alice sending 3 BTC to Bob



5 BTC
1FxyjVSqEaVtPcSv9z4qQoHGCdoFtjmfyp

3 BTC
1K6yjVBVrUvAU8kHed3eQGZrfAmi3nwncS

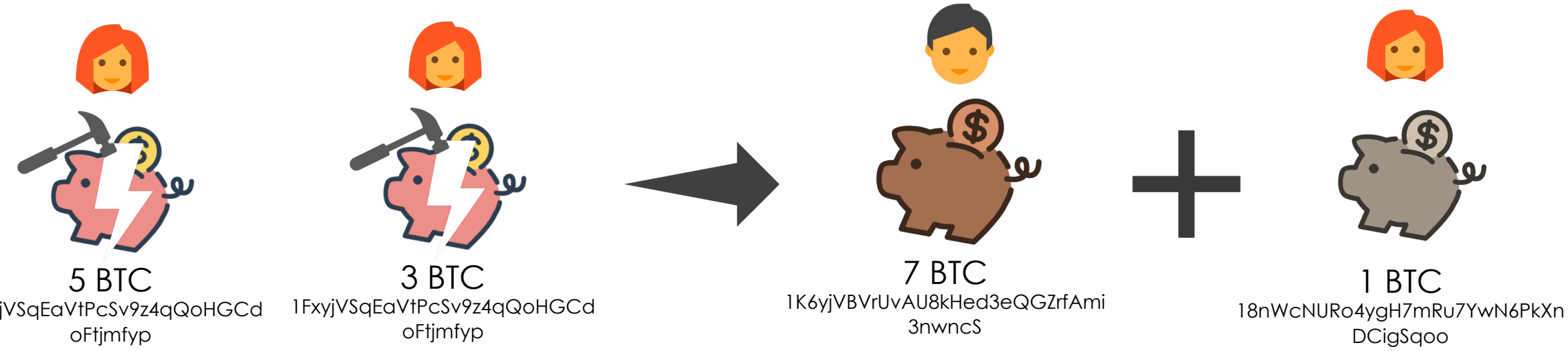
2 BTC
18nWcNURo4ygH7mRu7YwN6PkXnDCigSqoo

TIBA

# Bitcoin Transaction

## Behind the Scene – Spending UTXO

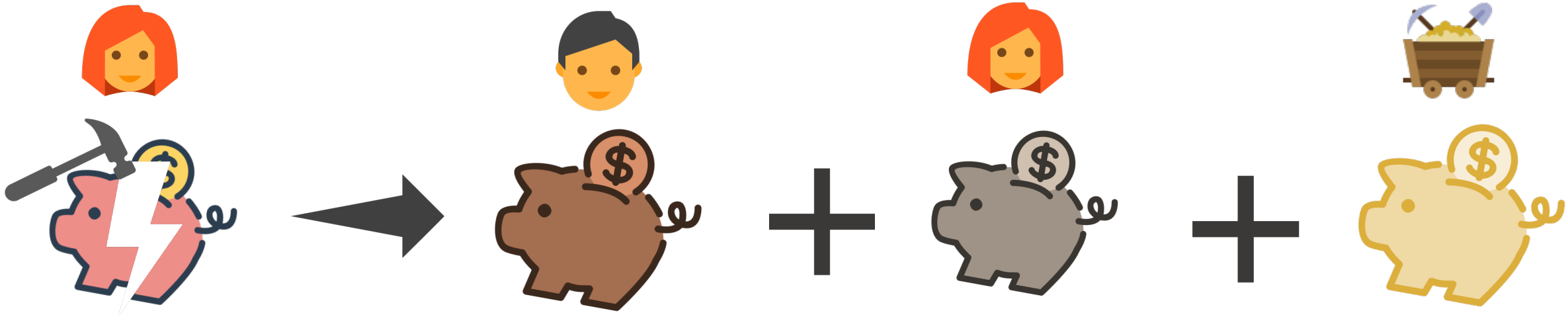
- example:  Alice sending 7 BTC to Bob



# Bitcoin Transaction

## Behind the Scene – Spending UTXO

- example:  Alice sending 3 BTC to Bob with transaction fee



5 BTC
1FxyjVSqEaVtPcSv9z4qQoHGCdoFtjmfyp

3 BTC
1K6yjVBVrUvAU8kHed3eQGZrfAmi3nwncS

1.8 BTC
18nWcNURo4ygH7mRu7YwN6PkXnDCigSqoo

0.2 BTC
Transaction Fee
Miner's address

TIBA

# Bitcoin Transaction

## UTXO Pool

- A memory pool of all current UTXOs
  - used by miners to verify transactions (by checking the money you're spending belongs to you)

UTXO pool

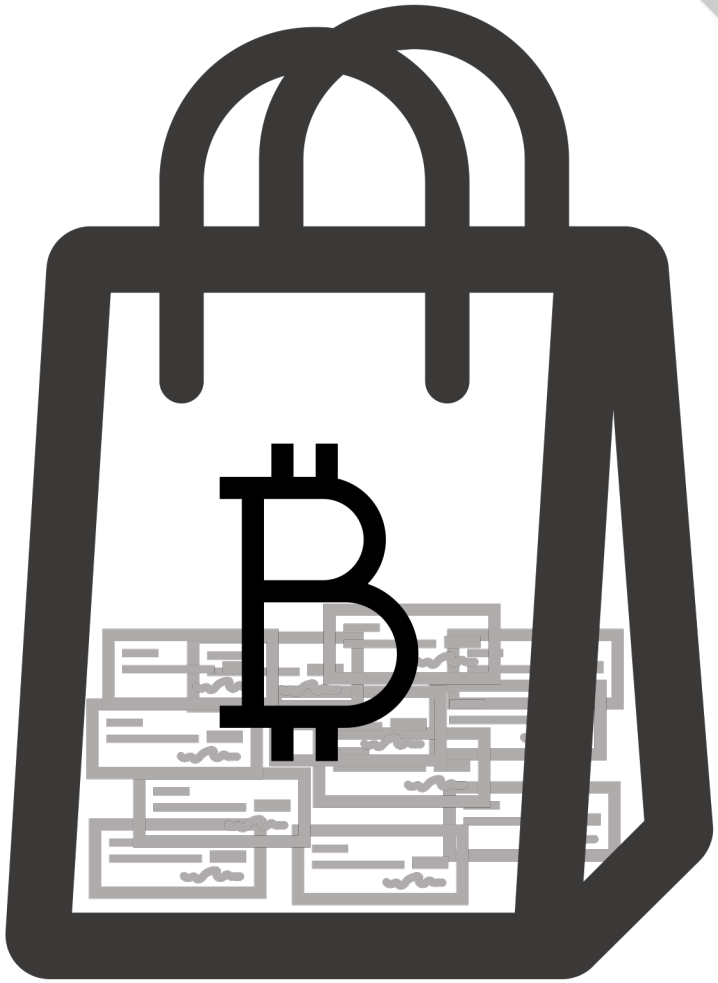
Source: https://thecoinrise.com/how-do-bitcoin-transactions-work/

TIBA

# Bitcoin Transaction

## Transaction Pool

- A memory pool of all current pending transactions
  - used by miners to pick transactions to verify



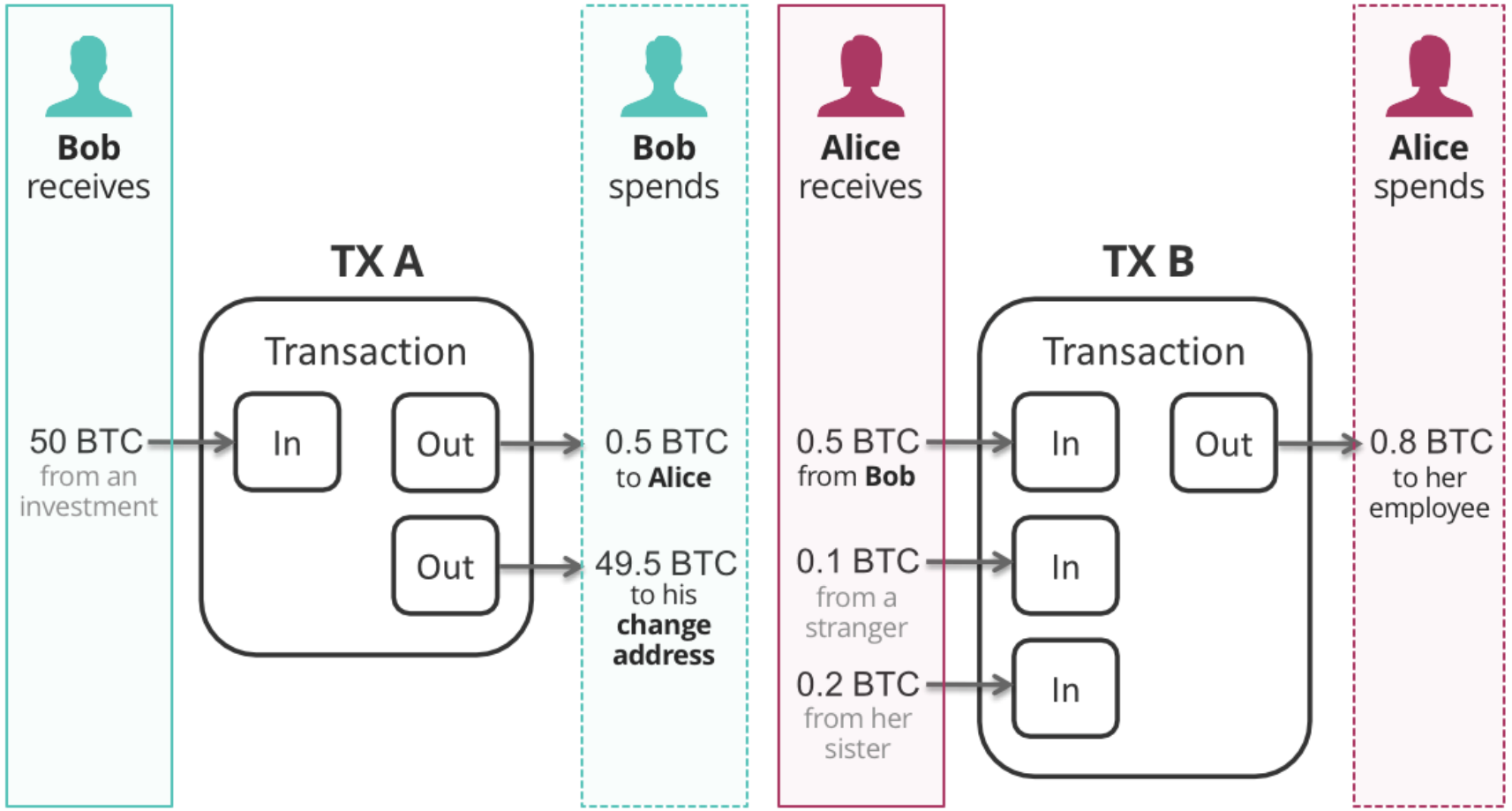
Transaction pool

Source: https://thecoinrise.com/how-do-bitcoin-transactions-work/

TIBA

# Bitcoin Transaction

## Example




Source: https://thecoinrise.com/how-do-bitcoin-transactions-work/

# TIBA Bitcoin Transaction

## Transaction in Details

metadata

input(s)

output(s)


```
{
    "hash":"5a42590fbe0a90ee8e8747244d6c84f0db1a3a24e8f1b95b10c9e050990b8b6b",
    "ver":1,
    "vin_sz":2,
    "vout_sz":1,
    "lock_time":0,
    "size":404,
    "in":[
     {
      "prev_out":{
       "hash":"3be4ac9728a0823cf5e2deb2e86fc0bd2aa503a91d307b42ba76117d79280260",
       "n":0
      },
        "scriptSig":"30440..."
     },
     {
      "prev_out":{
       "hash":"7508e6ab259b4df0fd5147bab0c949d81473db4518f81afc5c3f52f91ff6b34e",
       "n":0
      },
      "scriptSig":"3f3a4ce81...."
     }
    ],
    "out":[
     {
      "value":"10.12287097",
      "scriptPubKey":"OP_DUP OP_HASH160 69e02e18b5705a05dd6b28ed517716c894b3d42e OP_EQUALVERIFY OP_CHECKSIG"
     }
    ]
}
```


Img: Princeton Bitcoin and Cryptocurrency Technologies

TIBA

# Bitcoin Transaction

## Summary

> Transaction Z:
>
> I am [public key matching Bitcoin address Q].
>
> I am spending the Bitcoins paid to me from transactions A, B, and C.
>
> Pay N satoshis to address P and M satoshis to address Q. Whoever mines the block containing this transaction may keep the remainder as a tip.
>
> Signed,
> [Signature with public key mentioned above]

Source: https://www.quora.com/How-does-the-Bitcoin-network-know-what-the-public-key-of-a-given-address-is

TIBA

# Bitcoin Transaction

## Summary

**Simple version**:

If I want to send some of my bitcoin to you, I publish my intention and the nodes scan the entire bitcoin network to validate that I 1) have the bitcoin that I want to send, and 2) haven't already sent it to someone else. Once that information is confirmed, my transaction gets included in a "block" which gets attached to the previous block – hence the term "blockchain." Transactions can't be undone or tampered with, because it would mean re-doing all the blocks that came after.

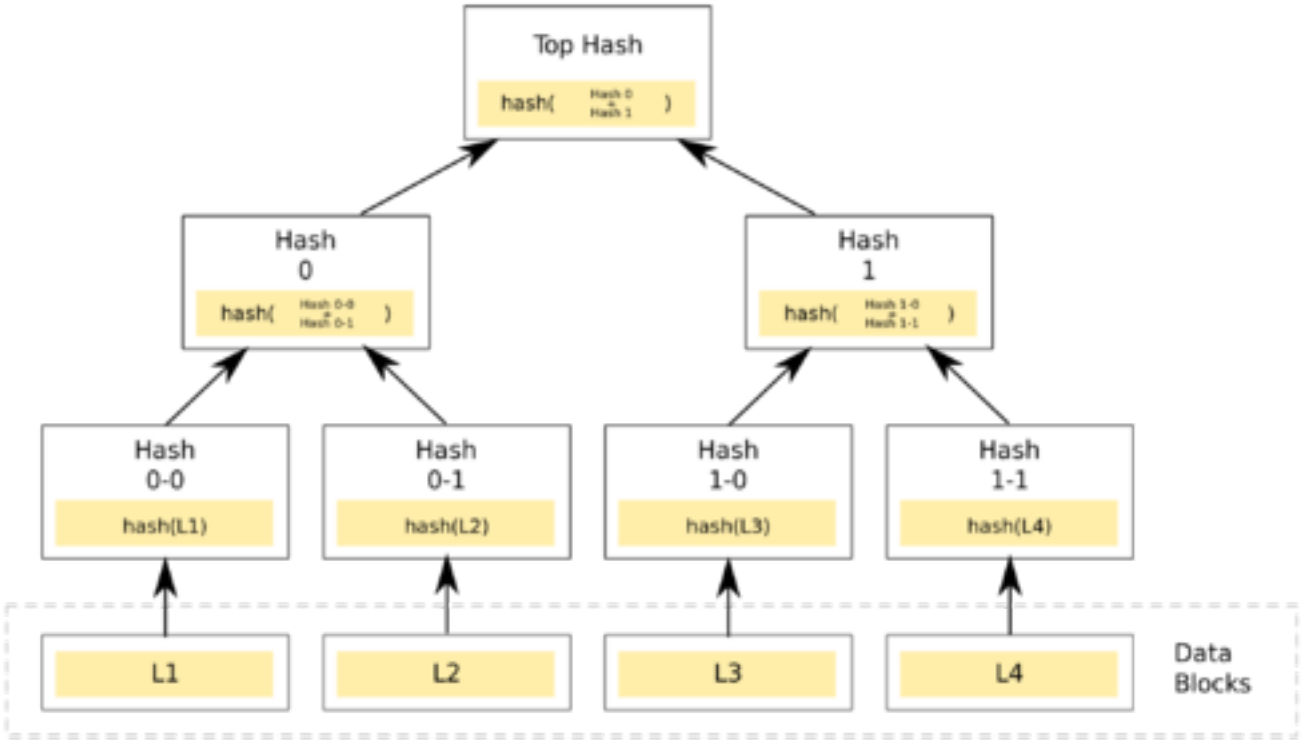
Source: https://www.coindesk.com/learn/bitcoin-101/how-do-bitcoin-transactions-work

TIBA

# Merkle Tree

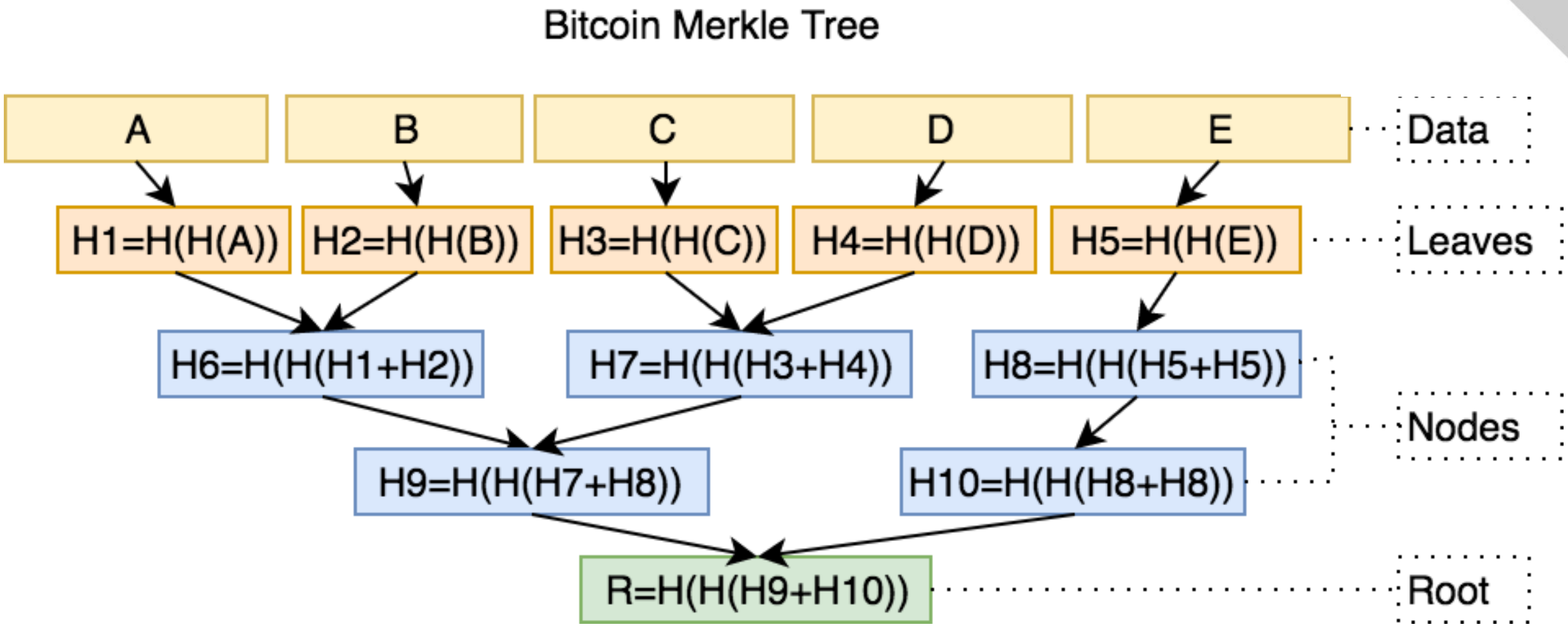
## Storing Transactions

- **Merkle Tree** – a high-efficient data structure for storing transactions
  - each non-leaf node is the hash of its two child nodes
  - Leaf node is transaction data
  - **Merkel Root**
    - a simple way to verify all transactions




Img: https://en.bitcoinwiki.org/wiki/Merkle_tree

# TIBA Merkel Tree




Img: https://www.npmjs.com/package/merkletreejs/v/0.1.6

TIBA

TIBA

Question: Who verify those transactions?

Answer: Miners

TIBA

# Bitcoin Network

## Miners & Mining

- **Miner** – people who do the work of mining
  - in theory, everyone could be a miner
- **Mining** – verifying transactions and put them into a new block, solve a puzzle, then publish this block to the blockchain
- Miners are in a race to compete who can publish a new block onto the blockchain first
- approx. every 10 minutes == a new block

TIBA

# Bitcoin Network

## Proof of Work (PoW) – solving a puzzle

- **Proof of work** – the process of solving a cryptographic puzzle
  - hard to solve, easy to verify
  - the only way to solve is by using brute force method
  - consumes a lot of energy
  - **Bitcoin**:
    - Find a nonce (number only used once) such that the hash of the block results in certain amount of leading zeros
    - able to adjust mining difficulty by changing the number of leading zeros

TIBA

# Bitcoin Network

## Proof of Work (PoW) – example

### Example

Let's say the base string that we are going to do work on is "Hello, world!". Our target is to find a variation of it that SHA-256 hashes to a value smaller than 2^240. We vary the string by adding an integer value to the end called a nonce and incrementing it each time, then interpreting the hash result as a long integer and checking whether it's smaller than the target 2^240. Finding a match for "Hello, world!" takes us 4251 tries.

```
"Hello, world!0" => 1312af178c253f84028d480a6adc1e25e81caa44c749ec81976192e2ec934c64 = 2^252.253458683
"Hello, world!1" => e9afc424b79e4f6ab42d99c81156d3a17228d6e1eef4139be78e948a9332a7d8 = 2^255.868431117
"Hello, world!2" => ae37343a357a8297591625e7134cbea22f5928be8ca2a32aa475cf05fd4266b7 = 2^255.444730341
...
"Hello, world!4248" => 6e110d98b388e77e9c6f042ac6b497cec46660deef75a55ebc7cfdf65cc0b965 = 2^254.782233115
"Hello, world!4249" => c004190b822f1669cac8dc37e761cb73652e7832fb814565702245cf26ebb9e6 = 2^255.585082774
"Hello, world!4250" => 0000c3af42fc31103f1fdc0151fa747ff87349a4714df7cc52ea464e12dcd4e9 = 2^239.61238653
```

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

Question: Why would people mine bitcoin?

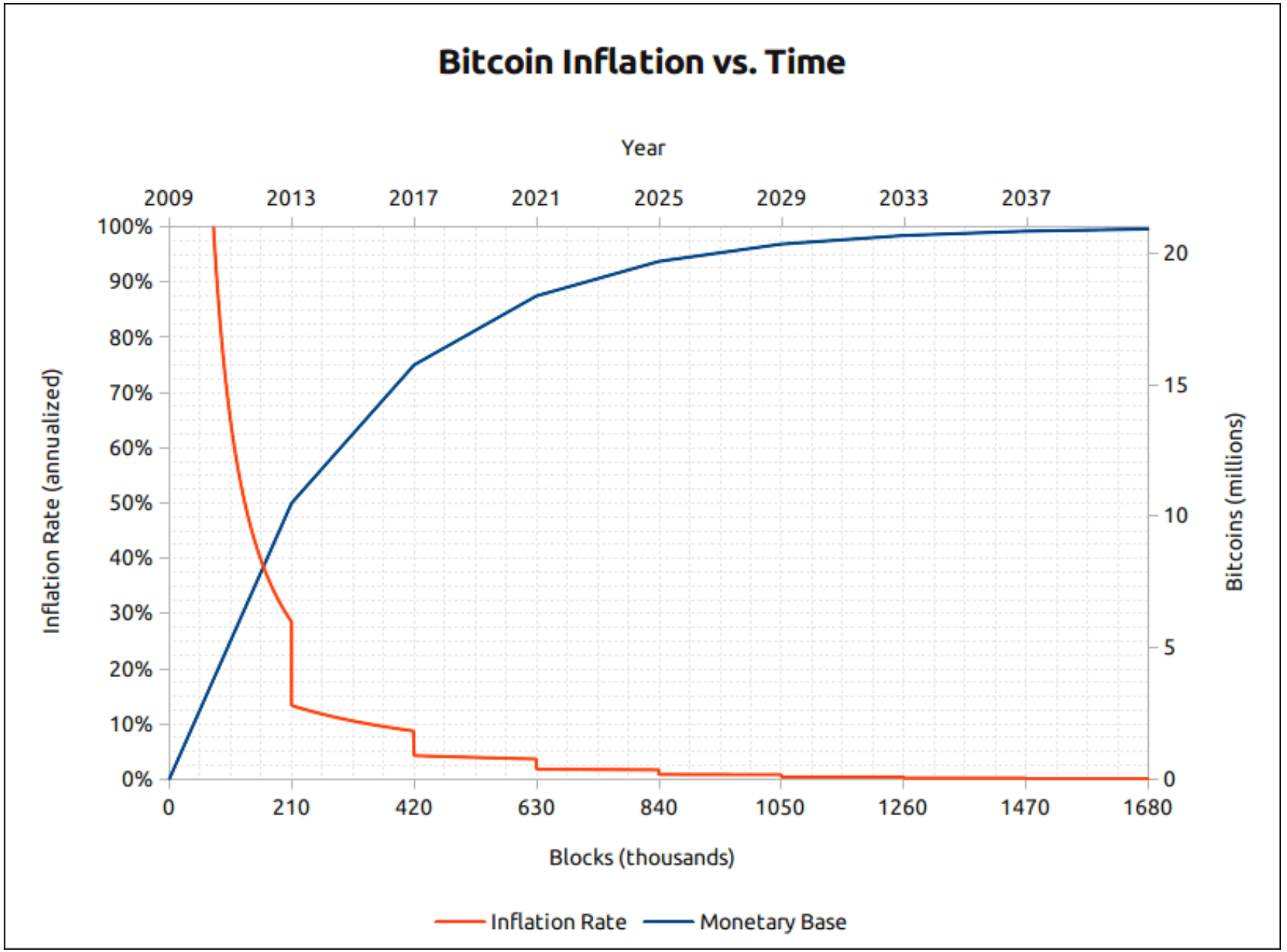
Answer: Incentive!

TIBA

# Bitcoin Network

## Mining Incentive

- **Mining incentive**
  - the only way bitcoins are created
  - sometimes call the "coinbase" transaction
  - the reward (in bitcoins) that miners get when they publish a new block
    - Bitcoin amount halving every 210,000 blocks ( ~ four years)
    - 2008/2009 -> 50 bitcoins
    - 2012 -> 25 bitcoins
    - 2016 -> 12.5 bitcoins
    - 2020 -> 6.25 bitcoins (May 11)
    - …
  - there're only 21 million bitcoins that can be mined/created
  - last bitcoin will be mined in 2140




Source: https://www.bitcoinblockhalf.com/

TIBA

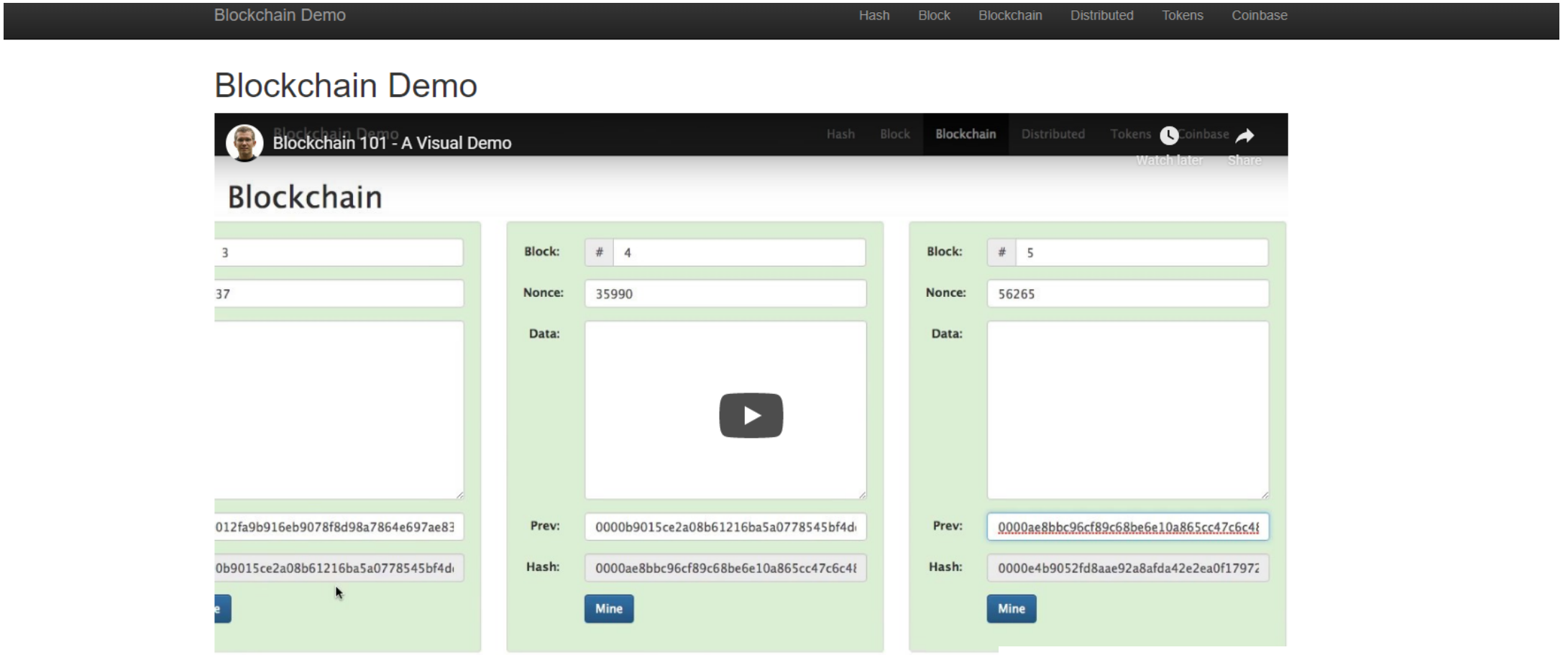
# Bitcoin Network

## Mining

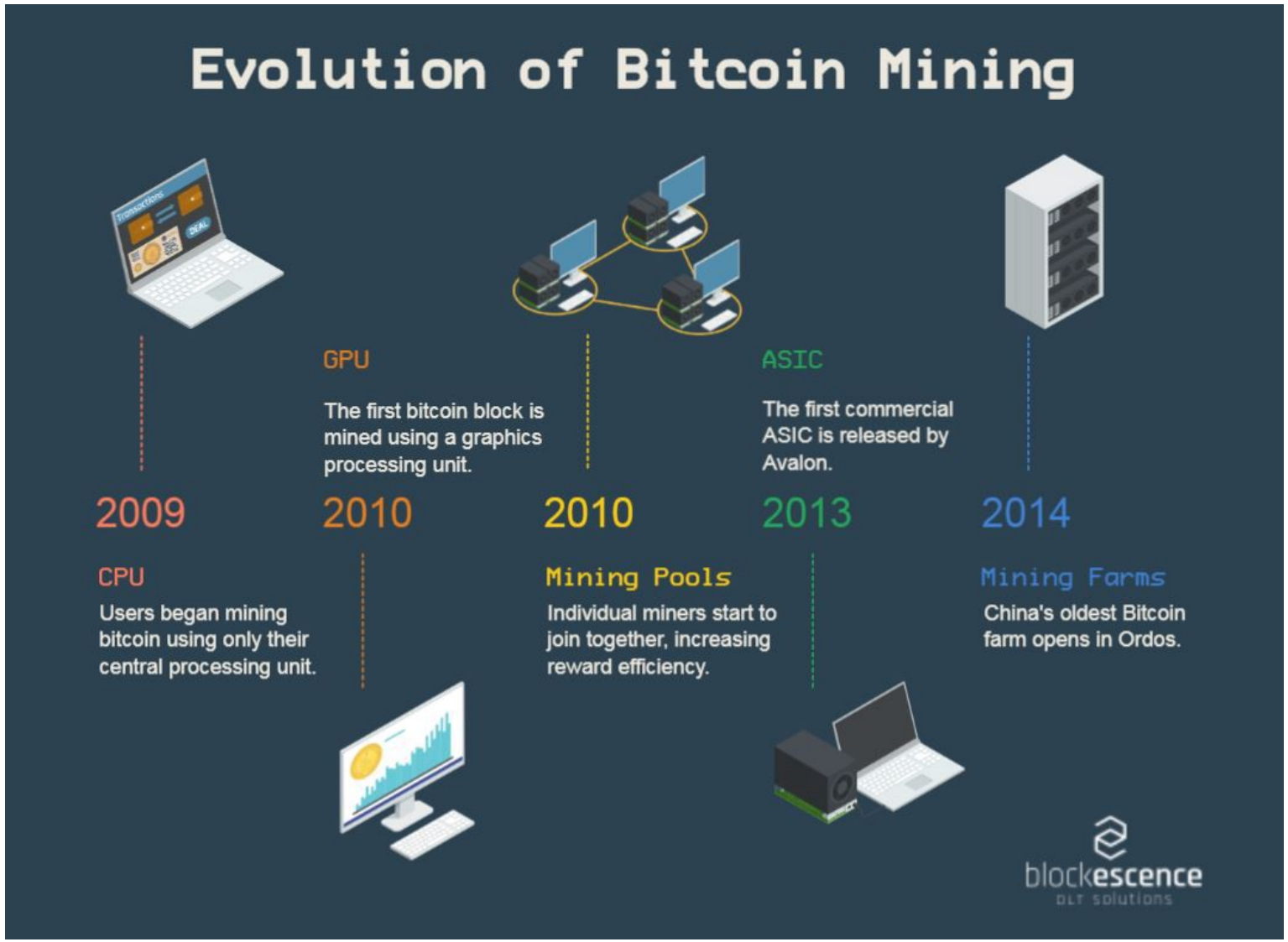
- **Steps to mine a block:**
  1. Download the entire blockchain
  2. Verify transactions
  3. Put verified transactions into a block
  4. Fina a valid nonce (solve the puzzle, aka PoW)
  5. Broadcast your block
  6. Profit!

Source: UCBerkeley Blockchain at Berkeley Fundamental Decal

# Blockchain Visual Demo




Source: https://andersbrownworth.com/blockchain/




Source: https://medium.com/@blockescence/the-evolution-of-cryptocurrency-mining-941e5ea8ea9f

TIBA

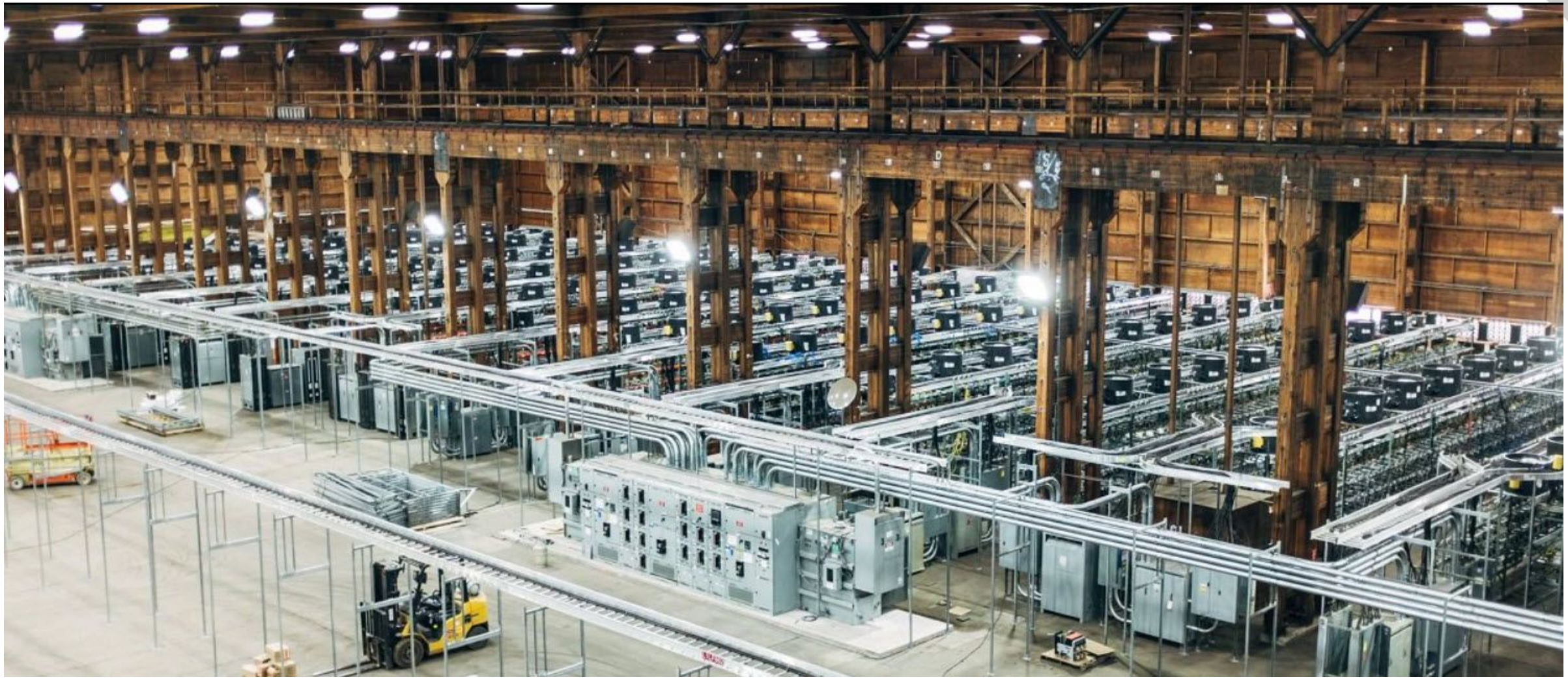
# Bitcoin Network

## Mining Race & Evolution

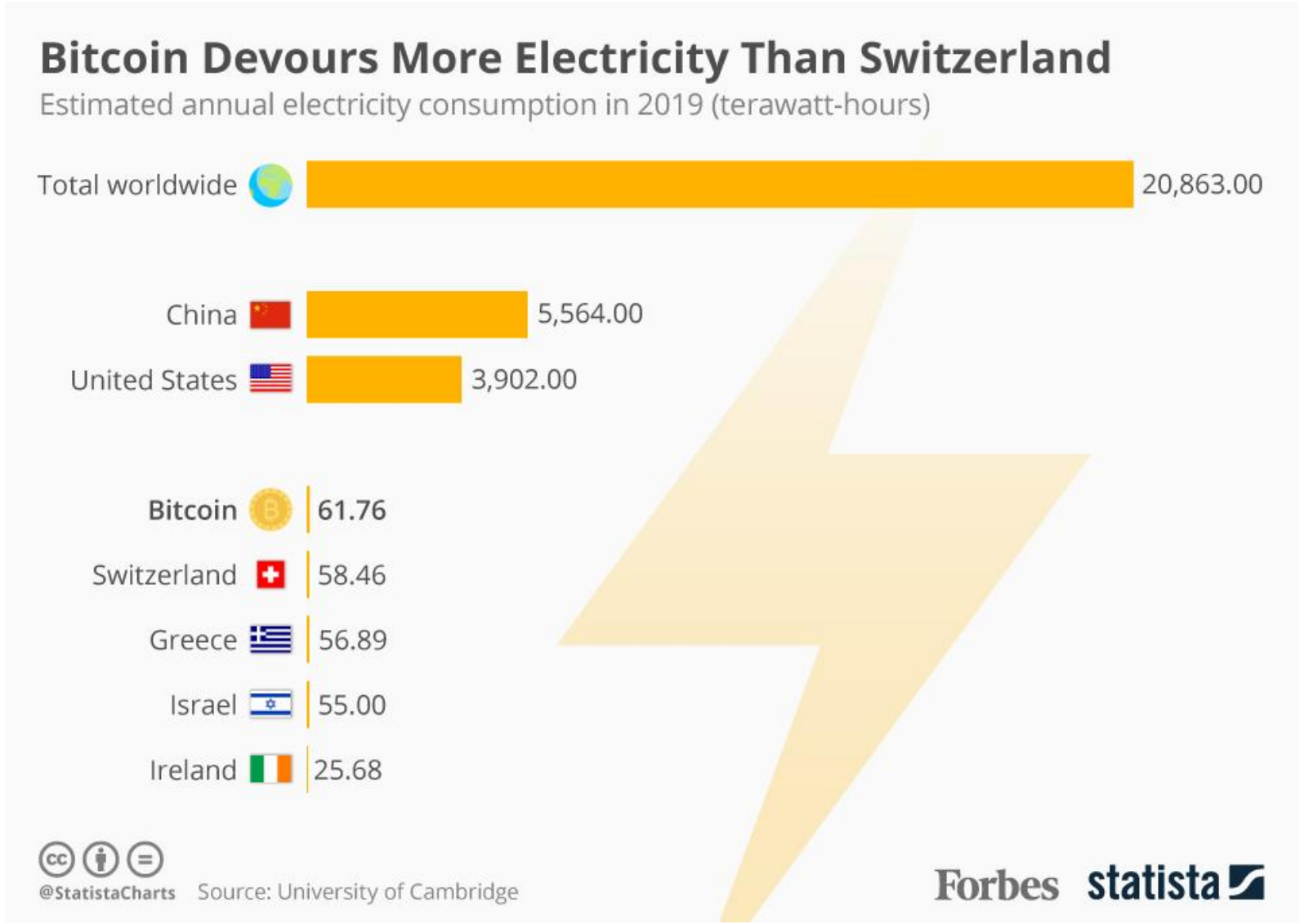



Source: https://thenextweb.com/hardfork/2018/02/02/a-brief-history-of-bitcoin-mining-hardware/, https://www.extremetech.com/gaming/264692-cryptocurrency-era-approach-used-gpus-caution, , https://www.amazon.com/DragonX-Whatsminer-Included-200V-240V-Required/dp/B07WNS9D6D

TIBA

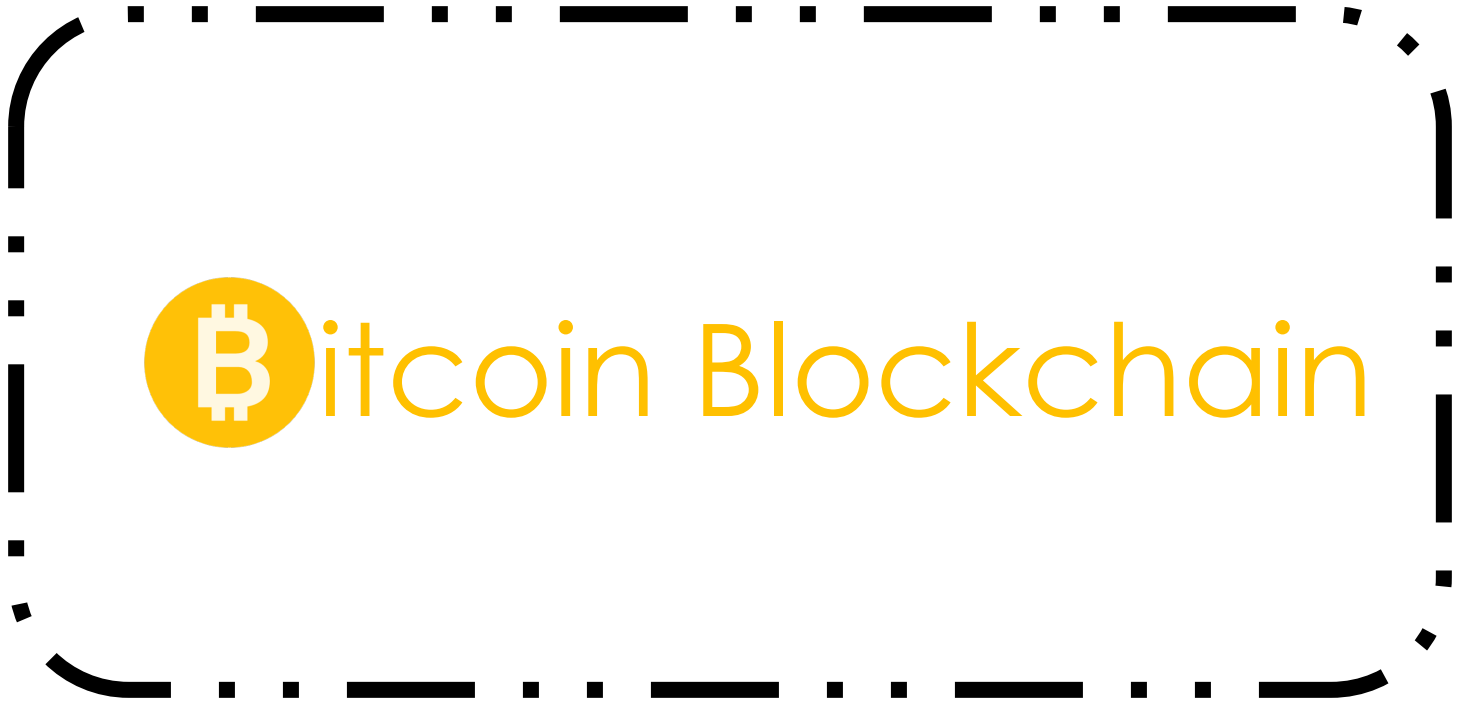


Source: https://blog.honeyminer.com/history-of-cryptocurrency-mining/




Source: https://www.forbes.com/sites/niallmccarthy/2019/07/08/bitcoin-devours-more-electricity-than-switzerland-infographic/#461d721c0ea1/

TIBA

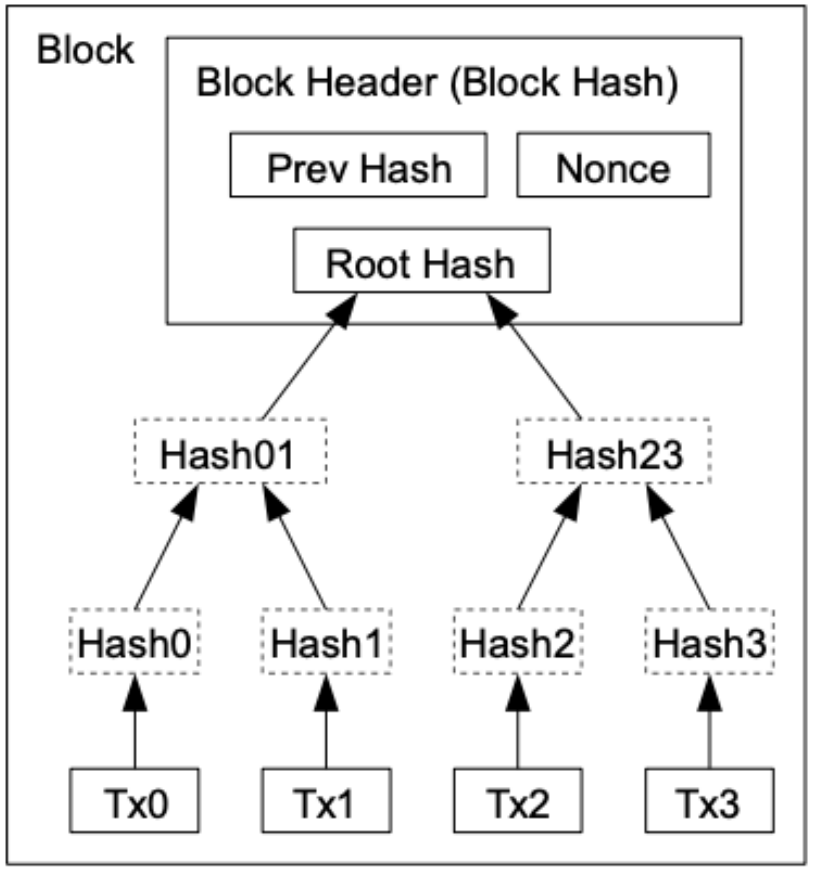


TIBA

# Bitcoin Blockchain

## Blocks

- **A Bitcoin block contains (simplified):**
  - Block header
    - Previous block hash
    - Nonce
    - Merkle tree root hash
  - All transactions in Merkle tree




Transactions Hashed in a Merkle Tree

Img: Bitcoin Whitepaper

# TIBA Bitcoin Blockchain

## Blocks in Details


Img: Princeton Bitcoin and Cryptocurrency Technologies

TIBA

# Bitcoin Blockchain

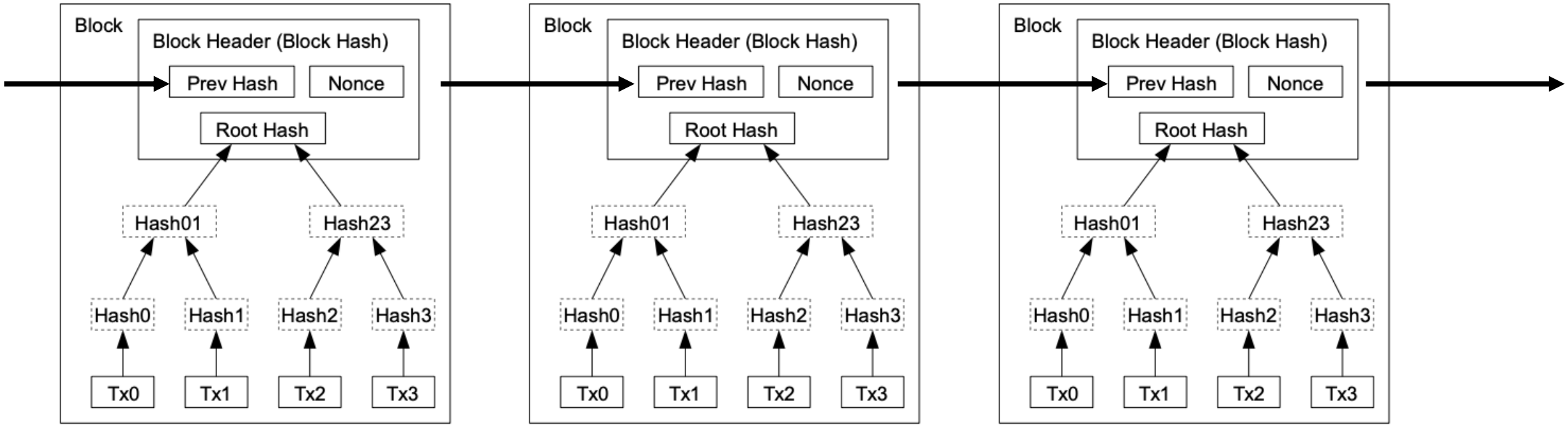
## Types of Users

- **Full Node**
  - hold and distributes full-copy of the entire blockchain ledger since the genesis block
- **Light Node**
  - only store block headers to validate the authenticity of the transactions
- **Miner**
  - verify transactions and create new blocks
- **Wallet**
  - interact with the blockchain

TIBA

# Bitcoin Blockchain

## Full Nodes

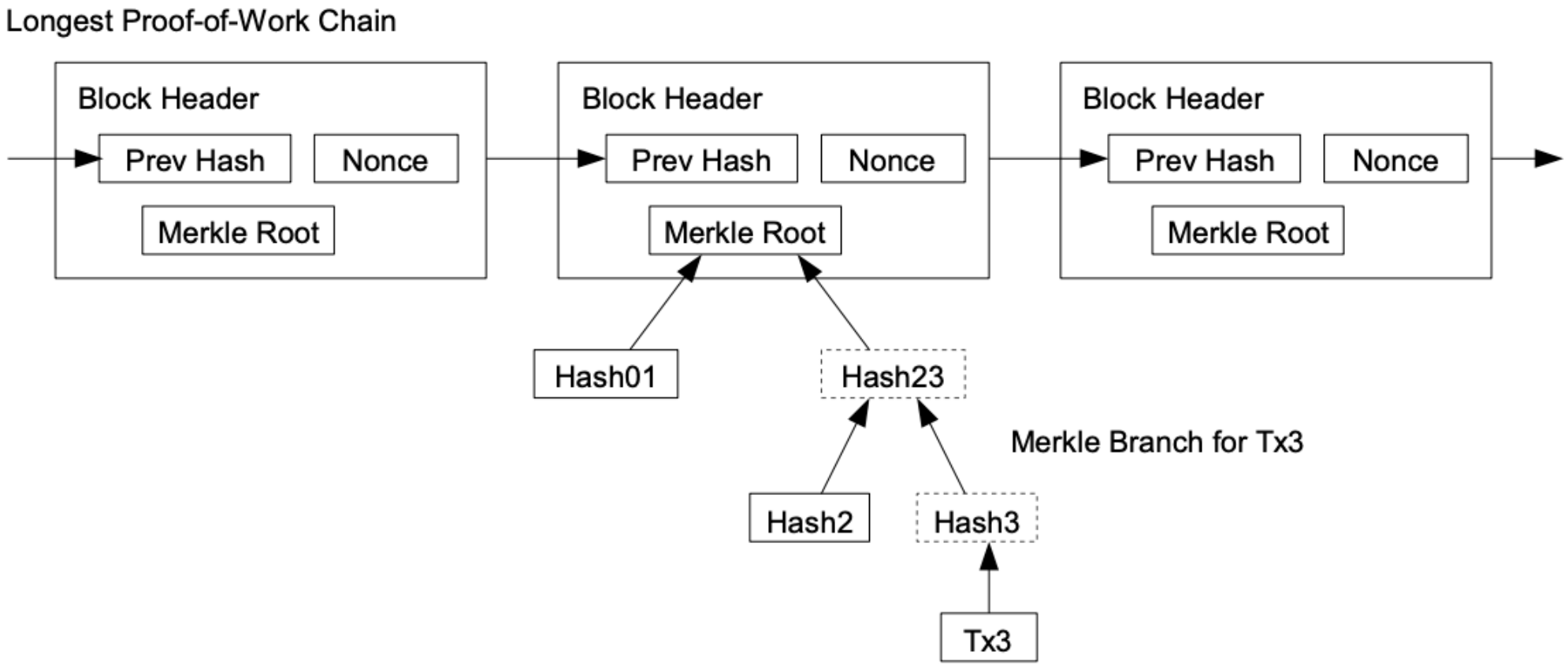



Img: Bitcoin Whitepaper

TIBA

# Bitcoin Blockchain

## Light Nodes




Img: Bitcoin Whitepaper

# TIBA Real-time Transaction Demo

SUPPORT@BILLFODL.COM

USD 0

**Billfodl**

SHOP BILLFODL HOW IT WORKS ABOUT BLOGS CONTACT


CLOSE

**Block Hash**

000000000000000000a40e998fb4c9647008001222decb8687f24b31ac384b4

| | |
|---|---|
| **Height** | 629144 |
| **Size** | 1085.549KB |
| **Difficulty** | 16104807485529.383 |
| **Found by** | |
| **Time** | Wed, 06 May 2020 03:16:23 GMT |

Source: https://billfodl.com/pages/bitbonkers

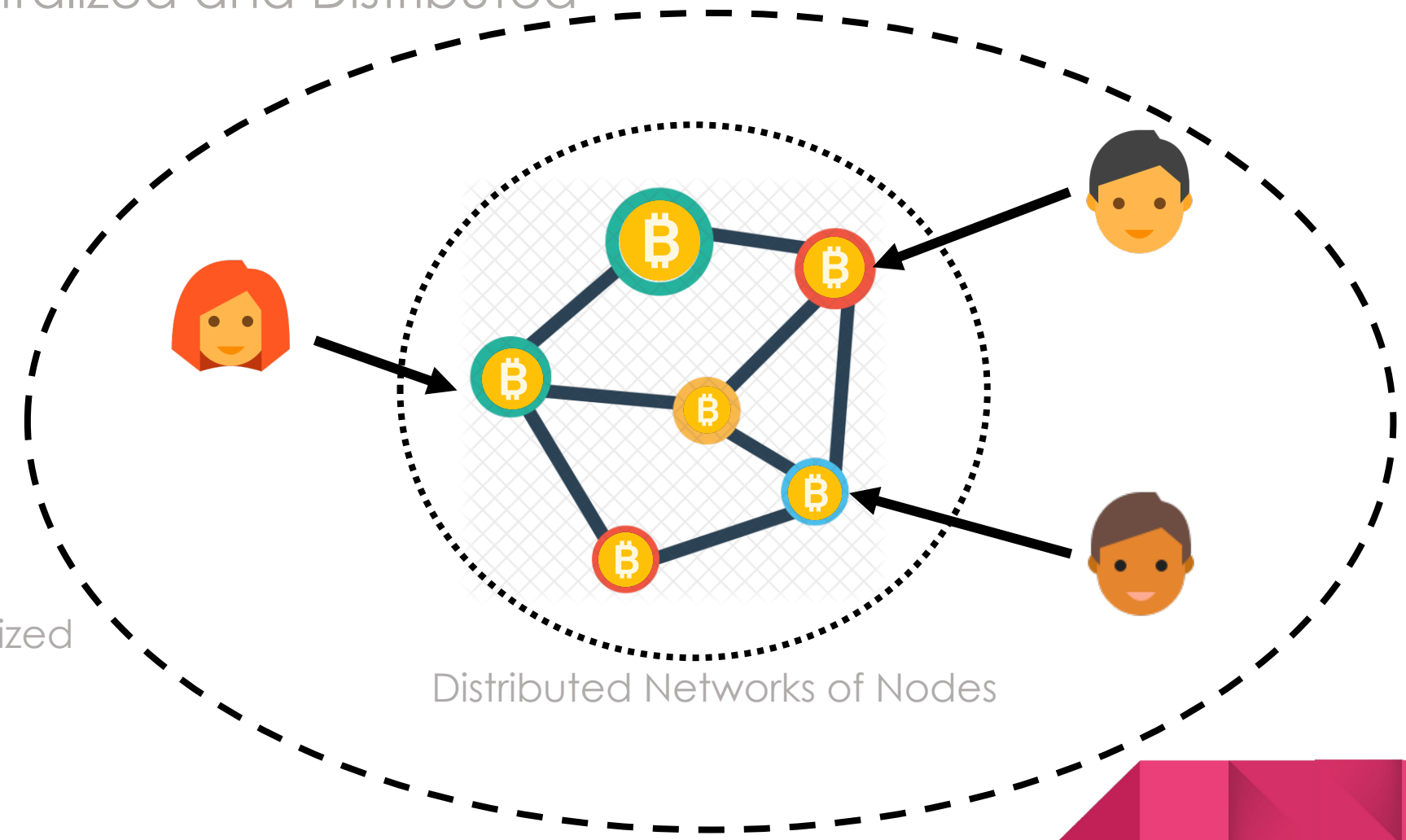
TIBA

# Bitcoin's Value

TIBA

# Bitcoin's Value

## Decentralized and Distributed

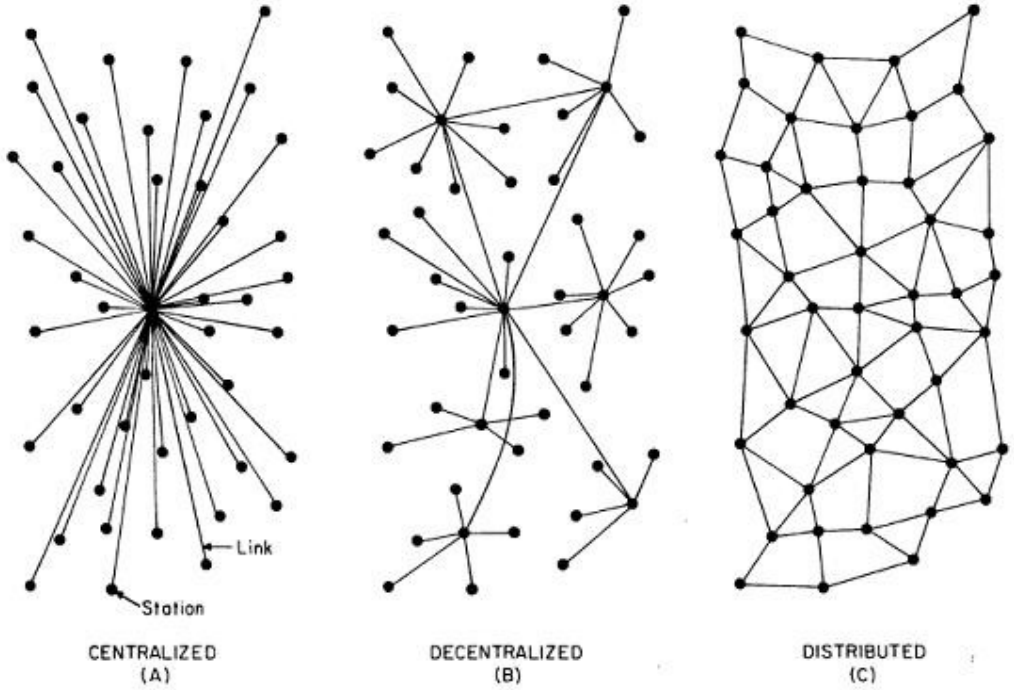


TIBA

# Bitcoin's Value

## Digital Gold

- **Bitcoin Blockchain** ==
  - immutable transaction database
  - **distributed** network of nodes
    - chain of blocks + chain of individual transactions
- **Core Value**:
  - **decentralized** payment system
    - an immutable ledger of data without relying on a central authority
  - digital asset with real value
  - digital currency without boundary




Source: https://medium.com/distributed-economy/what-is-the-difference-between-decentralized-and-distributed-systems-f4190a5c6462

TIBA

# Homework Assignments

- Bitcoin: A Peer-to-Peer Electronic Cash System by Satoshi Nakamoto
- But how does bitcoin actually work?
- Bitcoin Halving Clock
- Bitcoin 101, Ch7 How Bitcoin Mining Works
- What is the merkle tree in Bitcoin?
- How the Bitcoin protocol actually works
- How Bitcoin Works Under the Hood

TIBA

# Questions?

TIBA

Blockchain 1.0
Bitcoin
by
Samuel Tang

Thank you for listening!
See you again soon!