TIBA

Blockchain 1.0

₿itcoin

By Samuel Tang, TIBA@TsinghuaUniversity

Goal: How does Bitcoin work?

Content

- Bitcoin
  - Identity
  - Transaction
  - Decentralized Network
  - Blockchain

Bitcoin

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

Bitcoin Identity

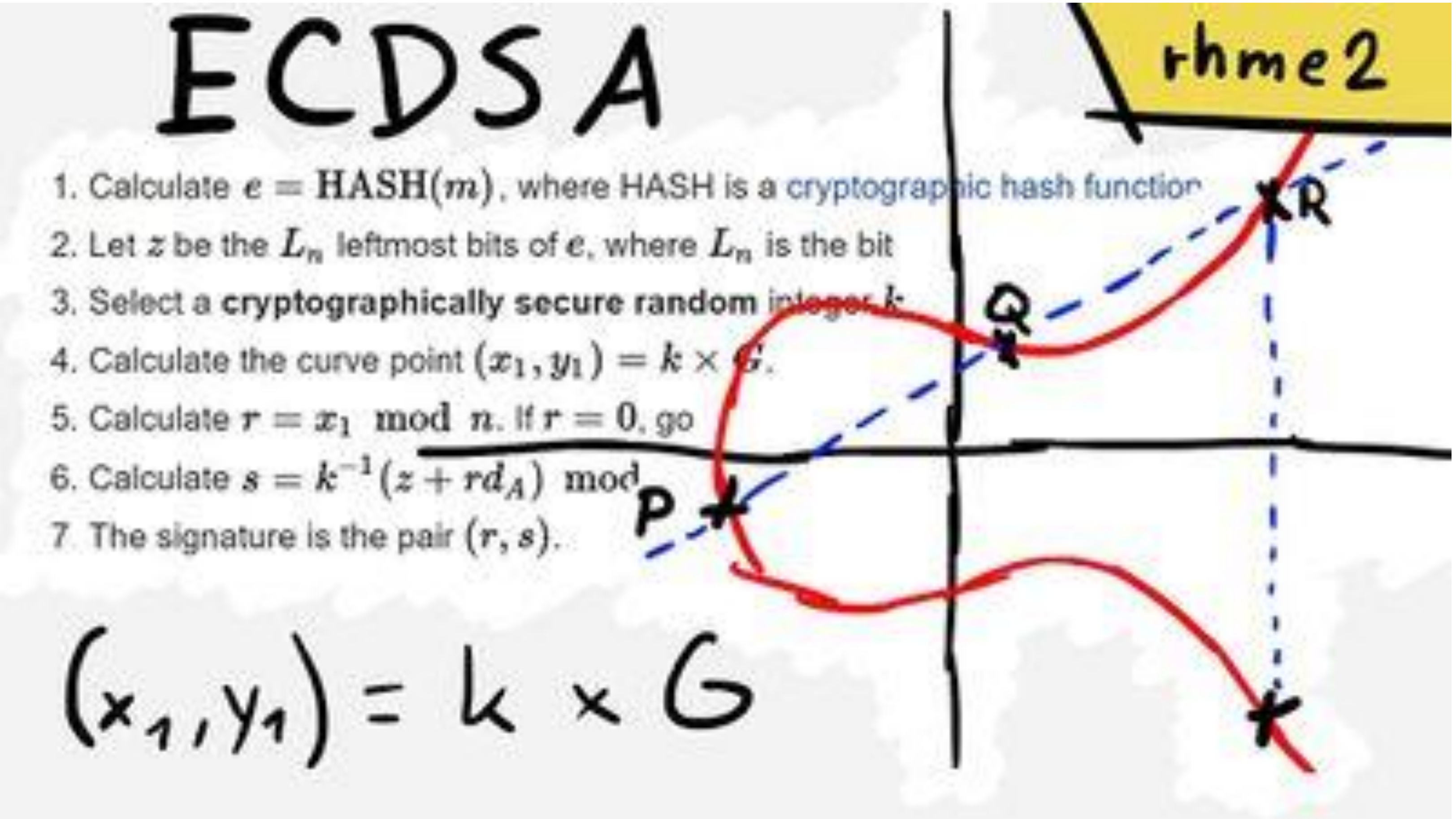
Random strings as identity

- **Public key**
  - **your username**
  - generated from private key using
    Elliptic Curve Digital Signature Algorithm (**ECDSA**)
  - 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

Bitcoin Identity

ECDSA



ECDSA

1. Calculate $e = \mathrm{HASH}(m)$, where HASH is a cryptographic hash function
2. Let z be the L_n leftmost bits of e, where L_n is the bit
3. Select a **cryptographically secure random** integer k
4. Calculate the curve point $(x_1, y_1) = k \times G$.
5. Calculate $r = x_1 \mod n$. If $r = 0$, go
6. Calculate $s = k^{-1}(z + rd_A) \mod$
7. The signature is the pair (r, s).

$$(x_1, y_1) = k \times G$$

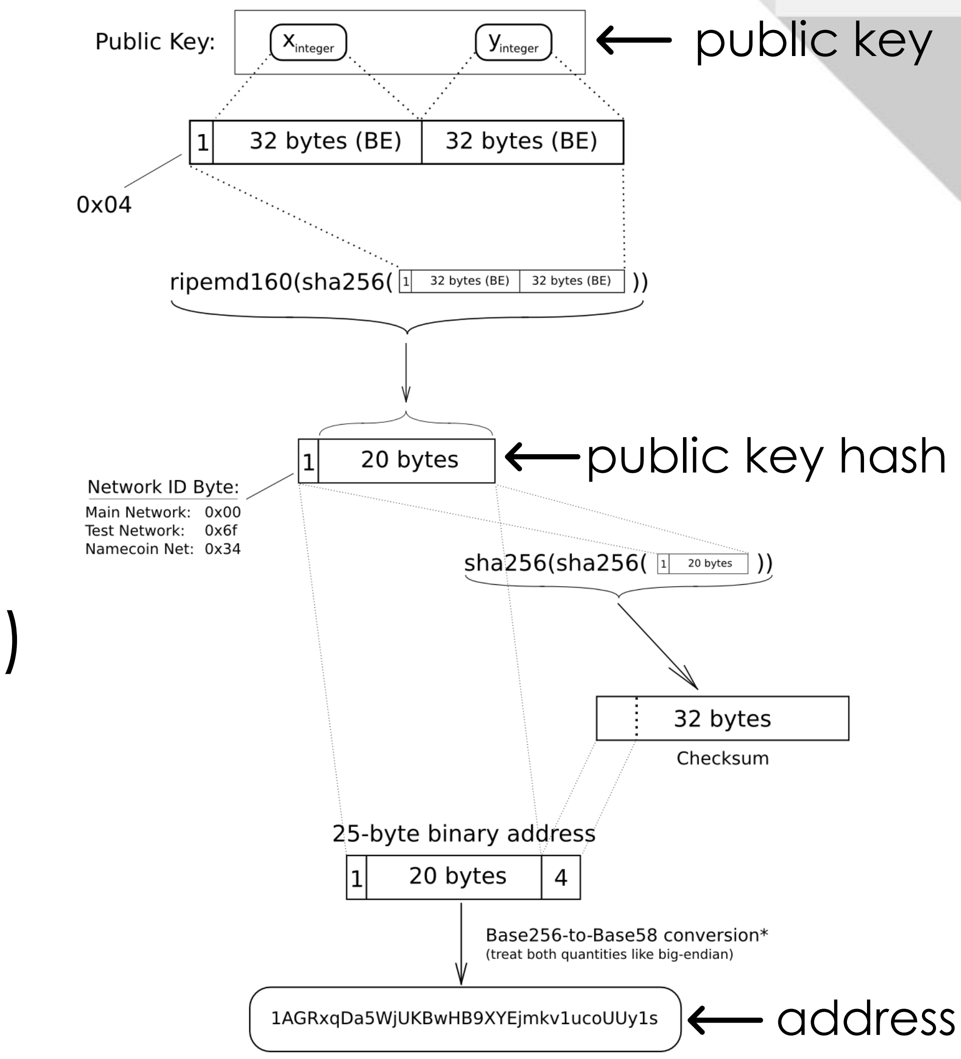
Source: https://en.bitcoinwiki.org/wiki/Elliptic_Curve_Digital_Signature_Algorithm

Bitcoin Identity

Random strings as identity

- **Address**
  - **your user id**
  - generated from public key (public key -> public key hash -> address)
  - 20 bytes
  - 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'

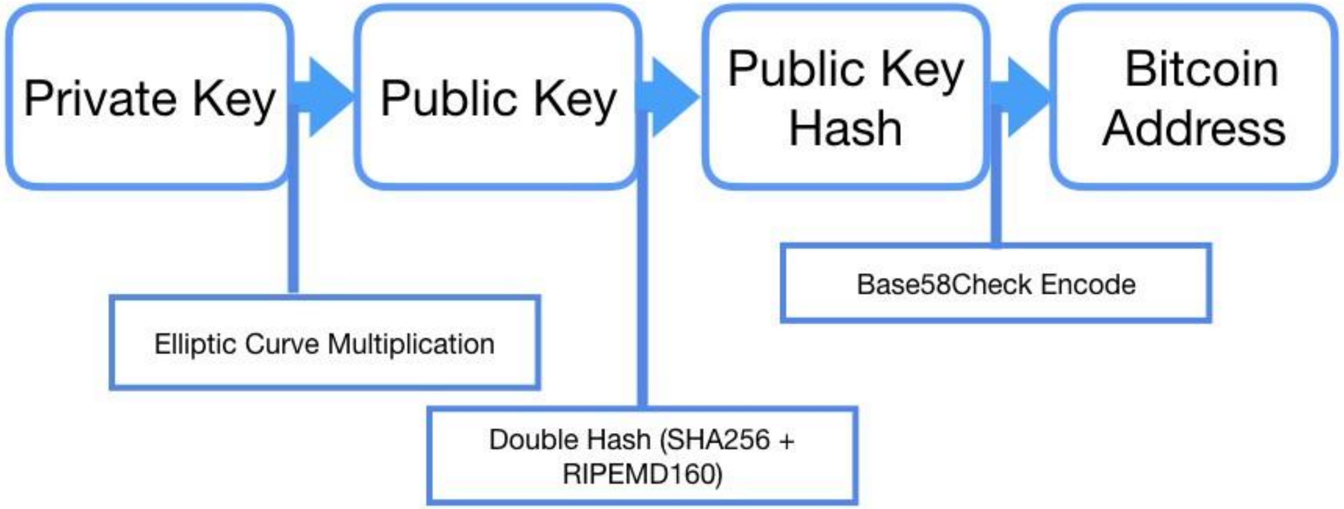
etotheipi@gmail.com / 1Gffm7LKXcNFPrtxy6yF4JBoe5rVka4sn1

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

Bitcoin Identity

Random strings as identity

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



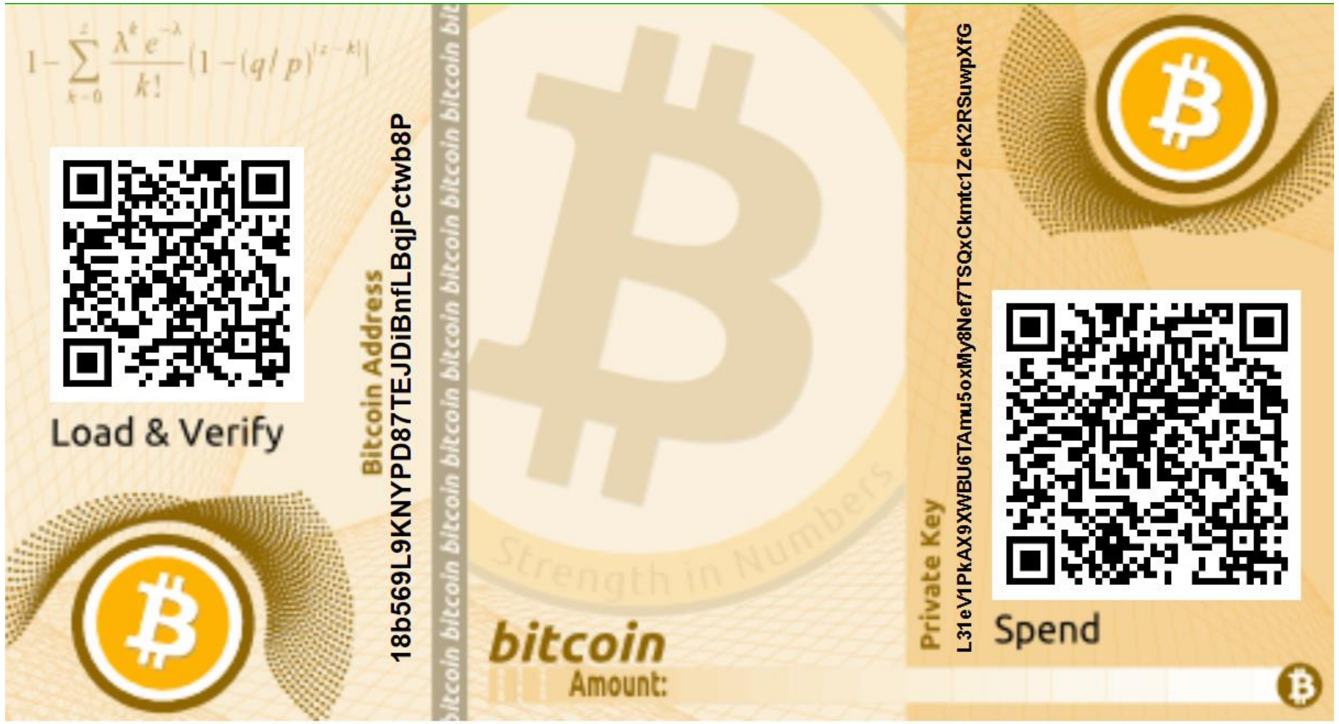
*wise advice: use a new address for each transaction
== generate a new key pair each time

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

Bitcoin Identity

Keys Storage

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


Load & Verify
Bitcoin Address
18b569L9KNYPD87TEJDiBnfLBqjPctwb8P
Strength in Numbers
bitcoin
Amount:
Private Key
L31eV1PkAX9XWBU6TAmu5oxMy8Nef7TSQxCkmtc1ZeK2RSuwpXfG
Spend

paper wallet

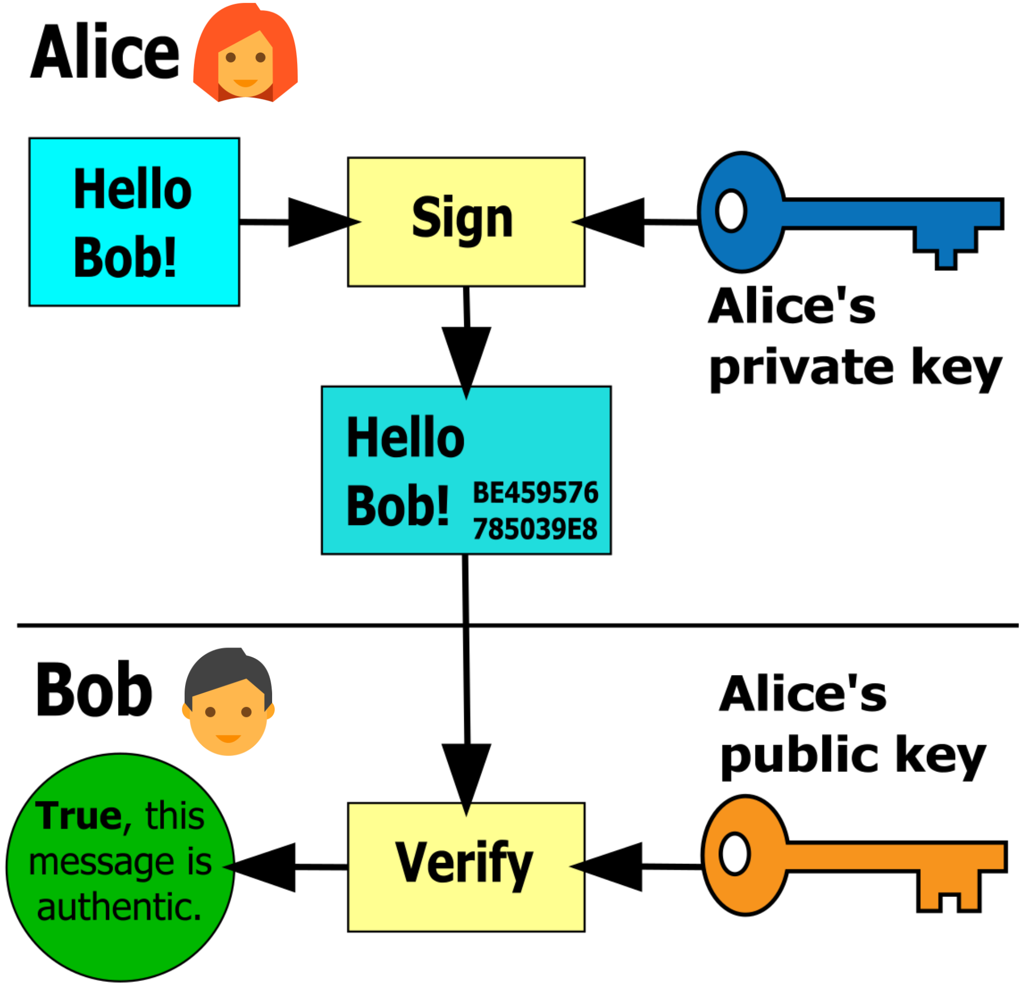
Source: https://www.coindesk.com/learn/bitcoin-101/how-to-store-your-bitcoins
https://www.bitaddress.org/

TIBA

Bitcoin Identity

Proving Identity

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

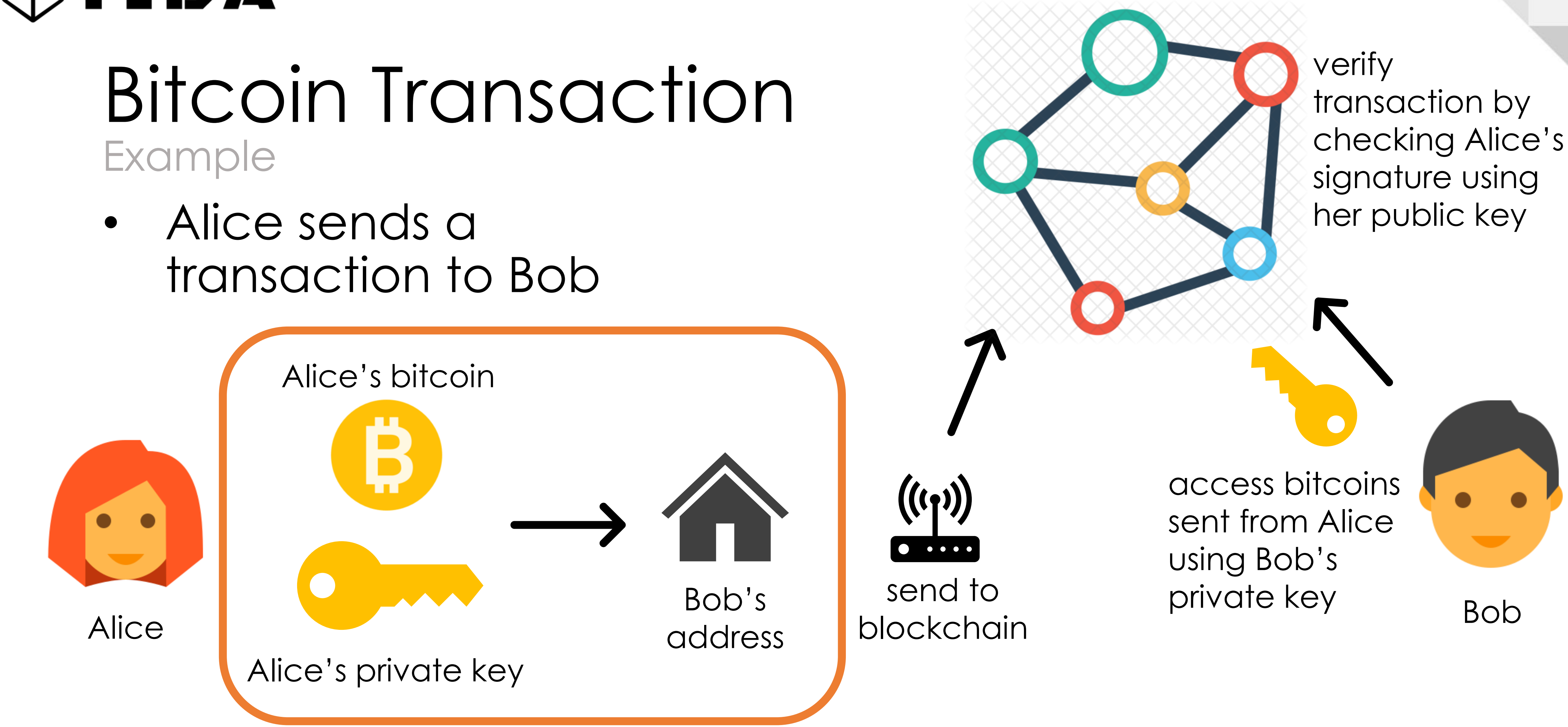


Source: https://en.wikipedia.org/wiki/Digital_signature

Bitcoin Transaction

Example

- Alice sends a transaction to Bob



Bitcoin's network

verify transaction by checking Alice's signature using her public key

Alice

Alice's bitcoin

Alice's private key

Bob's address

send to blockchain

access bitcoins sent from Alice using Bob's private key

Bob

A transaction signed by Alice's signature

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

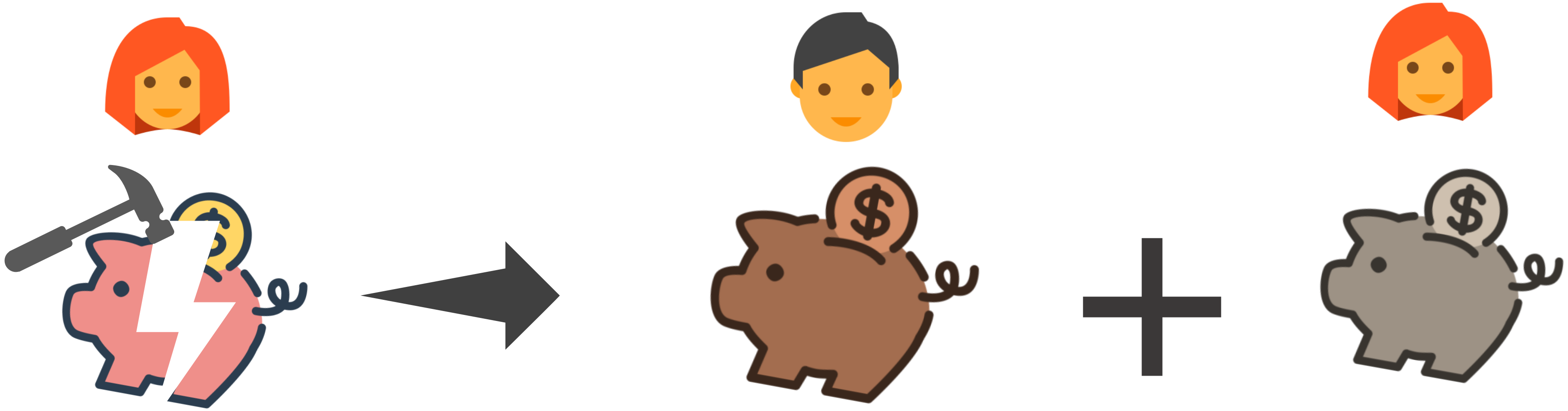
5 BTC
1FxyjVSqEaVtPcSv9z4qQoHGCdoFtjmfyp

TIBA

Bitcoin Transaction

Behind the Scene – Spending UTXO

- example: Alice sending 3 BTC to Bob



5 BTC
1FxyjVSqEaVtPcSv9z4qQoHGCdoFtjmfyp

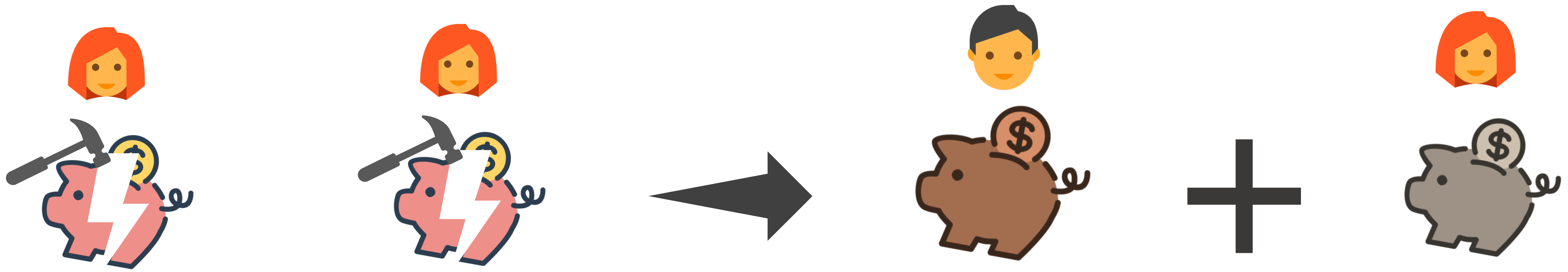
3 BTC
1K6yjVBVrUvAU8kHed3eQGZrfAmi3nwncS

2 BTC
18nWcNURo4ygH7mRu7YwN6PkXnDCigSqoo

Bitcoin Transaction

Behind the Scene – Spending UTXO

- example: Alice sending 7 BTC to Bob



5 BTC
1FxyjVSqEaVtPcSv9z4qQoHGCd
oFtjmfyp

3 BTC
1FxyjVSqEaVtPcSv9z4qQoHGCd
oFtjmfyp

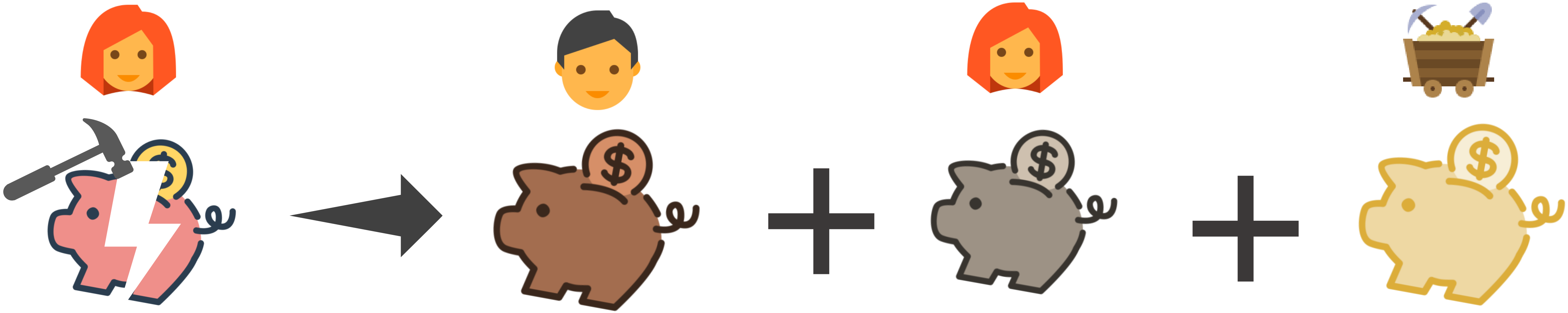
7 BTC
1K6yjVBVrUvAU8kHed3eQGZrfAmi
3nwncS

1 BTC
18nWcNURo4ygH7mRu7YwN6PkXn
DCigSqoo

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

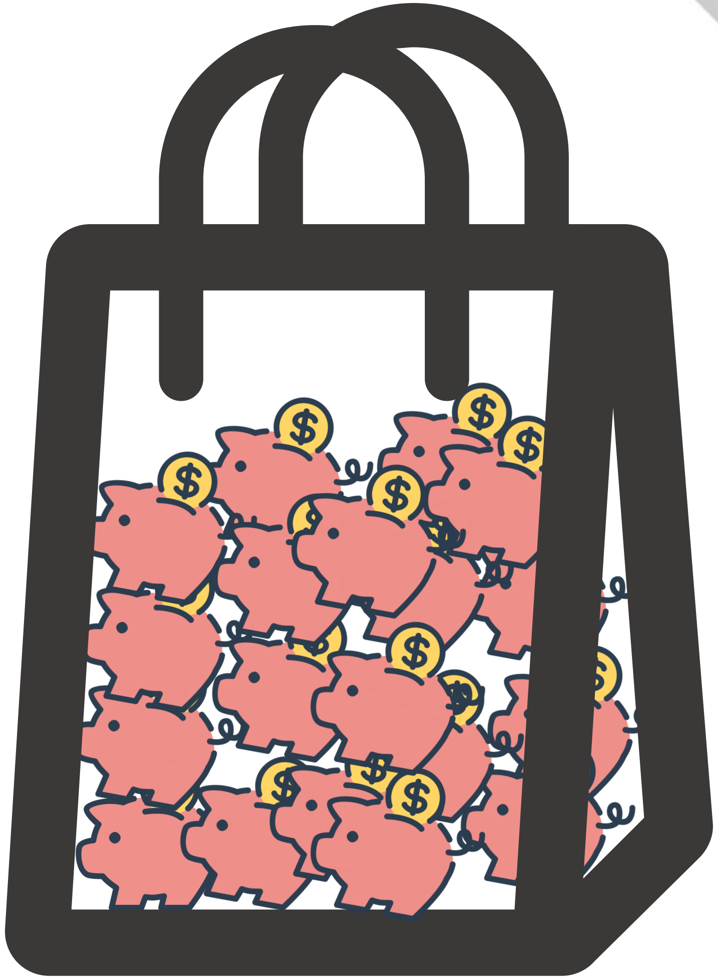
0.2 BTC
Transaction Fee
Miner's address

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

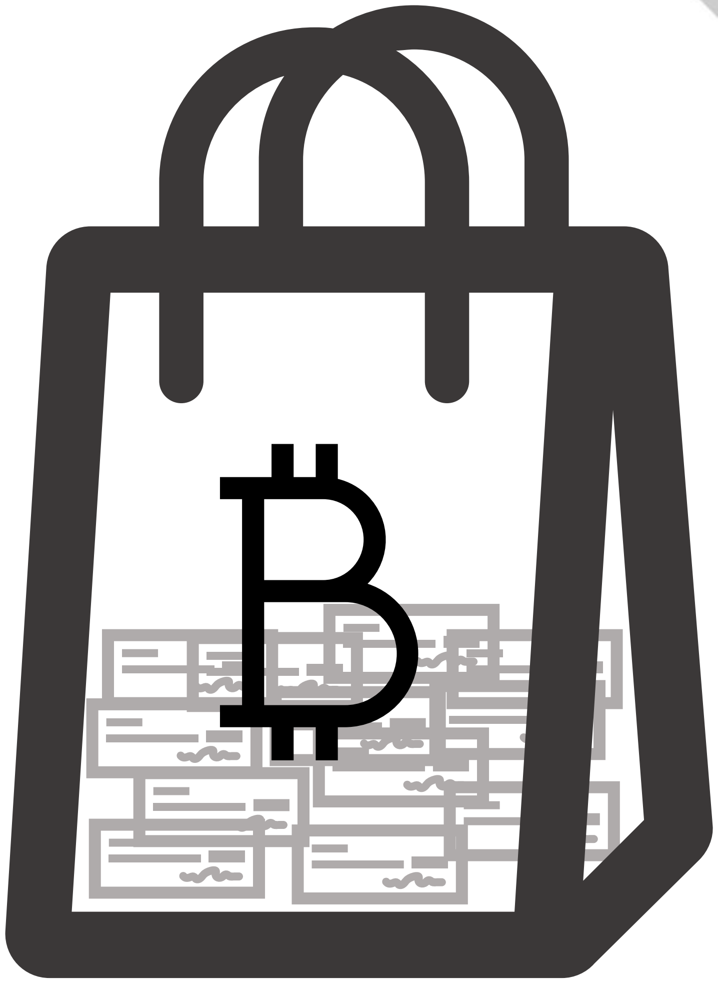
Source: https://thecoinrise.com/how-do-bitcoin-transactions-work/

TIBA

Bitcoin Transaction

Transaction Pool

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



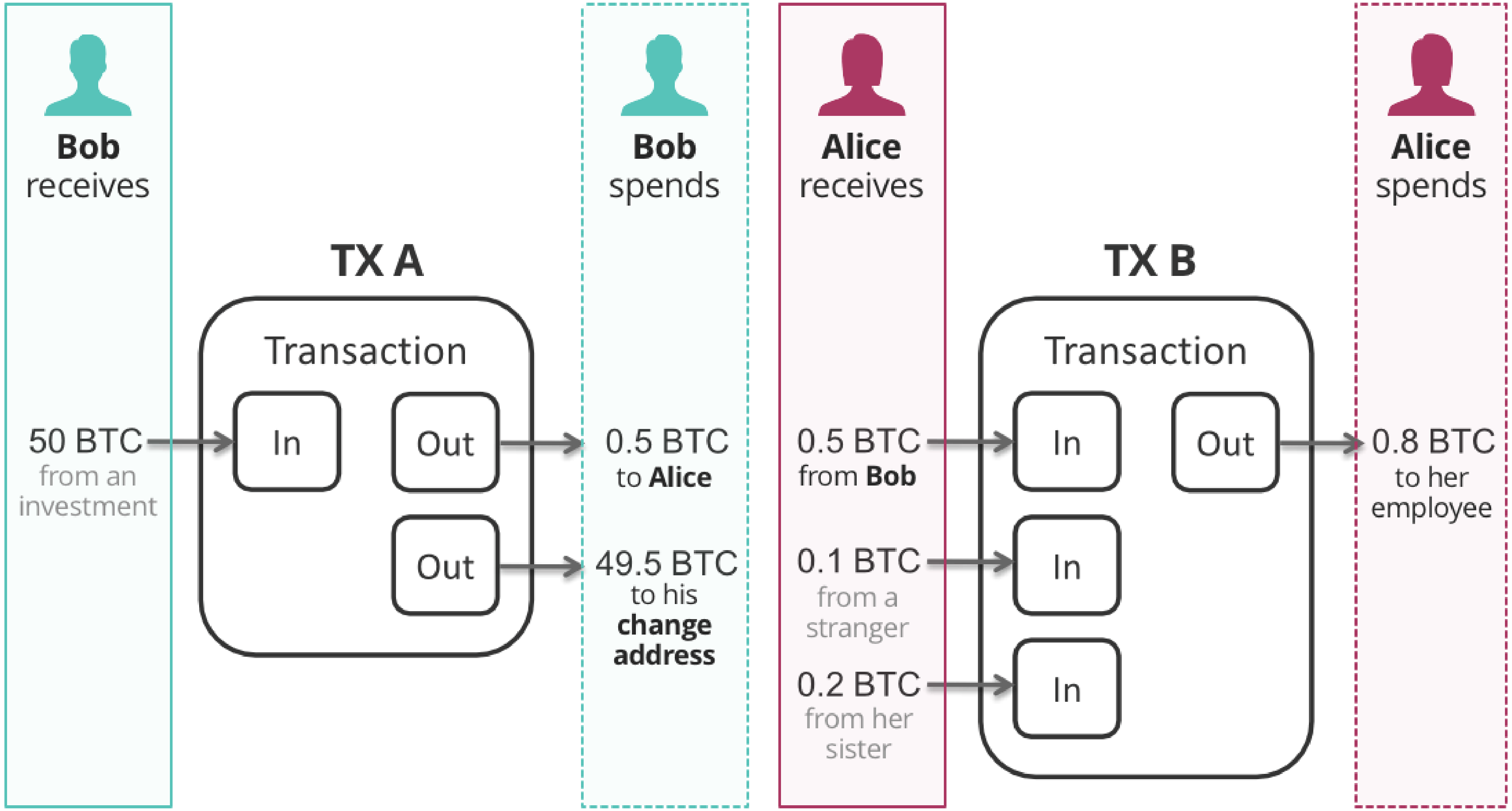
Transaction pool

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

TIBA

Bitcoin Transaction

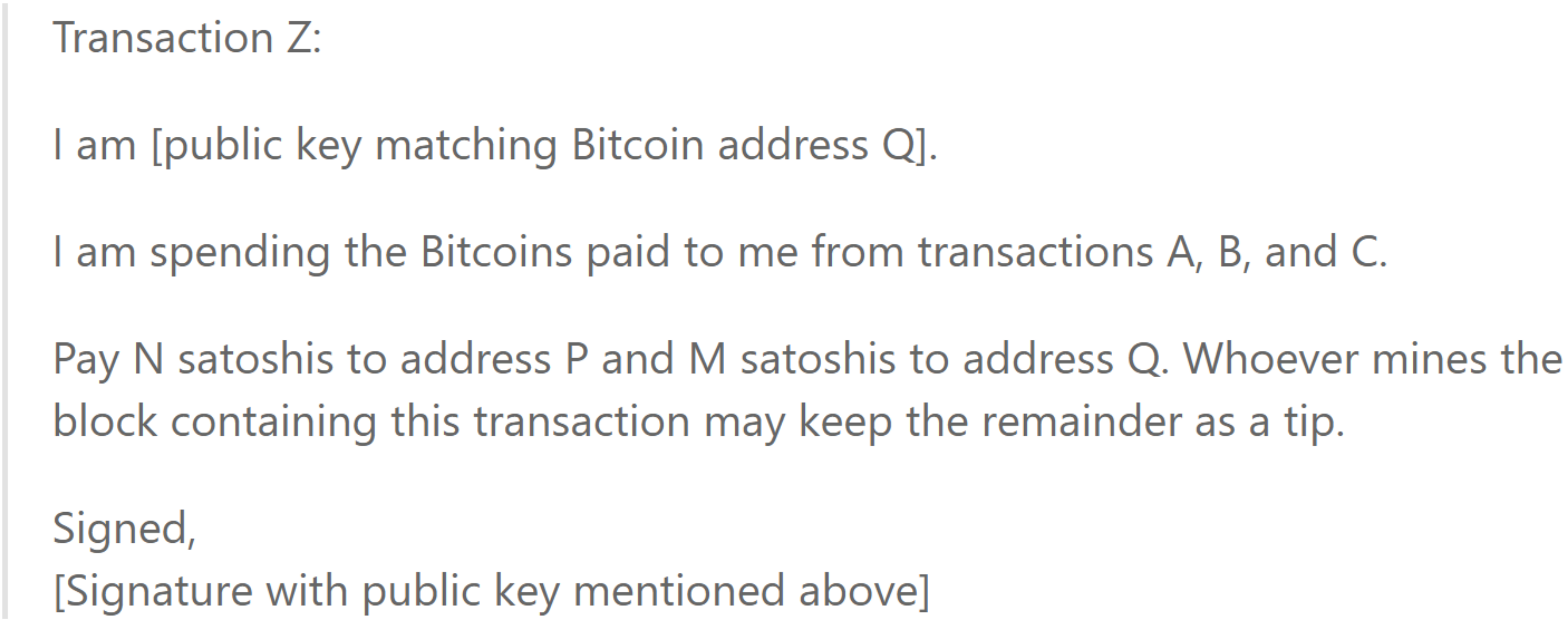
Example



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

Bitcoin Transaction

Summary

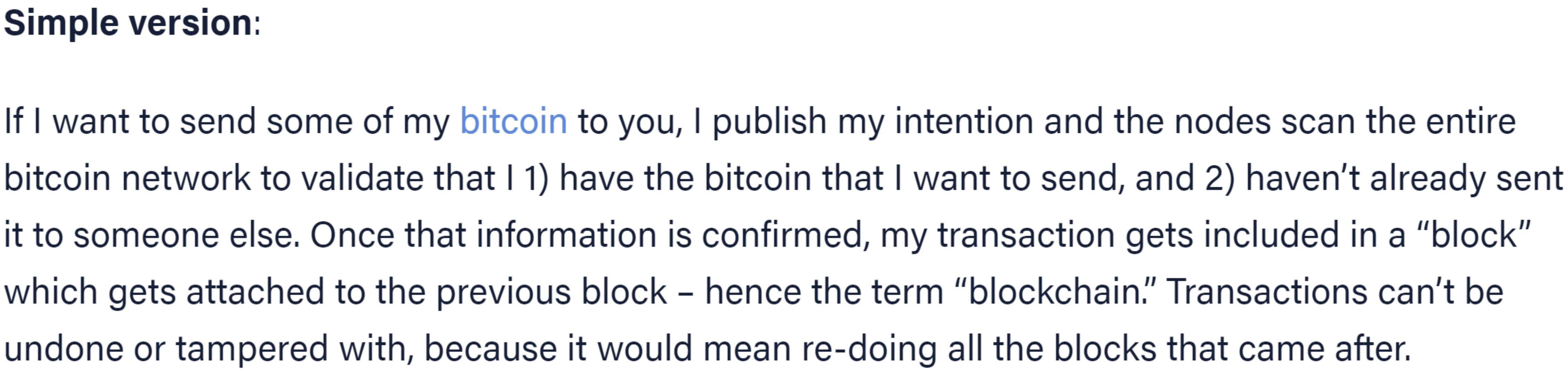


> Transaction Z:
>
> I am [public key matching Bitcoin address Q].
>
> I am spending the Bitcoins paid to me from transactions A, B, and C.
>
> Pay N satoshis to address P and M satoshis to address Q. Whoever mines the block containing this transaction may keep the remainder as a tip.
>
> Signed,
> [Signature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

Bitcoin Transaction

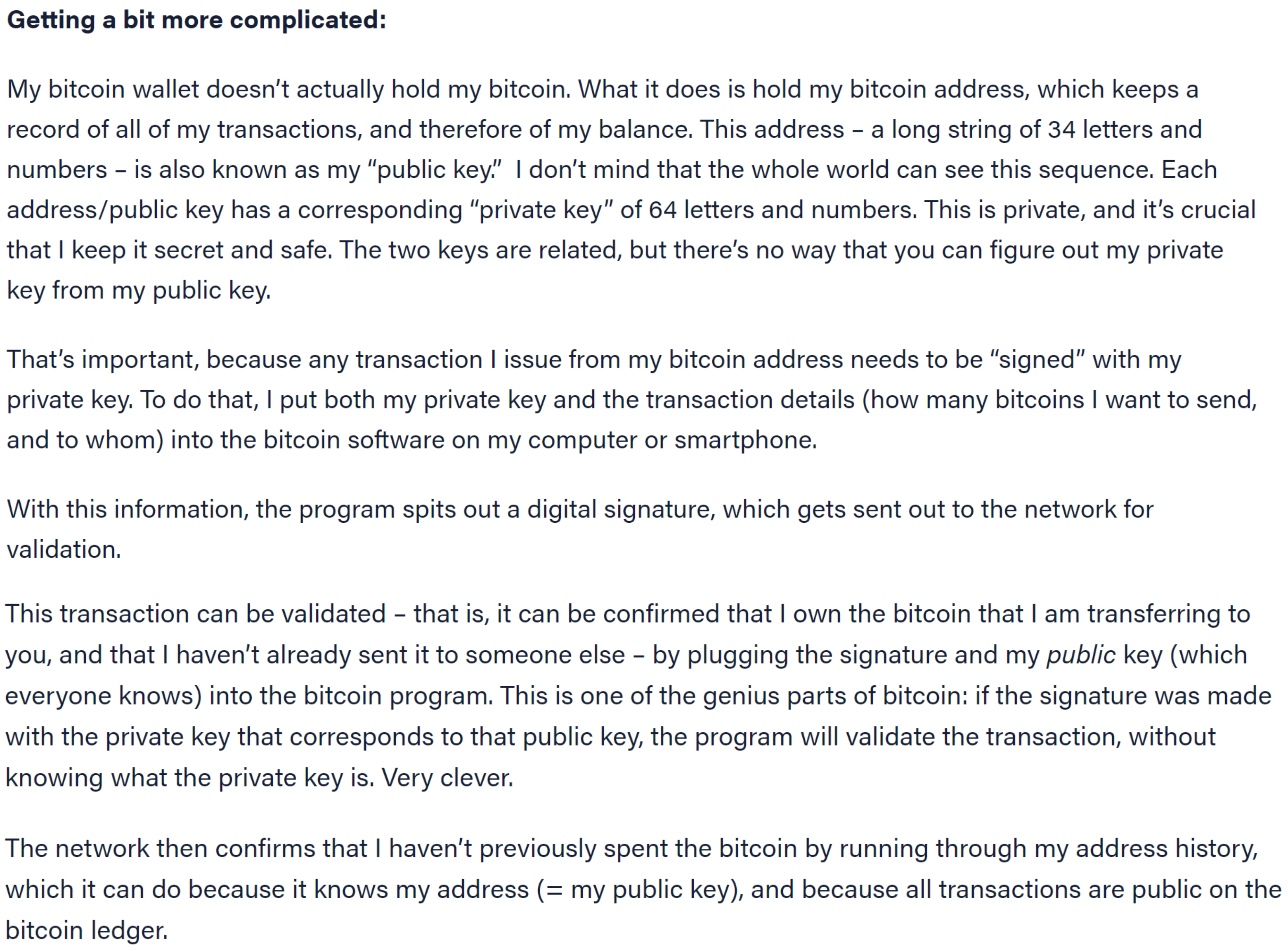
Summary



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



Getting a bit more complicated:

My bitcoin wallet doesn't actually hold my bitcoin. What it does is hold my bitcoin address, which keeps a record of all of my transactions, and therefore of my balance. This address – a long string of 34 letters and numbers – is also known as my "public key." I don't mind that the whole world can see this sequence. Each address/public key has a corresponding "private key" of 64 letters and numbers. This is private, and it's crucial that I keep it secret and safe. The two keys are related, but there's no way that you can figure out my private key from my public key.

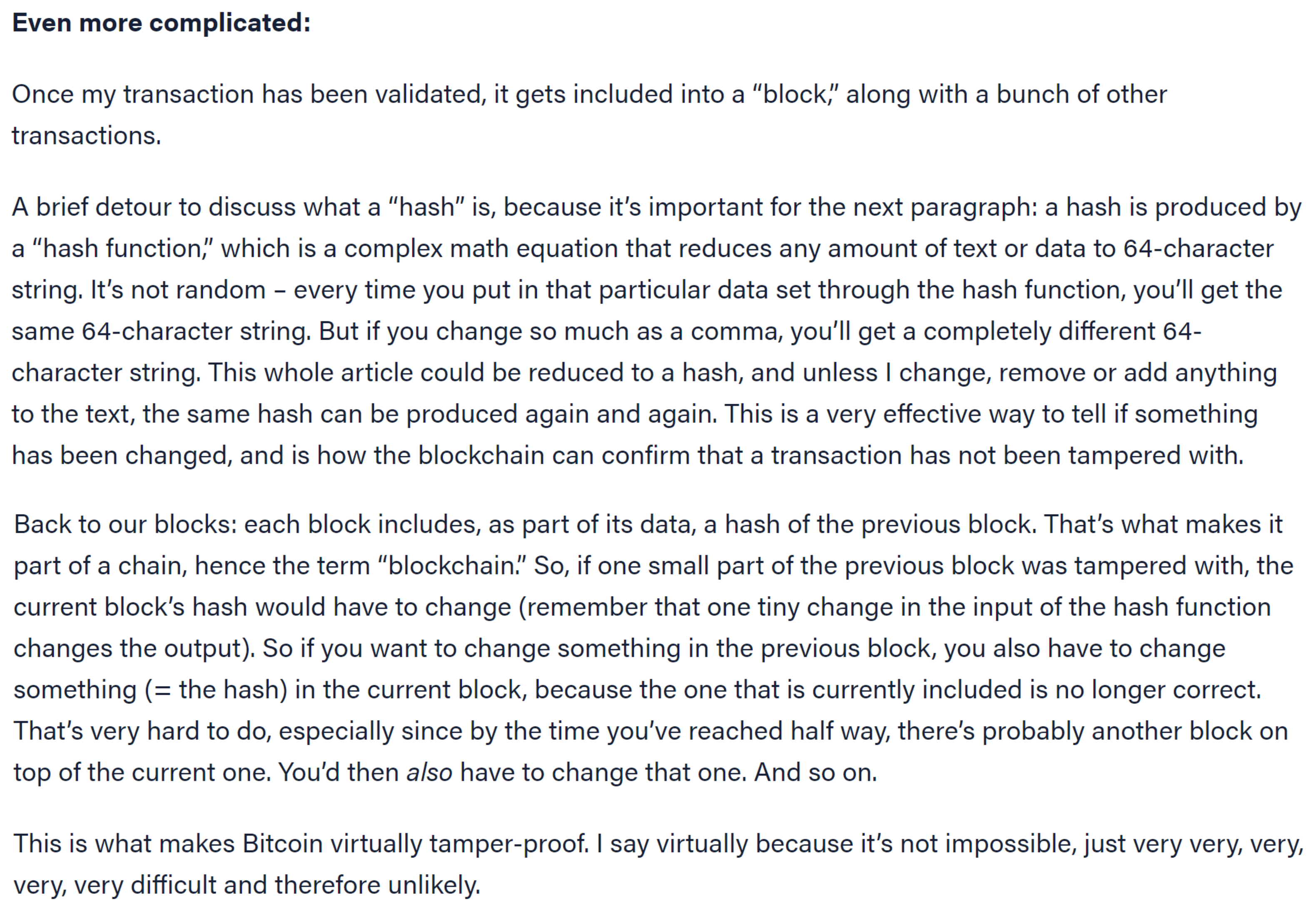
That's important, because any transaction I issue from my bitcoin address needs to be "signed" with my private key. To do that, I put both my private key and the transaction details (how many bitcoins I want to send, and to whom) into the bitcoin software on my computer or smartphone.

With this information, the program spits out a digital signature, which gets sent out to the network for validation.

This transaction can be validated – that is, it can be confirmed that I own the bitcoin that I am transferring to you, and that I haven't already sent it to someone else – by plugging the signature and my *public* key (which everyone knows) into the bitcoin program. This is one of the genius parts of bitcoin: if the signature was made with the private key that corresponds to that public key, the program will validate the transaction, without knowing what the private key is. Very clever.

The network then confirms that I haven't previously spent the bitcoin by running through my address history, which it can do because it knows my address (= my public key), and because all transactions are public on the bitcoin ledger.

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



Even more complicated:

Once my transaction has been validated, it gets included into a "block," along with a bunch of other transactions.

A brief detour to discuss what a "hash" is, because it's important for the next paragraph: a hash is produced by a "hash function," which is a complex math equation that reduces any amount of text or data to 64-character string. It's not random – every time you put in that particular data set through the hash function, you'll get the same 64-character string. But if you change so much as a comma, you'll get a completely different 64-character string. This whole article could be reduced to a hash, and unless I change, remove or add anything to the text, the same hash can be produced again and again. This is a very effective way to tell if something has been changed, and is how the blockchain can confirm that a transaction has not been tampered with.

Back to our blocks: each block includes, as part of its data, a hash of the previous block. That's what makes it part of a chain, hence the term "blockchain." So, if one small part of the previous block was tampered with, the current block's hash would have to change (remember that one tiny change in the input of the hash function changes the output). So if you want to change something in the previous block, you also have to change something (= the hash) in the current block, because the one that is currently included is no longer correct. That's very hard to do, especially since by the time you've reached half way, there's probably another block on top of the current one. You'd then *also* have to change that one. And so on.

This is what makes Bitcoin virtually tamper-proof. I say virtually because it's not impossible, just very very, very, very, very difficult and therefore unlikely.

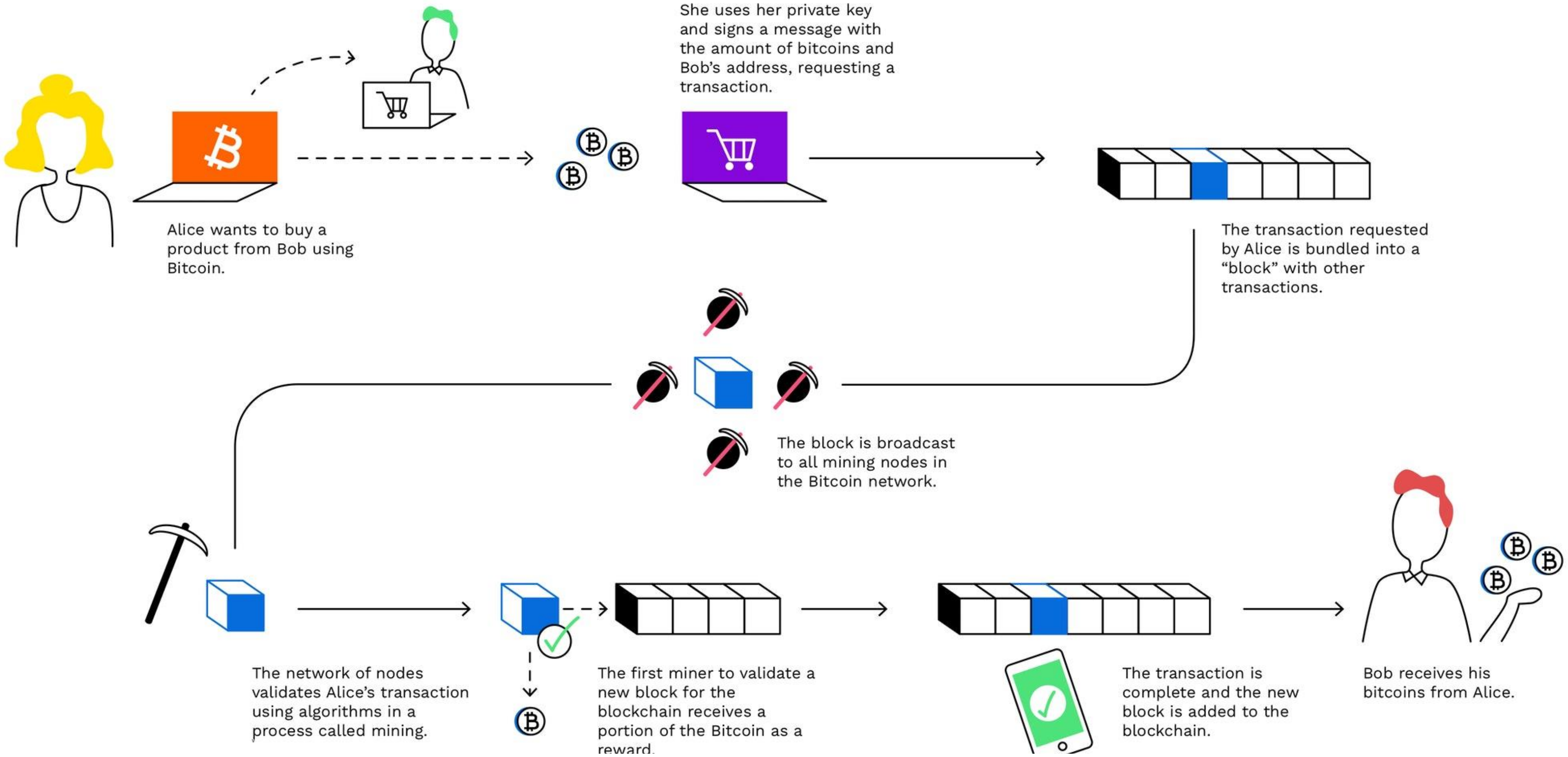
Source: https://www.coindesk.com/learn/bitcoin-101/how-do-bitcoin-transactions-work

Question: Who verify those transactions?

Answer: Miners

What is Bitcoin Mining?

How Bitcoin Transactions work



Alice wants to buy a product from Bob using Bitcoin.

She uses her private key and signs a message with the amount of bitcoins and Bob's address, requesting a transaction.

The transaction requested by Alice is bundled into a "block" with other transactions.

The block is broadcast to all mining nodes in the Bitcoin network.

The network of nodes validates Alice's transaction using algorithms in a process called mining.

The first miner to validate a new block for the blockchain receives a portion of the Bitcoin as a reward.

The transaction is complete and the new block is added to the blockchain.

Bob receives his bitcoins from Alice.

Source: https://www.bitpanda.com/academy/en/lessons/what-is-bitcoin-mining-and-how-does-mining-work/

Bitcoin Decentralized 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

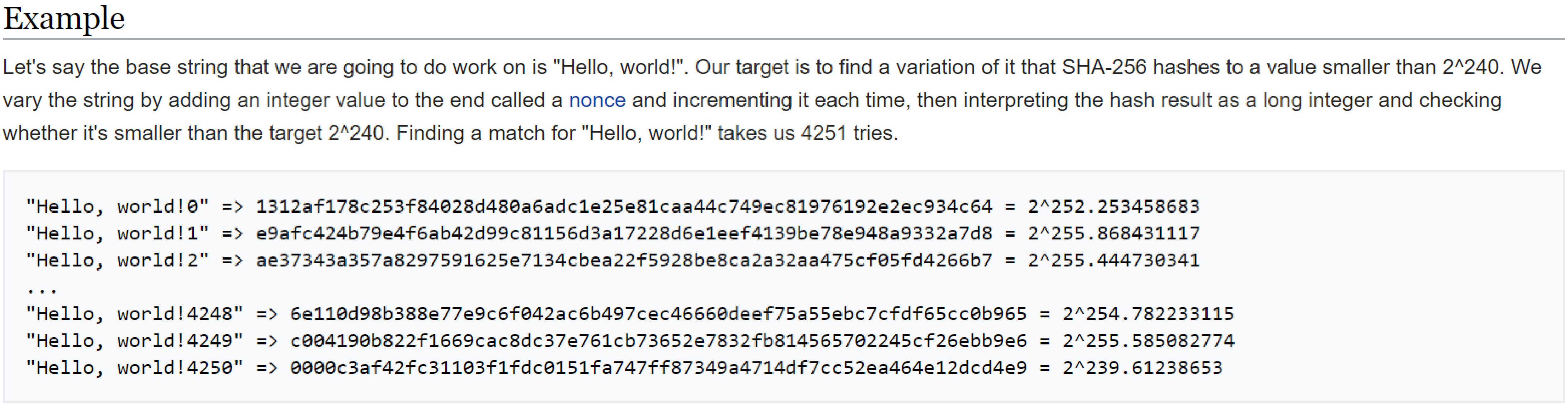
Bitcoin Decentralized Network

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

Bitcoin Decentralized Network

Proof of Work (PoW) – example



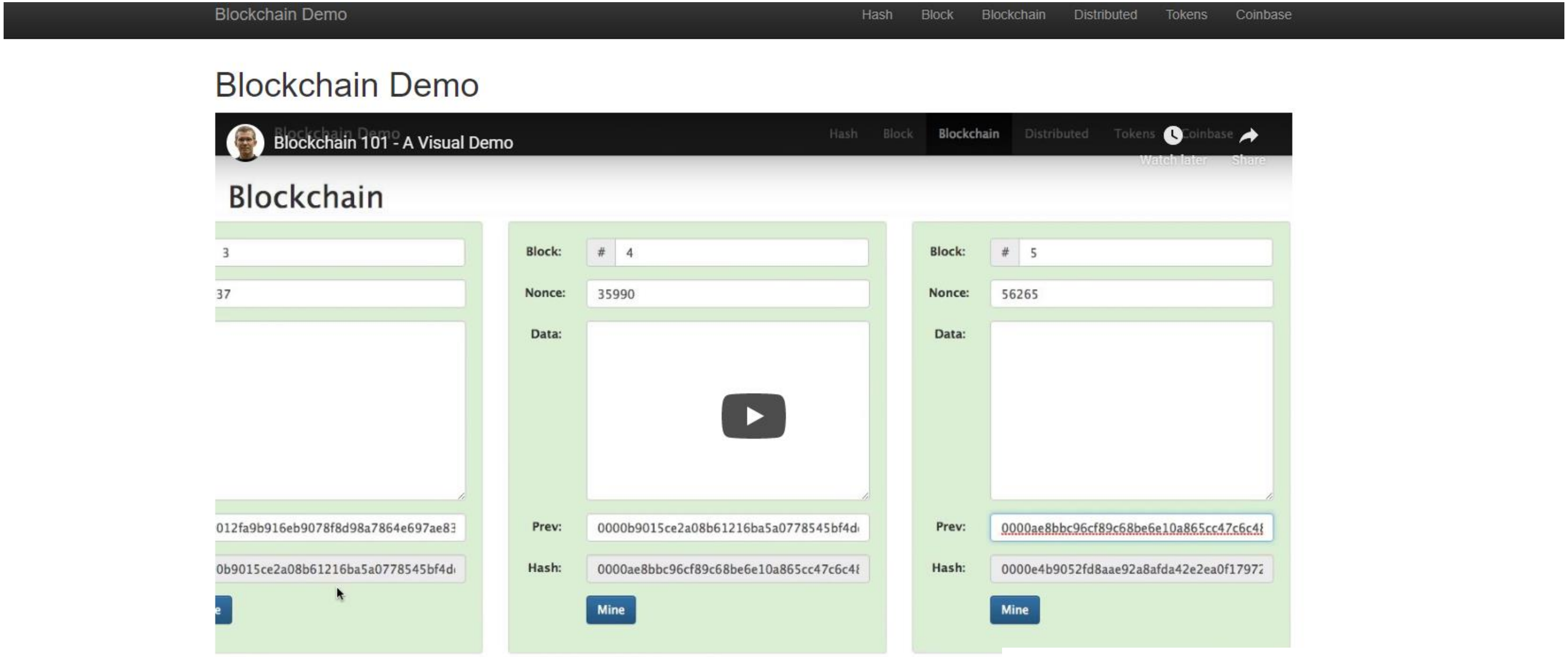
Example

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/

Blockchain Visual Demo



Blockchain Demo

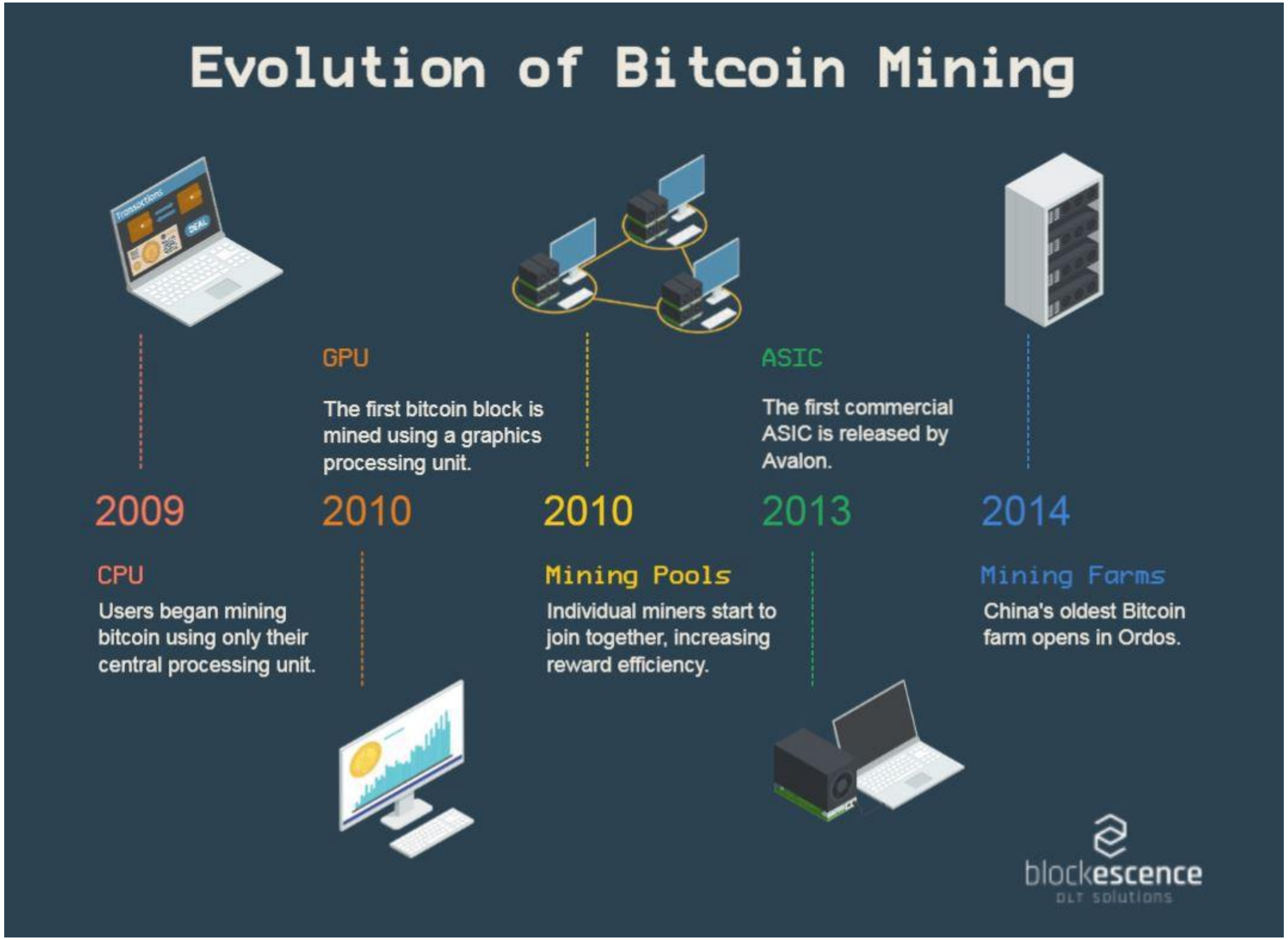
Blockchain

3
37
012fa9b916eb9078f8d98a7864e697ae83
0b9015ce2a08b61216ba5a0778545bf4d

Block: # 4
Nonce: 35990
Data:
Prev: 0000b9015ce2a08b61216ba5a0778545bf4d
Hash: 0000ae8bbc96cf89c68be6e10a865cc47c6c48

Block: # 5
Nonce: 56265
Data:
Prev: 0000ae8bbc96cf89c68be6e10a865cc47c6c48
Hash: 0000e4b9052fd8aae92a8afda42e2ea0f17972

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



Evolution of Bitcoin Mining

2009

CPU

Users began mining bitcoin using only their central processing unit.

2010

GPU

The first bitcoin block is mined using a graphics processing unit.

2010

Mining Pools

Individual miners start to join together, increasing reward efficiency.

2013

ASIC

The first commercial ASIC is released by Avalon.

2014

Mining Farms

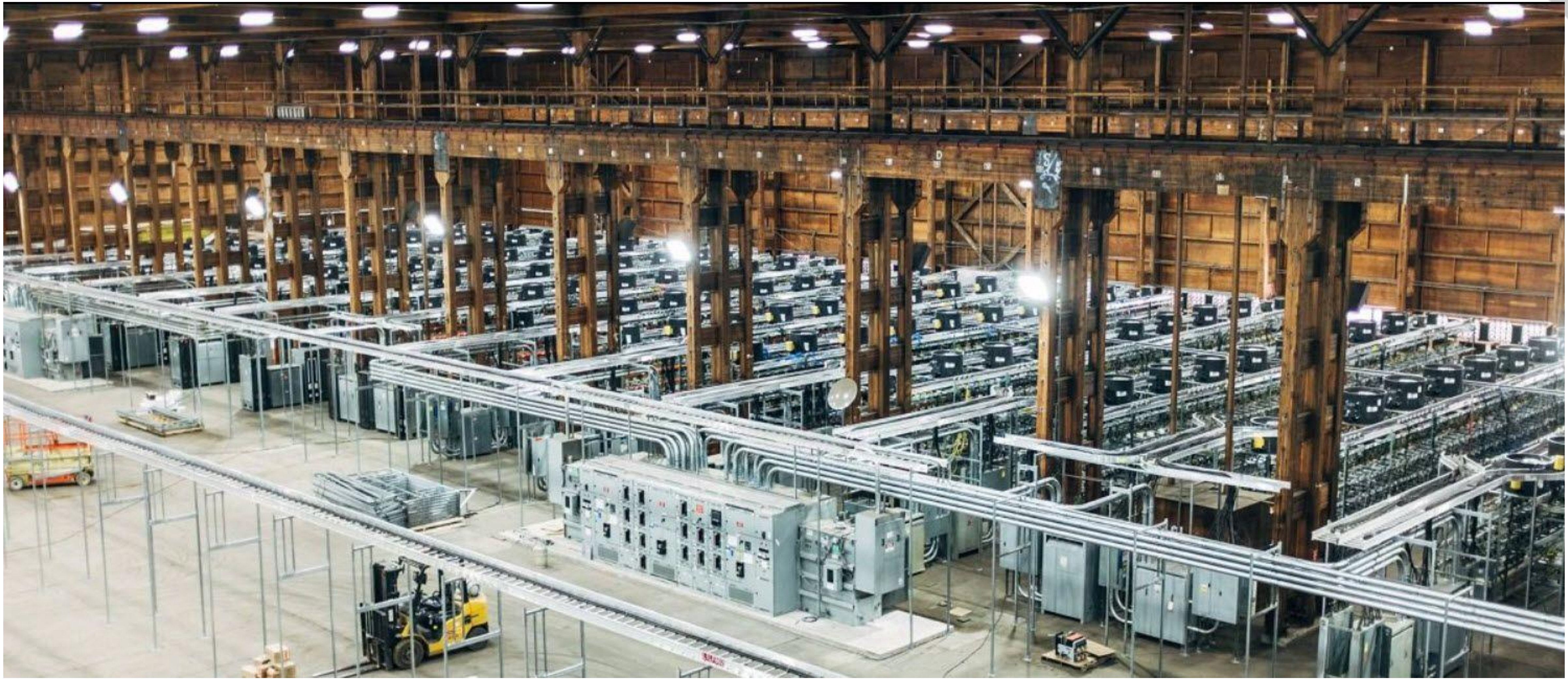
China's oldest Bitcoin farm opens in Ordos.

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

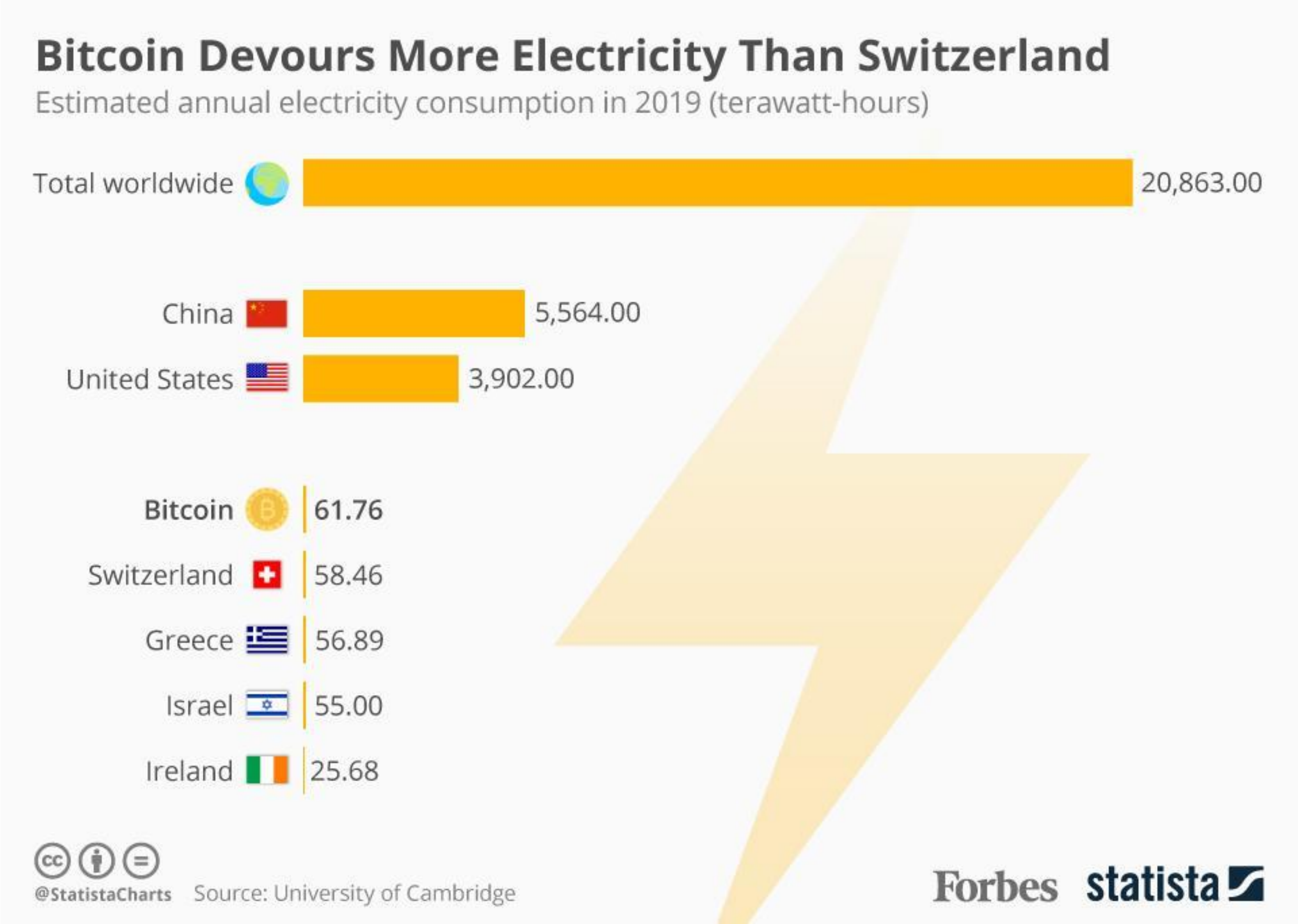
Bitcoin Decentralized Network

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



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



Bitcoin Devours More Electricity Than Switzerland

Estimated annual electricity consumption in 2019 (terawatt-hours)

Source: University of Cambridge

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

Bitcoin Decentralized Network

Mining in Detail

- **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

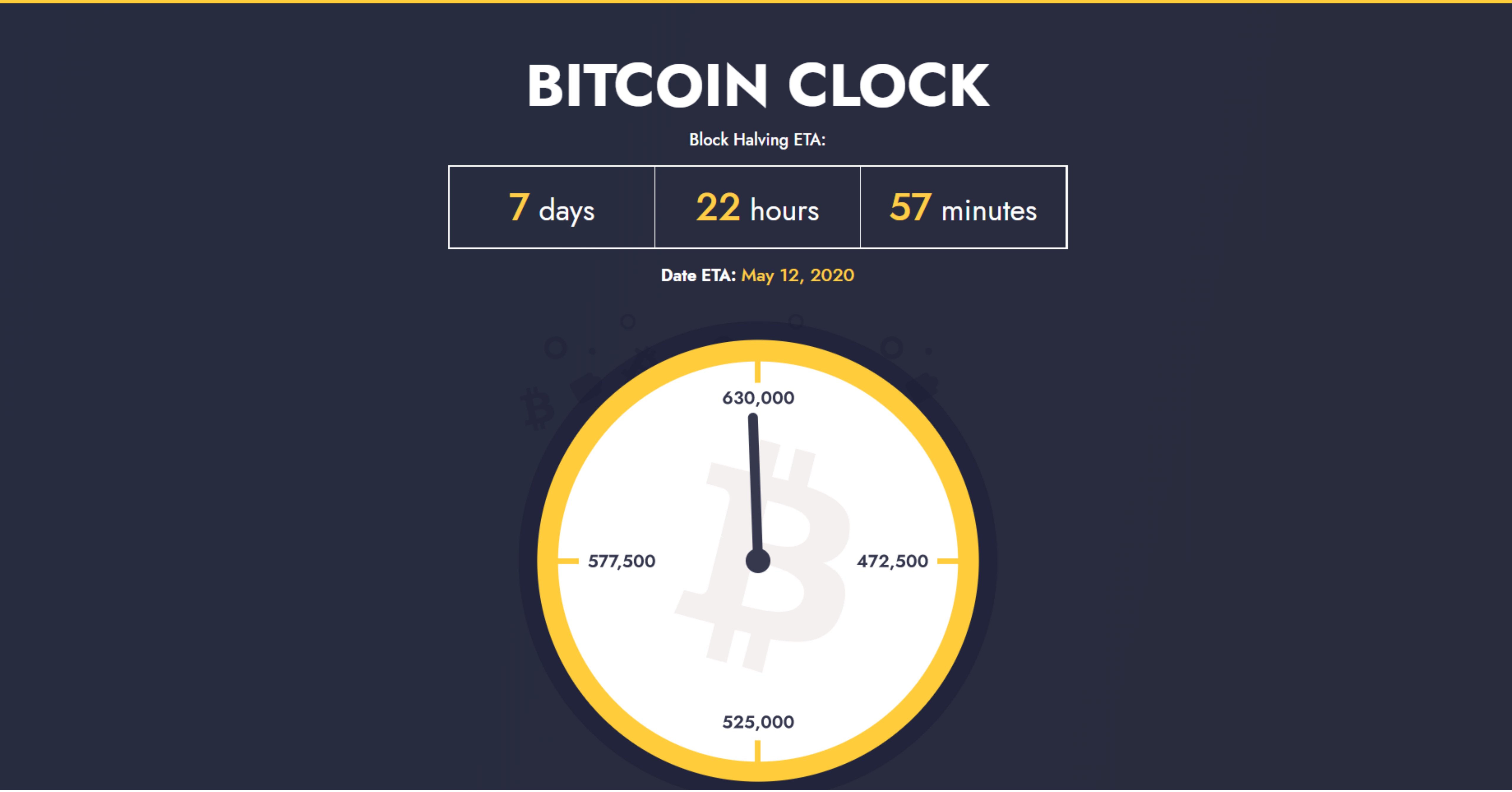
Question: Why would people mine bitcoin?

Answer: Incentive!

Bitcoin Decentralized Network

Mining Incentive

- **Mining incentive**
  - 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 (most likely on May 12)
    - …
  - there’re only 21 million bitcoins that can be mined/created
  - last bitcoin will be mined in 2140



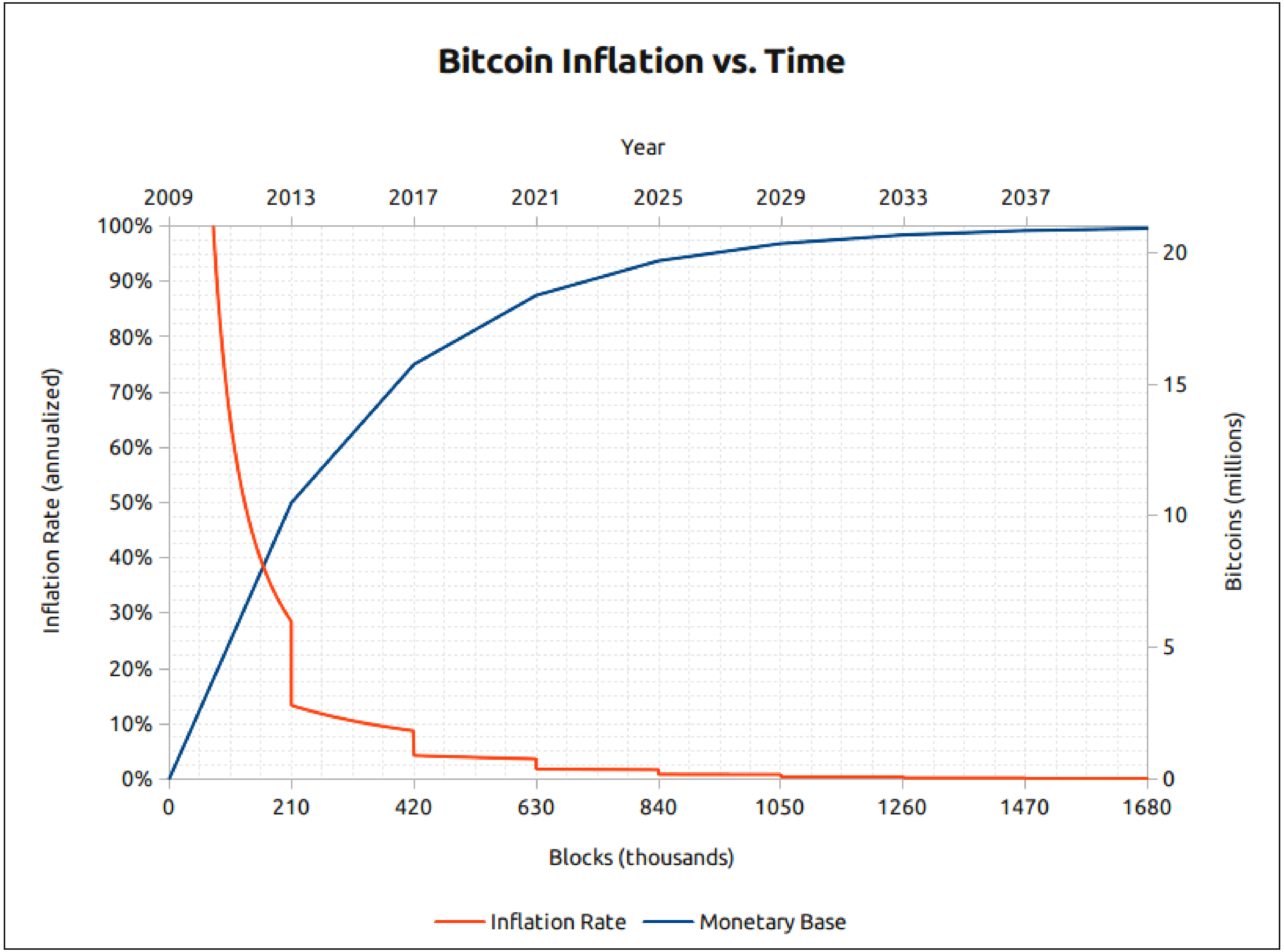
BITCOIN CLOCK

Block Halving ETA:

7 days	22 hours	57 minutes

Date ETA: May 12, 2020

Source: https://www.buybitcoinworldwide.com/bitcoin-clock/



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

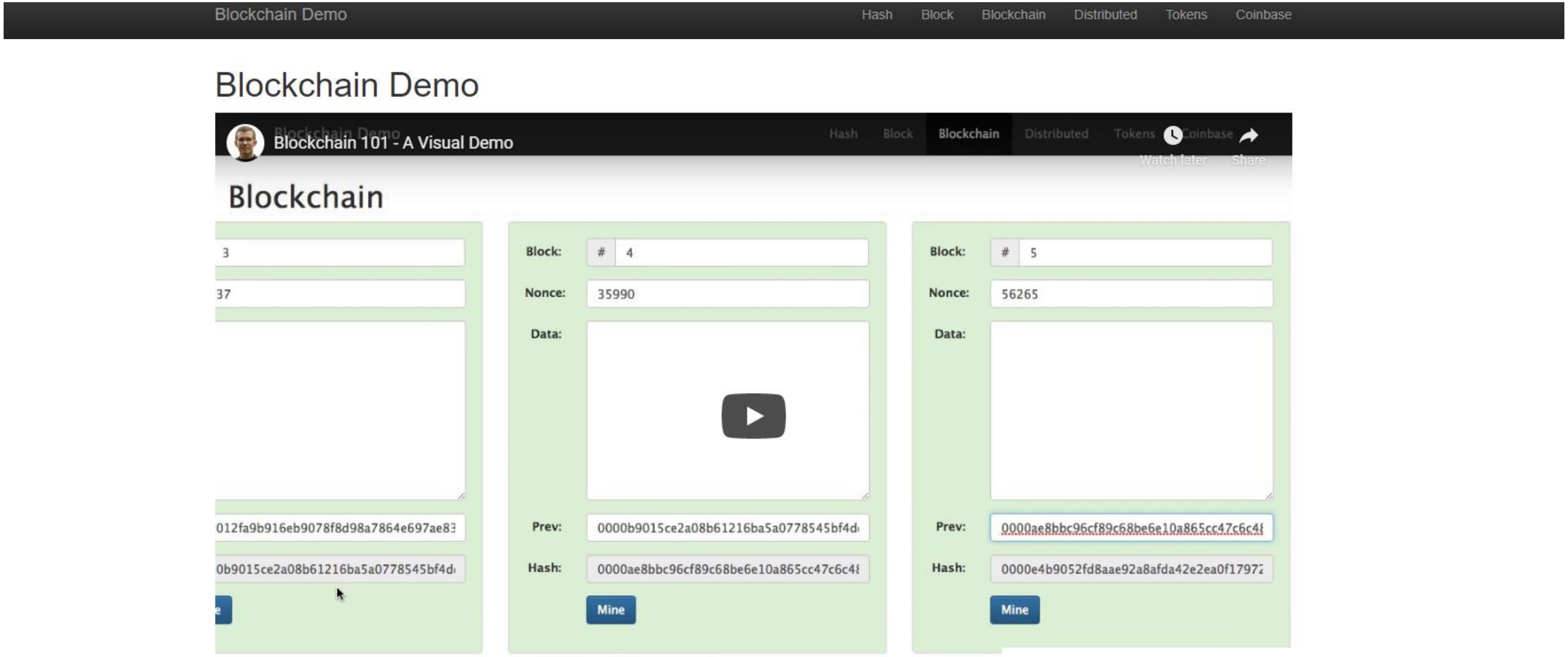
coindesk
NEWS
LEARN
RESEARCH
EVENTS
Bitcoin 24h $8,883.12 +0.33%
Ethereum 24h $204.66 -0.22%
XRP 24h $0.216365 -0.72%
Bitcoin Cash 24h $245.37 -0.02%
Bitcoin 101
06 How Bitcoin Mining Works

How Bitcoin Mining Works

Aug 20, 2013 at 20:59 UTC   Jan 31, 2018 at 17:35 UTC

Source: https://www.coindesk.com/learn/bitcoin-101/how-bitcoin-mining-works

Blockchain Visual Demo



Blockchain Demo

Blockchain

3
37
Data:
012fa9b916eb9078f8d98a7864e697ae83
0b9015ce2a08b61216ba5a0778545bf4d

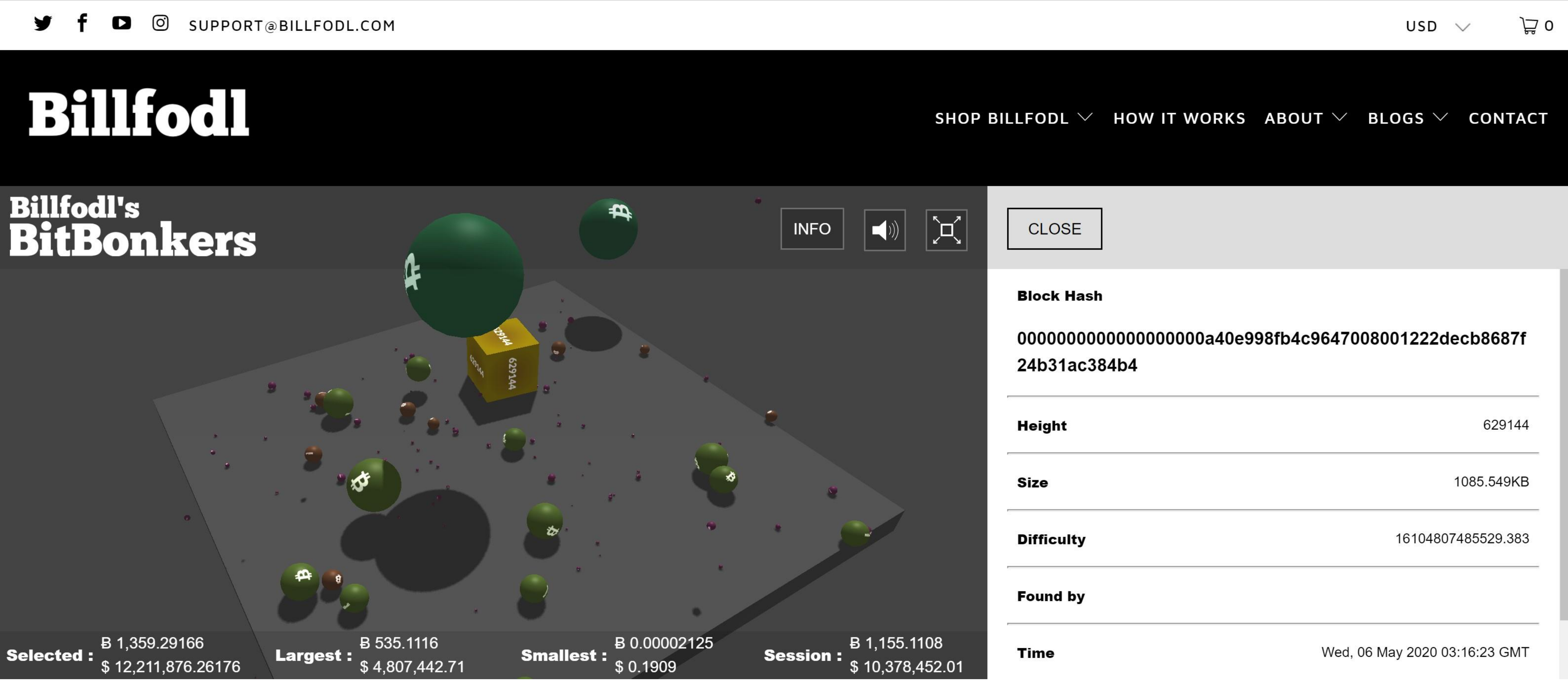
Block: # 4
Nonce: 35990
Data:
Prev: 0000b9015ce2a08b61216ba5a0778545bf4d
Hash: 0000ae8bbc96cf89c68be6e10a865cc47c6c4

Block: # 5
Nonce: 56265
Data:
Prev: 0000ae8bbc96cf89c68be6e10a865cc47c6c4
Hash: 0000e4b9052fd8aae92a8afda42e2ea0f1797

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

TIBA

Real-time Transaction Demo



SUPPORT@BILLFODL.COM

USD

0

Billfodl

SHOP BILLFODL HOW IT WORKS ABOUT BLOGS CONTACT

Billfodl's BitBonkers

INFO

CLOSE

Block Hash

0000000000000000000a40e998fb4c9647008001222decb8687f24b31ac384b4

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

Selected : Ƀ 1,359.29166 $ 12,211,876.26176

Largest : Ƀ 535.1116 $ 4,807,442.71

Smallest : Ƀ 0.00002125 $ 0.1909

Session : Ƀ 1,155.1108 $ 10,378,452.01

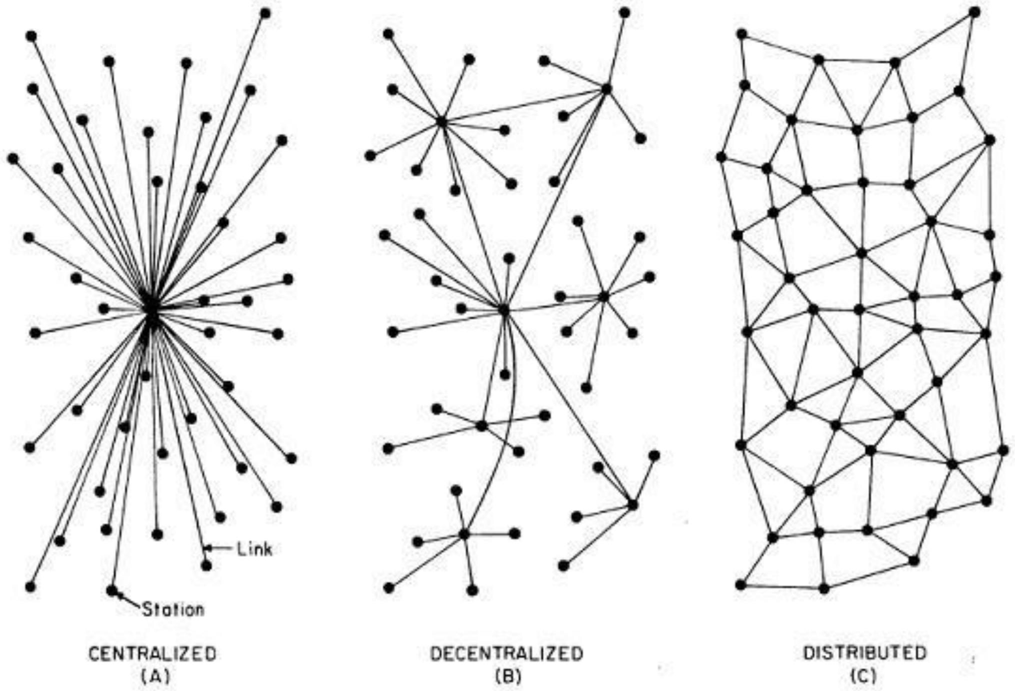
Source: https://billfodl.com/pages/bitbonkers

TIBA

Bitcoin Blockchain

Block & Chain

- **Bitcoin Blockchain** ==
  - Immutable Transaction Database
  - Decentralized Network
  - chain of blocks + chain of individual transactions
- **Core Value**:
  - 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

Thank you for listening!
See you again soon!

Questions?

TIBA

More Resources

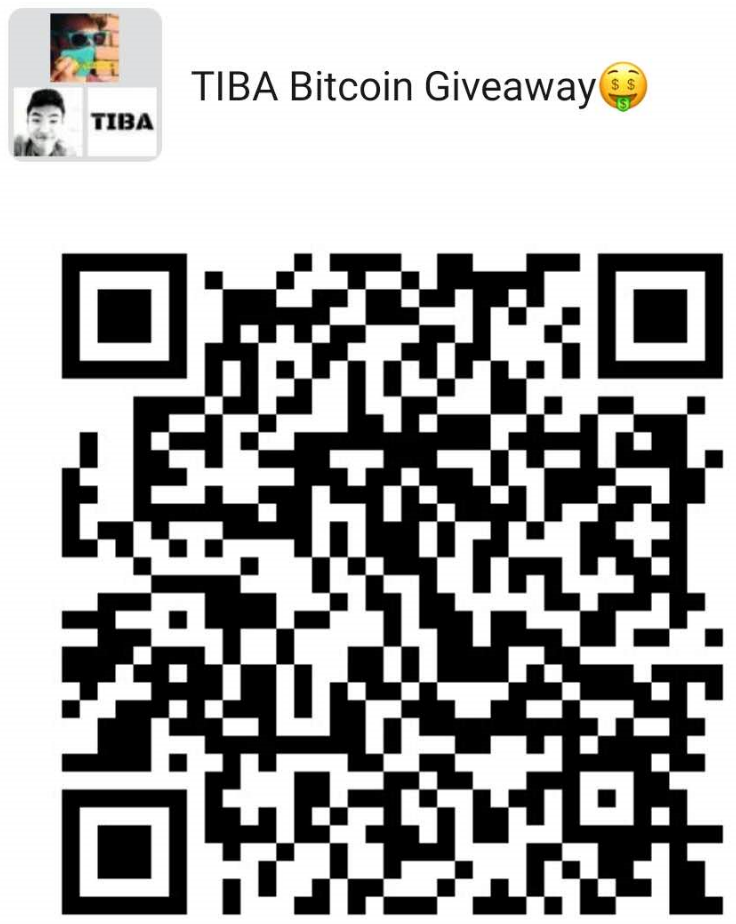
- Digital Gold by Nathaniel Popper
- Blockchain at Berkeley Fundamentals Decal by University of California, Berkeley
- Bitcoin and Cryptocurrency Technologies by Princeton University
- Blockchain & Money by Prof. Gary Gensler, MIT

TIBA

Bitcoin Giveaway!!

Thank you for joining!

- Steps:
  1. Join the group chat
  2. Install a wallet
  3. Post your bitcoin address in the chat
  4. Enjoy your bitcoins!

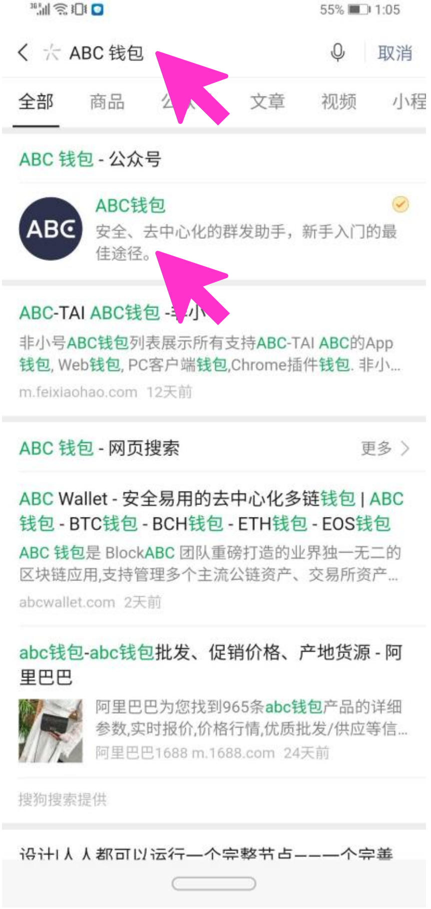


TIBA Bitcoin Giveaway🤑

TIBA

Bitcoin Giveaway!!

Installing Wallet



55% 1:05

ABC 钱包 取消

全部 商品 公 文章 视频 小程

ABC 钱包 - 公众号

ABC钱包
安全、去中心化的群发助手，新手入门的最佳途径。

ABC-TAI ABC钱包 - 非小
非小号ABC钱包列表展示所有支持ABC-TAI ABC的App钱包, Web钱包, PC客户端钱包,Chrome插件钱包. 非小...
m.feixiaohao.com 12天前

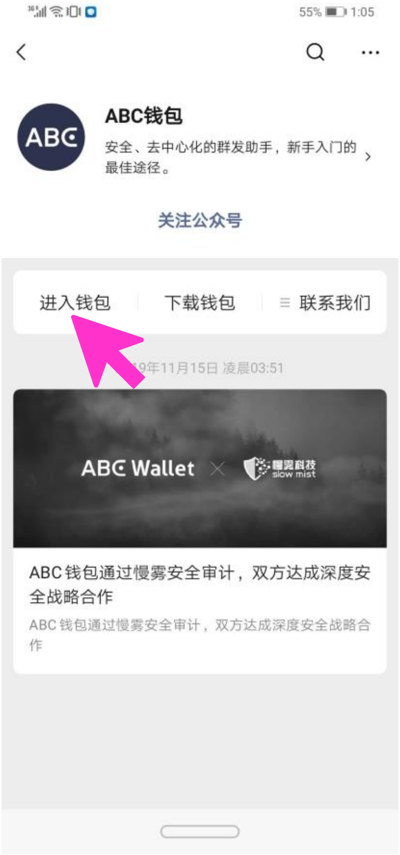
ABC 钱包 - 网页搜索 更多 >

ABC Wallet - 安全易用的去中心化多链钱包 | ABC钱包 - BTC钱包 - BCH钱包 - ETH钱包 - EOS钱包
ABC 钱包是 BlockABC 团队重磅打造的业界独一无二的区块链应用,支持管理多个主流公链资产、交易所资产...
abcwallet.com 2天前

abc钱包-abc钱包批发、促销价格、产地货源 - 阿里巴巴
阿里巴巴为您找到965条abc钱包产品的详细参数,实时报价,价格行情,优质批发/供应等信...
阿里巴巴1688 m.1688.com 24天前

搜狗搜索提供

设计|人人都可以运行一个完整节点——一个完善



55% 1:05

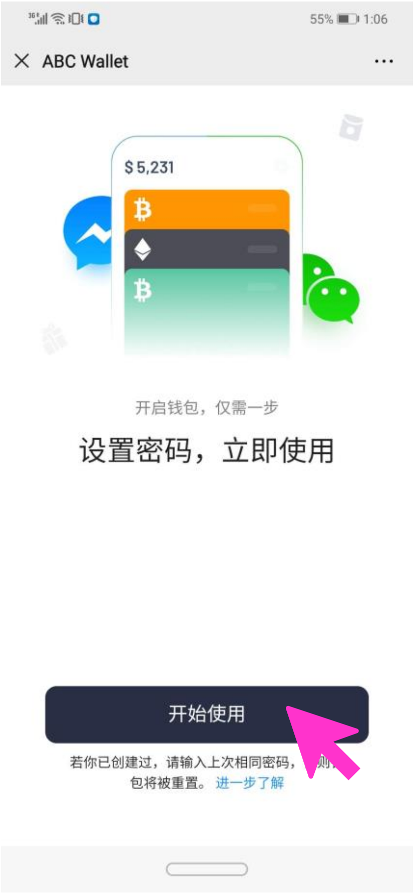
ABC钱包
安全、去中心化的群发助手，新手入门的最佳途径。 >

关注公众号

进入钱包 下载钱包 ≡ 联系我们

19年11月15日 凌晨03:51

ABC 钱包通过慢雾安全审计，双方达成深度安全战略合作
ABC 钱包通过慢雾安全审计，双方达成深度安全战略合作



55% 1:06

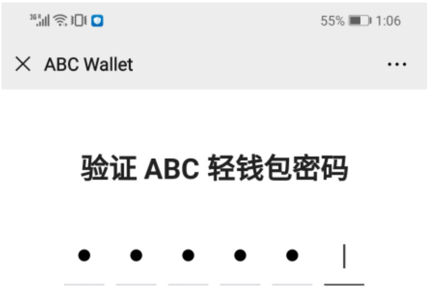
× ABC Wallet ···

开启钱包，仅需一步

设置密码，立即使用

开始使用

若你已创建过，请输入上次相同密码，则包将被重置。 进一步了解

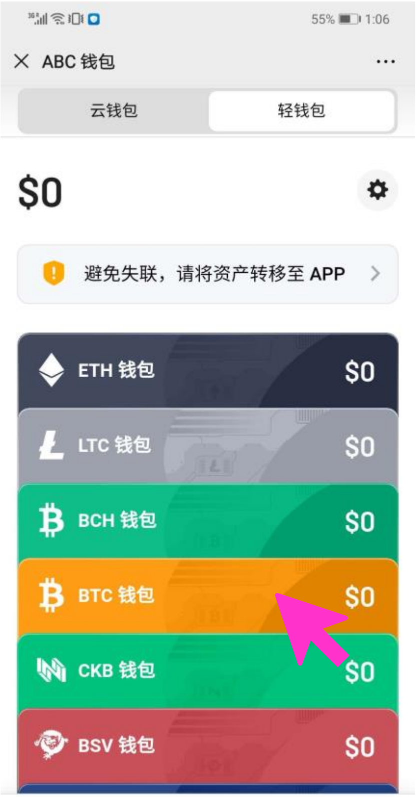


55% 1:06

× ABC Wallet ···

验证 ABC 轻钱包密码

● ● ● ● ●



55% 1:06

× ABC 钱包 ···

云钱包 轻钱包

$0

避免失联，请将资产转移至 APP >

ETH 钱包 $0

LTC 钱包 $0

BCH 钱包 $0

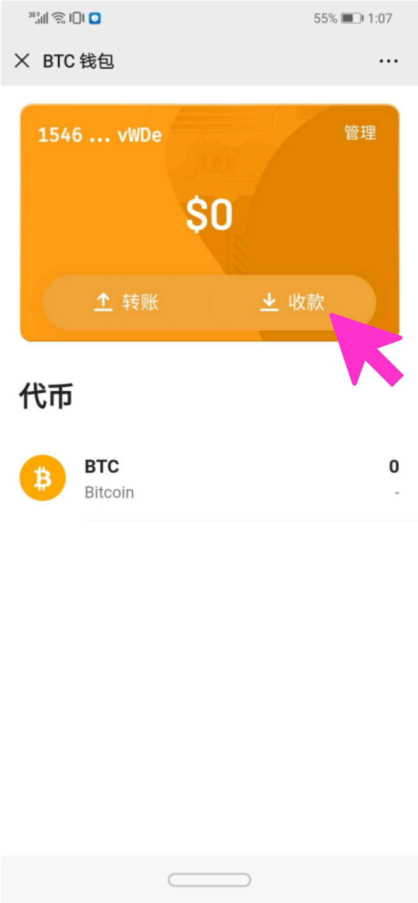
BTC 钱包 $0

CKB 钱包 $0

BSV 钱包 $0

Bitcoin Giveaway!!

Installing Wallet



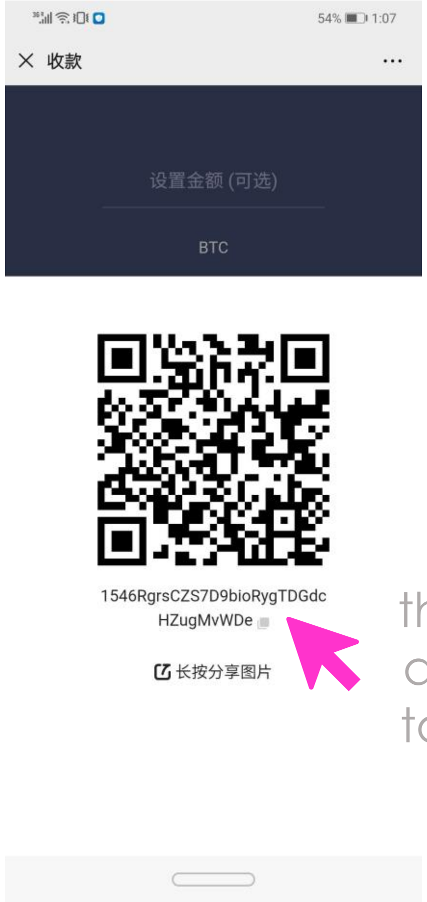
BTC 钱包

1546 ... vWDe

$0

代币

BTC Bitcoin	0 -



收款

设置金额 (可选)

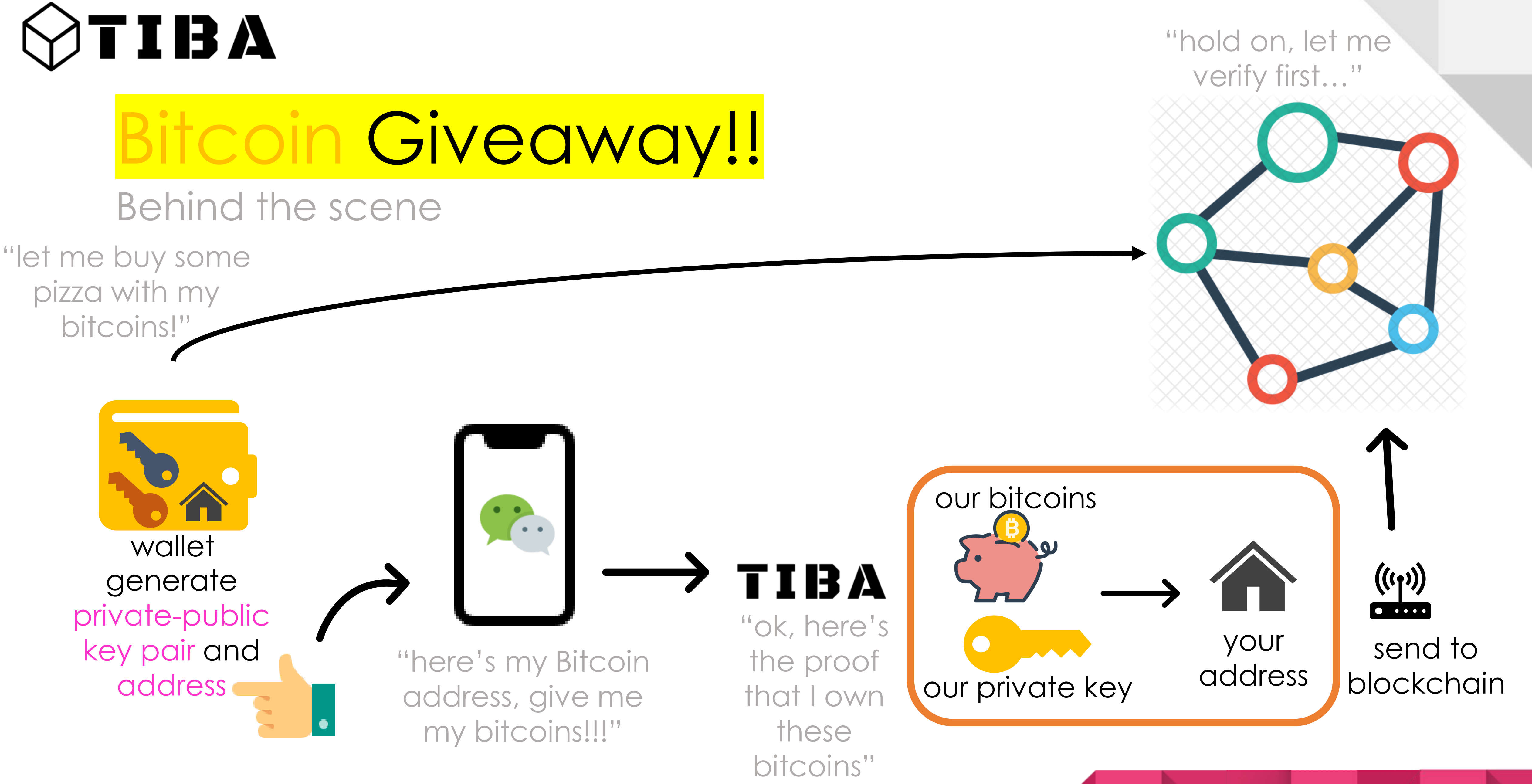
BTC

1546RgrsCZS7D9bioRygTDGdc
HZugMvWDe

that’s your bitcoin address, send this to the group chat

Bitcoin Giveaway!!

Behind the scene



"hold on, let me verify first..."

"let me buy some pizza with my bitcoins!"

wallet generate private-public key pair and address

"here's my Bitcoin address, give me my bitcoins!!!"

TIBA

"ok, here's the proof that I own these bitcoins"

our bitcoins

our private key

your address

send to blockchain