Bitcoin: A Peer-to-peer electronic cash system

BITCOIN DIGITAL CRYPTOCURRENCY
BITCOIN DIGITAL CRYPTOCURRENCY

Author: Satoshi Nakamoto

- Presented by: Kartikeya Agarwal

- Future of freely moving currency?

- Or a digital entity of questionable value and dubious origin?

History of Bitcoin

- 2008: The Bitcoin paper was first posted to a mailing list on cryptography by someone under the pseudonym Satoshi Nakamoto.

- 2009: The mining process through which new Bitcoins are created ‘begins’.

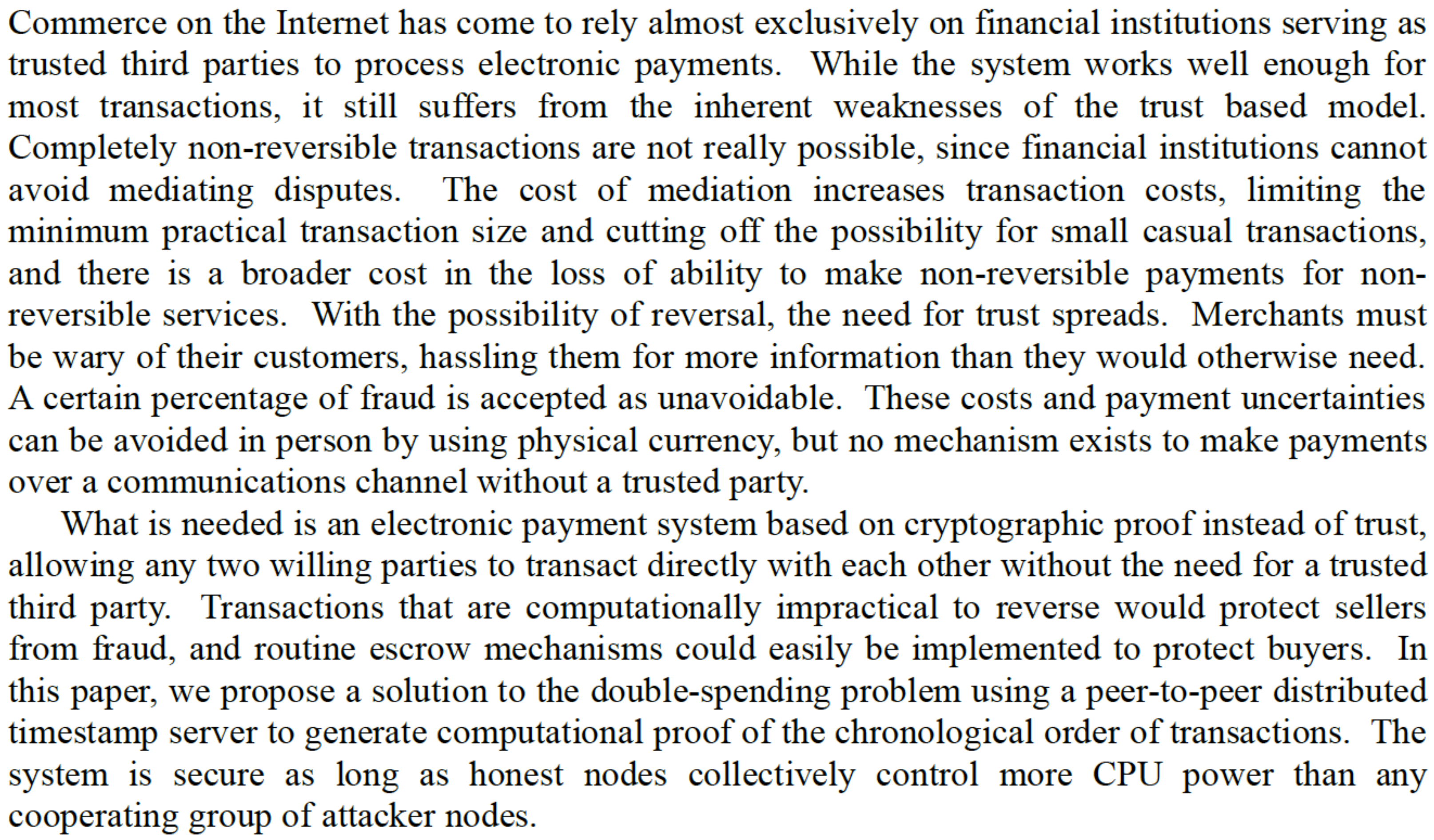
- 2010: Bitcoin was priced for the first time. Someone used 10,000 BTC to buy 2 pizzas.

- 2014: The largest Bitcoin exchange by the name of Mt. Gox went offline and 850,000 bitcoins were stolen.

- 2016: Rise of Ethereum and ICOs.

- 2017: Price of Bitcoin fizzles out a little after reaching an all time high of $19,783.

Introduction



Commerce on the Internet has come to rely almost exclusively on financial institutions serving as trusted third parties to process electronic payments. While the system works well enough for most transactions, it still suffers from the inherent weaknesses of the trust based model. Completely non-reversible transactions are not really possible, since financial institutions cannot avoid mediating disputes. The cost of mediation increases transaction costs, limiting the minimum practical transaction size and cutting off the possibility for small casual transactions, and there is a broader cost in the loss of ability to make non-reversible payments for non-reversible services. With the possibility of reversal, the need for trust spreads. Merchants must be wary of their customers, hassling them for more information than they would otherwise need. A certain percentage of fraud is accepted as unavoidable. These costs and payment uncertainties can be avoided in person by using physical currency, but no mechanism exists to make payments over a communications channel without a trusted party.

What is needed is an electronic payment system based on cryptographic proof instead of trust, allowing any two willing parties to transact directly with each other without the need for a trusted third party. Transactions that are computationally impractical to reverse would protect sellers from fraud, and routine escrow mechanisms could easily be implemented to protect buyers. In this paper, we propose a solution to the double-spending problem using a peer-to-peer distributed timestamp server to generate computational proof of the chronological order of transactions. The system is secure as long as honest nodes collectively control more CPU power than any cooperating group of attacker nodes.

Mechanics of Bitcoin

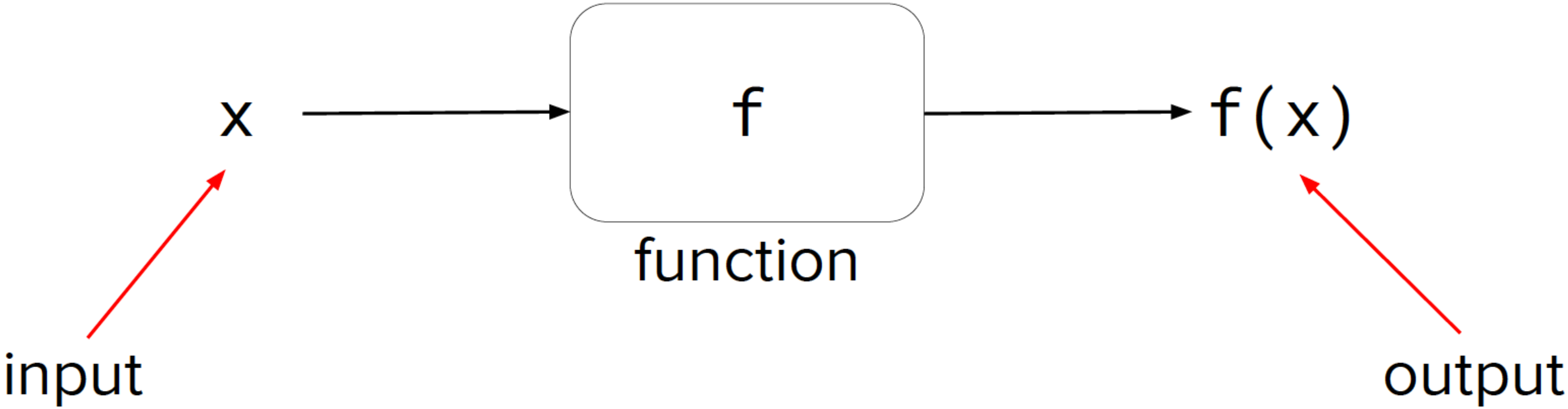
- How does it work?
- Incentives/disincentives?
- Changes?

Cryptographic Hash Function

- Its input can be any string of any size.

- It produces a fixed size output. In our case, it means 256-bit.

- It is efficiently computable.



x

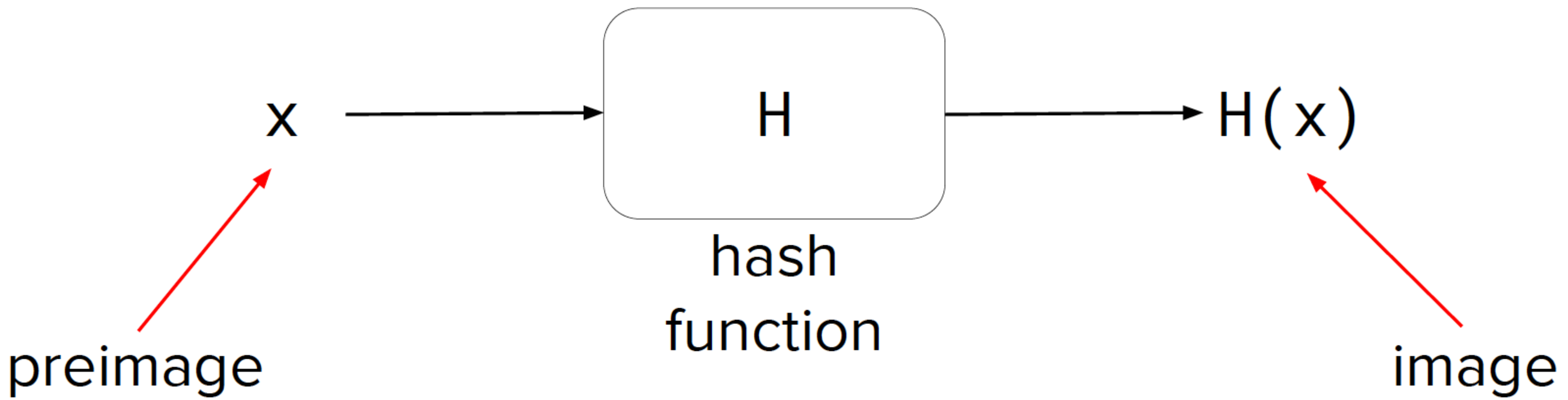
f

f(x)

function

input

output



x

H

H(x)

hash function

preimage

image

```
"Hello, world!" | sha256sum
```

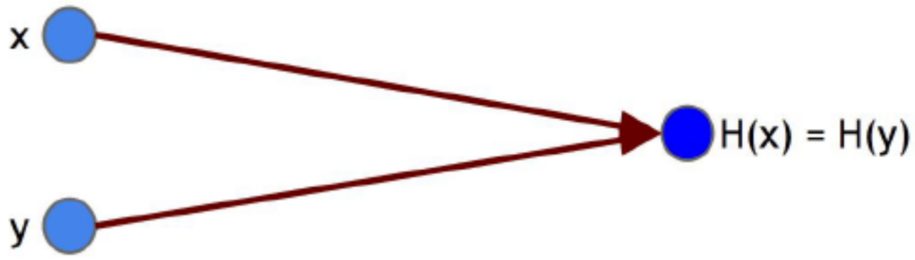
```
0xd9014c4624844aa5bac31
4773d6b689ad467fa4e1d1a
50a1b8a99d5a95f72ff5
```

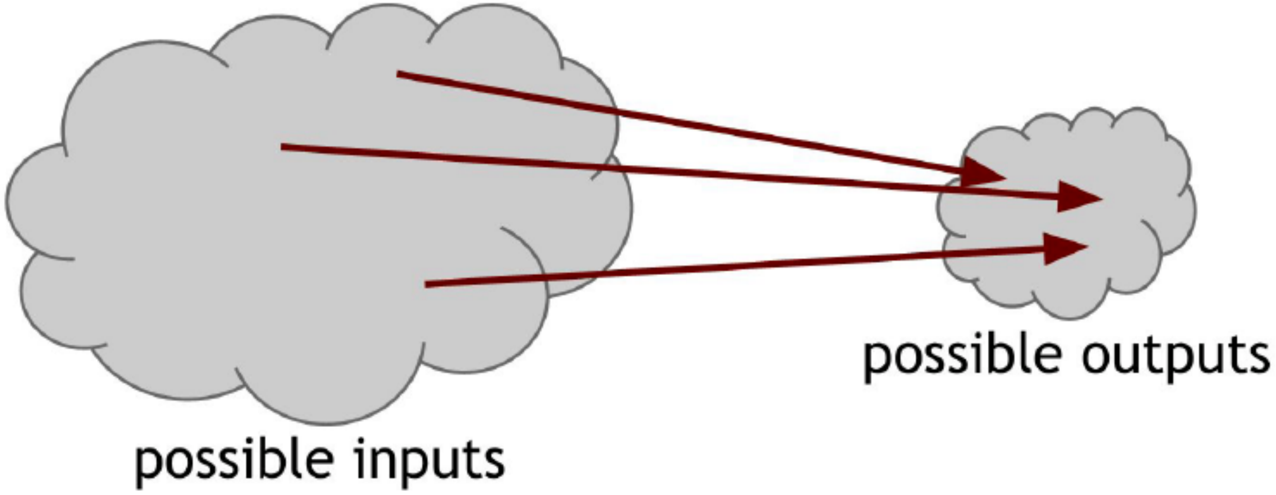
Three Important Properties

- Collision Resistant
- Hiding
- Puzzle-friendliness

Collision Resistant

- It is computationally difficult to find x and y such that H(x) == H(y).
- Fingerprint Analogy: Can you find 2 random people with the same fingerprint?





- Because the number of inputs exceeds the number of outputs, we are guaranteed that there must be at least one output to which the hash function maps more than one input.

What’s the catch?

- If a computer calculates 10,000 hashes per second, it would take more than one octillion (10^27) years to calculate 2^128 hashes!

Hiding

- Given H(x), there’s no feasible way to figure out what is ‘x’.

- Fingerprint Analogy: Whose fingerprint is it?

Puzzle Friendliness

- Given x, it is computationally difficult to find some value x’ such that H(x) == H(x’).

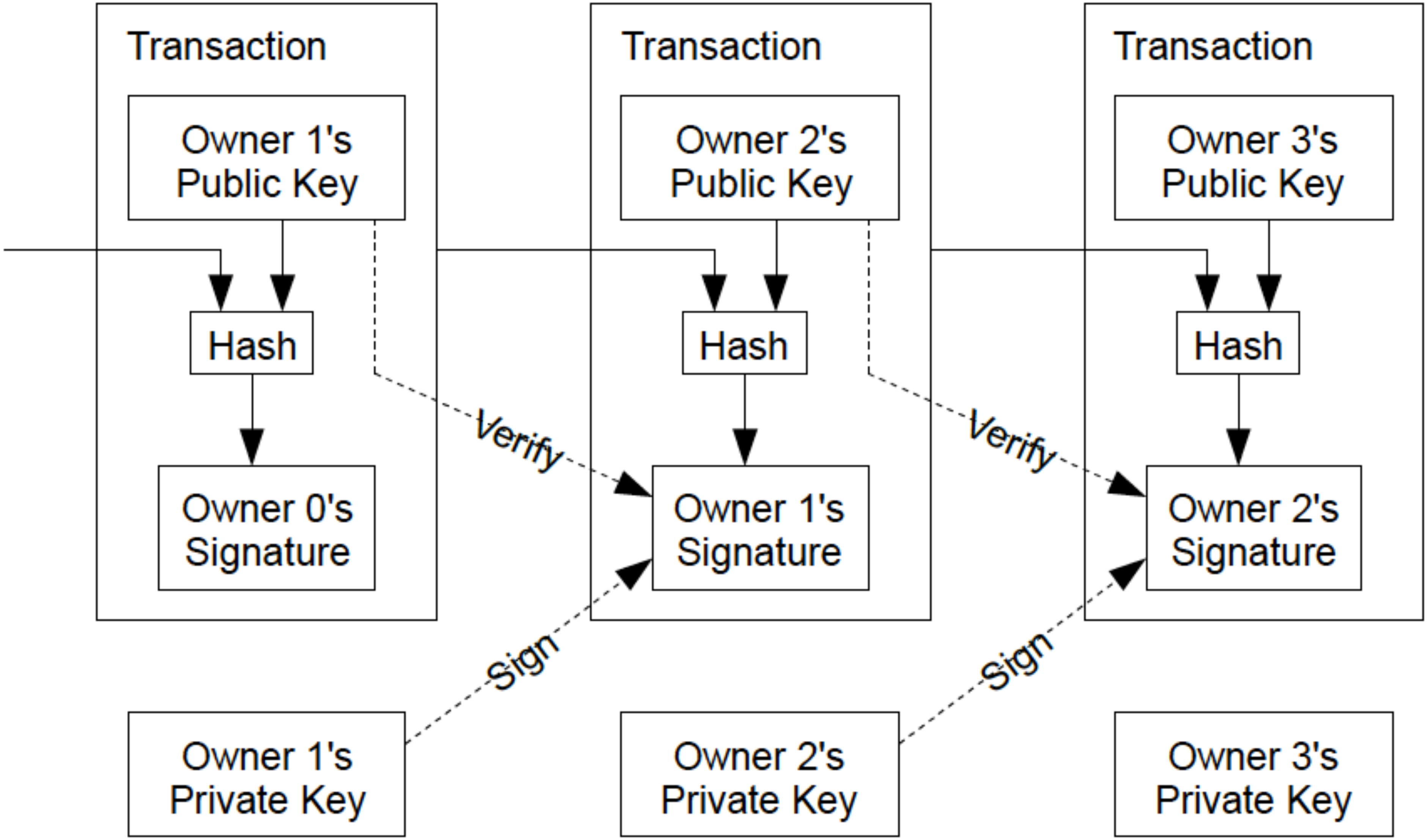
- Fingerprint Analogy: Can you find someone with the same fingerprint as you?

Transactions

- Electronic coin is defined as a chain of digital signatures.

- Each owner transfers the coin to the next by digitally signing a hash of the previous transaction and the public key of the next owner and adding these two the end of the coin.

- A payee can verify the signatures to verify the chain of ownership.


Transaction
Owner 1's Public Key
Hash
Owner 0's Signature
Transaction
Owner 2's Public Key
Hash
Owner 1's Signature
Transaction
Owner 3's Public Key
Hash
Owner 2's Signature
Verify
Verify
Sign
Sign
Owner 1's Private Key
Owner 2's Private Key
Owner 3's Private Key

- Payee can't verify that one of the owners did not double-spend the coin.

- We need a way for the payee to know that the previous owners did not sign any earlier transactions.

- The only way to confirm the absence of a transaction is to be aware of all transactions.

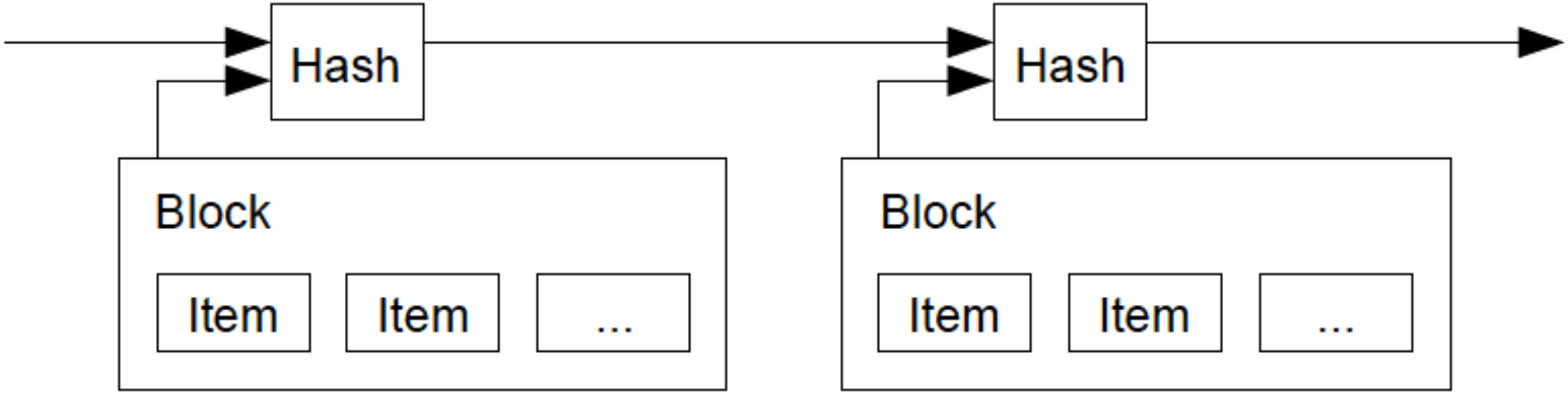
- To accomplish this without a trusted party, transactions must be publicly announced, and we need a system for participants to agree on a single history of the order in which they were received. The payee needs proof that at the time of each transaction, the majority of nodes agreed it was the first received.

Timestamp Server

- Takes a hash of a block of items to be timestamped and widely publishes the hash.

- Each timestamp includes the previous timestamp in its hash, forming a chain, with each additional timestamp reinforcing the ones before it.

- The timestamp proves that the data must have existed at the time, obviously, in order to get into the hash.


Hash
Hash
Block
Item
Item
...
Block
Item
Item
...

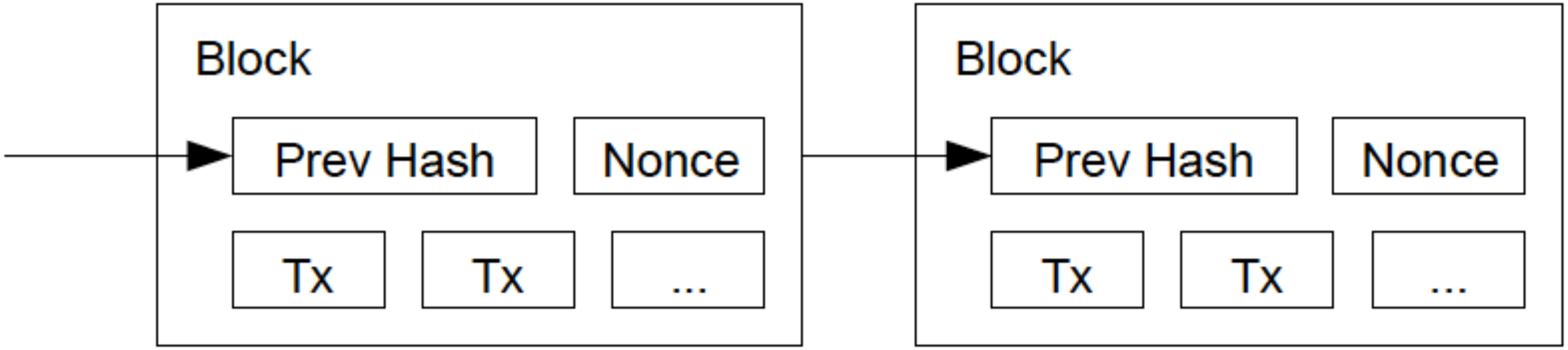
Proof of Work

- The proof-of-work involves scanning for a value that when hashed, such as with SHA-256, the hash begins with a number of zero bits.

- The average work required is exponential in the number of zero bits required and can be verified by executing a single hash.

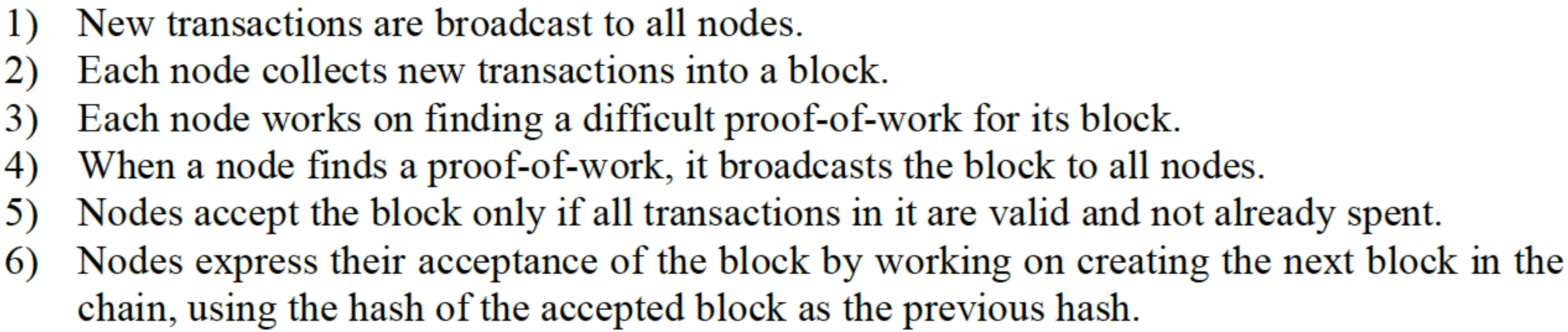
- For our timestamp network, we implement the proof-of-work by incrementing a nonce in the block until a value is found that gives the block's hash the required zero bits.

- Once the CPU effort has been expended to make it satisfy the proof-of-work, the block cannot be changed without redoing the work. As later blocks are chained after it, the work to change the block would include redoing all the blocks after it.



- Proof of work is essentially one CPU-one vote.

Network



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

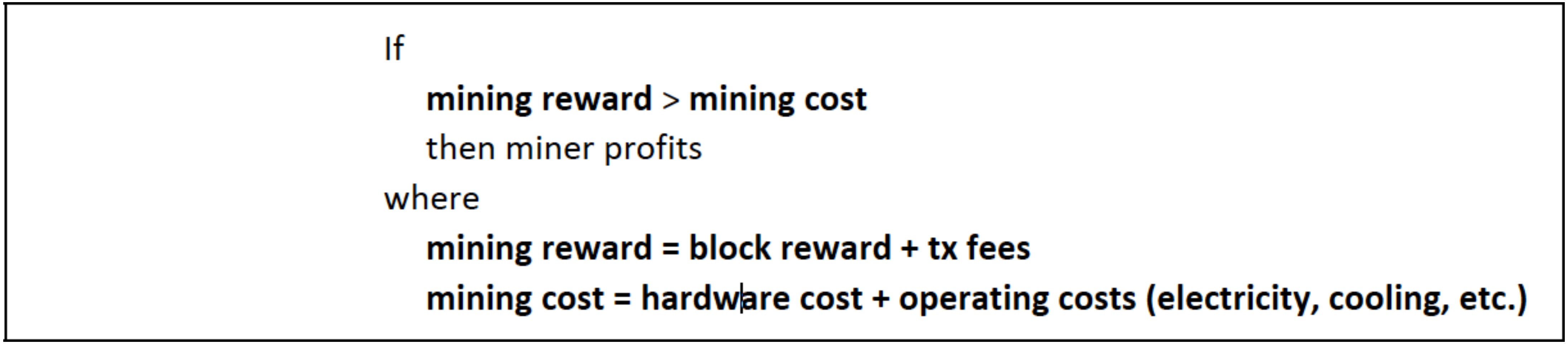
Incentive

- The first transaction in a block is a special transaction that starts a new coin owned by the creator of the block.

- The steady addition of a constant of amount of new coins is analogous to gold miners expending resources to add gold to circulation.

- Once a predetermined number of coins have entered circulation, the incentive can transition entirely to transaction fees and be completely inflation free.

Cost of Mining



If

mining reward > **mining cost**

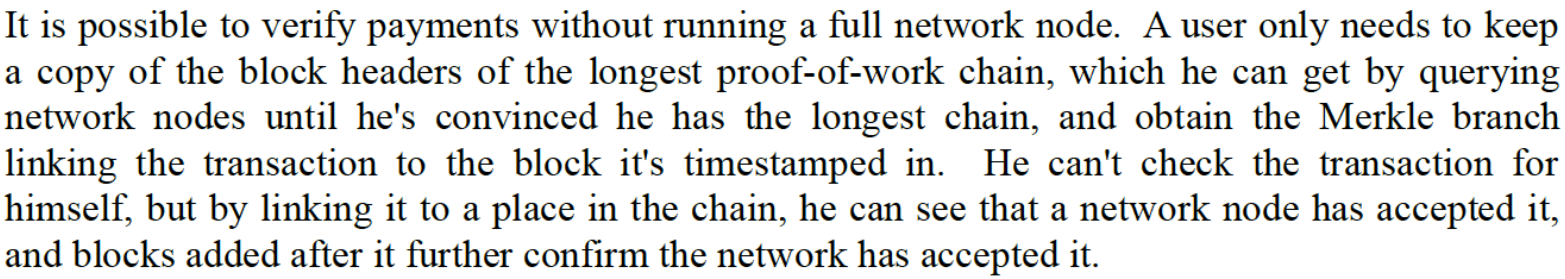
then miner profits

where

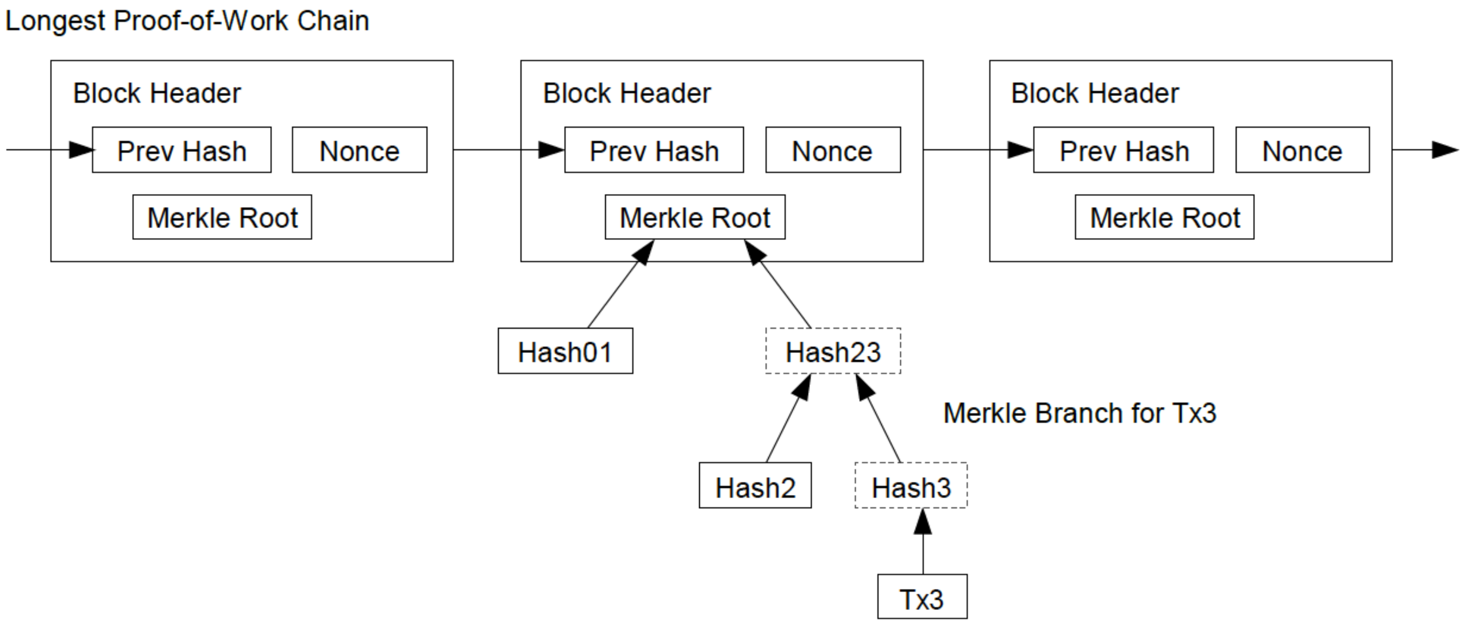
mining reward = block reward + tx fees

mining cost = hardware cost + operating costs (electricity, cooling, etc.)

Simplified Payment Verification



It is possible to verify payments without running a full network node. A user only needs to keep a copy of the block headers of the longest proof-of-work chain, which he can get by querying network nodes until he's convinced he has the longest chain, and obtain the Merkle branch linking the transaction to the block it's timestamped in. He can't check the transaction for himself, but by linking it to a place in the chain, he can see that a network node has accepted it, and blocks added after it further confirm the network has accepted it.

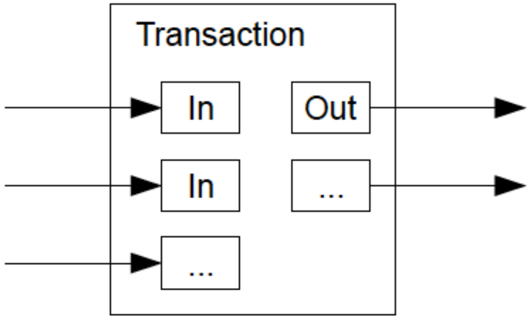


- Verification is reliable as long as honest nodes control the network, but is more vulnerable if the network is overpowered by an attacker.

- Businesses that receive frequent payments will probably still want to run their own nodes for more independent security and quicker verification.

Combining and Splitting Value

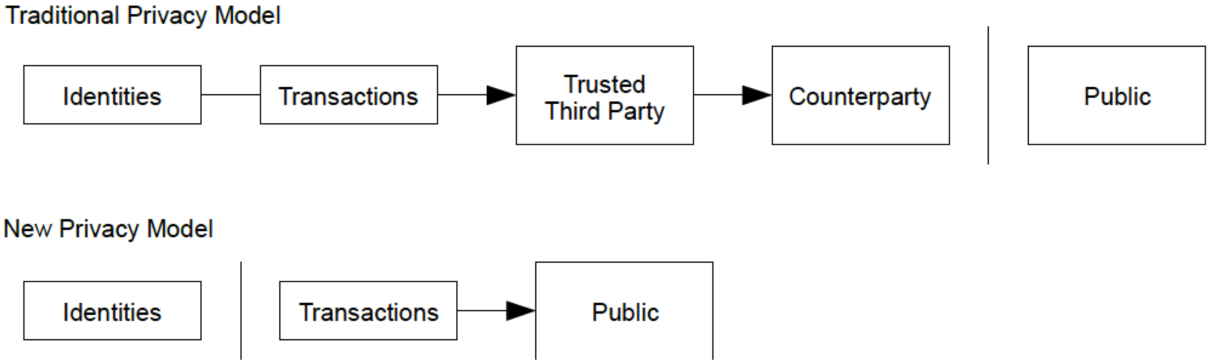
Although it would be possible to handle coins individually, it would be unwieldy to make a separate transaction for every cent in a transfer. To allow value to be split and combined, transactions contain multiple inputs and outputs. Normally there will be either a single input from a larger previous transaction or multiple inputs combining smaller amounts, and at most two outputs: one for the payment, and one returning the change, if any, back to the sender.



It should be noted that fan-out, where a transaction depends on several transactions, and those transactions depend on many more, is not a problem here. There is never the need to extract a complete standalone copy of a transaction's history.

Privacy

The traditional banking model achieves a level of privacy by limiting access to information to the parties involved and the trusted third party. The necessity to announce all transactions publicly precludes this method, but privacy can still be maintained by breaking the flow of information in another place: by keeping public keys anonymous. The public can see that someone is sending an amount to someone else, but without information linking the transaction to anyone. This is similar to the level of information released by stock exchanges, where the time and size of individual trades, the "tape", is made public, but without telling who the parties were.



As an additional firewall, a new key pair should be used for each transaction to keep them from being linked to a common owner. Some linking is still unavoidable with multi-input transactions, which necessarily reveal that their inputs were owned by the same owner. The risk is that if the owner of a key is revealed, linking could reveal other transactions that belonged to the same owner.

Is it fixed?

- Right now, Bitcoin’s supply is capped at 21 million Bitcoins.
- As of January 2018, there are 16.7 million Bitcoins ‘available’.
- Is that number set in stone?

A Tale of Two Narratives: Money vs Tech Crypto

- **Money Crypto:** Maintains that the point of cryptocurrency is to redefine how money works by (re-)introducing Sound Money.(Bitcoin Maximalism)

- **Tech Crypto:** Another belief system holds that the real point is to redefine how the internet works by introducing Web 3.0.(Ethereum Maximalism)

Money Crypto

- Sound money:

1)Has either fixed supply or predictable inflation rate.

2) Doesn’t appreciate quickly, and

3) Most importantly, can’t be controlled by governments via inflation or confiscation.

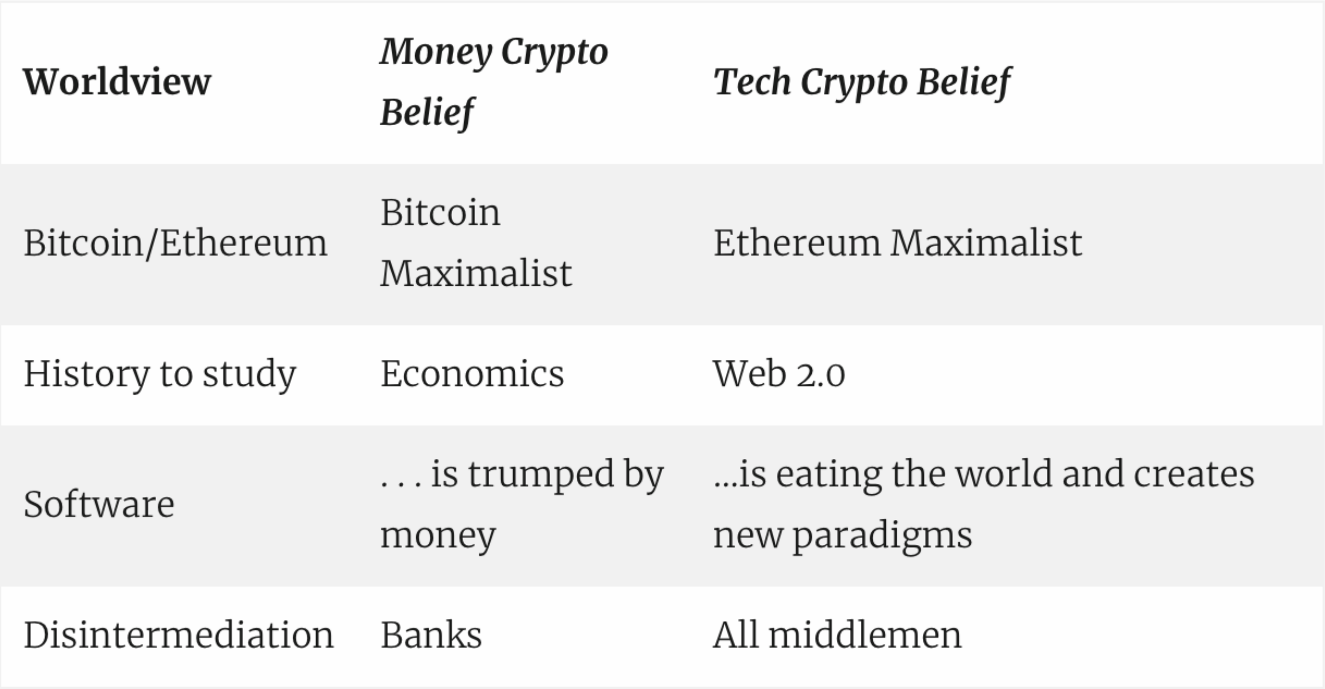
Tech Crypto

- Believes:

1. We should study history of the internet and its power structures.

2. Natural progression from a decentralized & open system to becoming centralized and concentrated. (Outcome vs opportunity)

Which narrative is right?



Worldview	***Money Crypto Belief***	***Tech Crypto Belief***
Bitcoin/Ethereum	Bitcoin Maximalist	Ethereum Maximalist
History to study	Economics	Web 2.0
Software	. . . is trumped by money	...is eating the world and creates new paradigms
Disintermediation	Banks	All middlemen

Decentralization: Fact or fiction?

- There is no ‘central’ authority like a central bank when it comes to Bitcoin. But, even with a decentralized structure, is there any advantage of the decentralization.

- I don’t think so.

- The way Bitcoin is mined is also subject to changes and the final decisions will rest in the hands of the largest miners.

- There is no guarantee that these Bitcoin miners will not influence the system to disproportionately benefit themselves in the future. The reward for mining is in proportion to the hash power available to Bitcoin miners. So, it is, in essence, not decentralized after all.

- In other words, there is just a shifting of the power dynamics from those controlling governments to those controlling computing power.

How has/will Bitcoin(and crypto) changed the landscape?

- Disrupting Venture Capital
- Disrupting Adjacent Fund Raising Institutions
- Disrupting Central Banks(also what I consider to be Bitcoin's biggest challenge/acid test)
- There is a reason every country in the world uses fiat currency. It enables a range of policy responses which cannot be done with non-fiat crypto.

THANK YOU

References

1. Berkeley edX Bitcoin course slides and text.
2. Bitcoin: A Peer-to-Peer Electronic Cash System, Satoshi Nakamoto
3. Bitcoin and Cryptocurrency Technologies, Princeton University Press
4. https://www.atrium.co/blog/money-tech-crypto/
5. https://coincentral.com/how-many-bitcoins-are-left/
6. https://www.coindesk.com/900-20000-bitcoins-historic-2017-price-run-revisited/
7. All images are courtesy of google.