BLOCKCHAIN

A simple insight into the complexity.

What’s Blockchain?

What’s Bitcoin?

What’s Bitcoin?

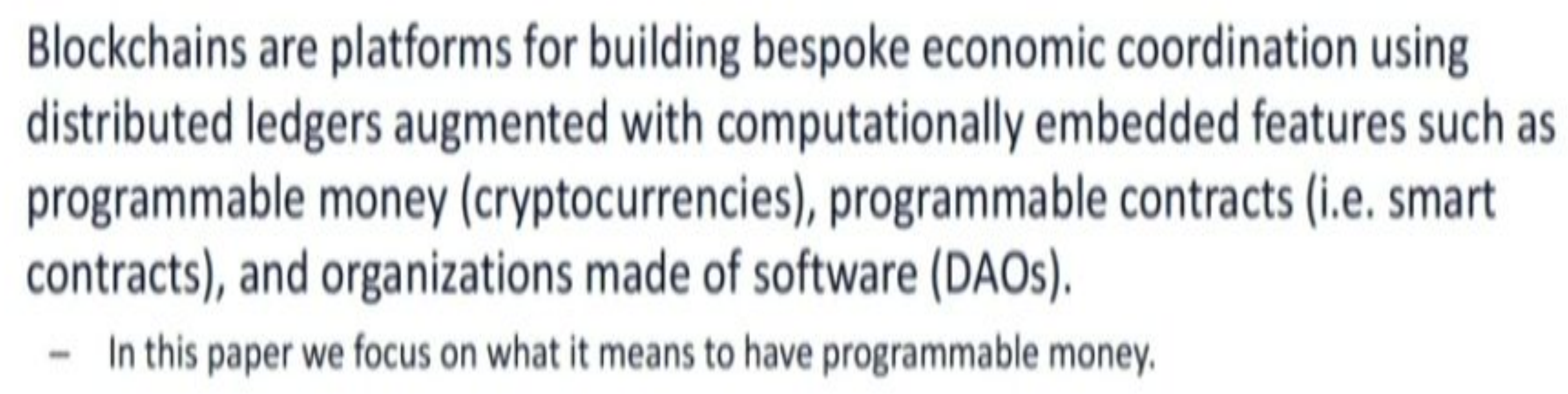
- Trust + Maths + Bits
- Bitcoin is the very first application of the blockchain running since 3rd Jan 2009.
- 21 Million only. 16 Million mined. Approx 3 million lost.

Why Bitcoin is Special?

- Anonymous
- Decentralized
- Consensus
- One currency = All countries
- Scalable

What’s Blockchain?

Words of Prof. Sinclair Davidson

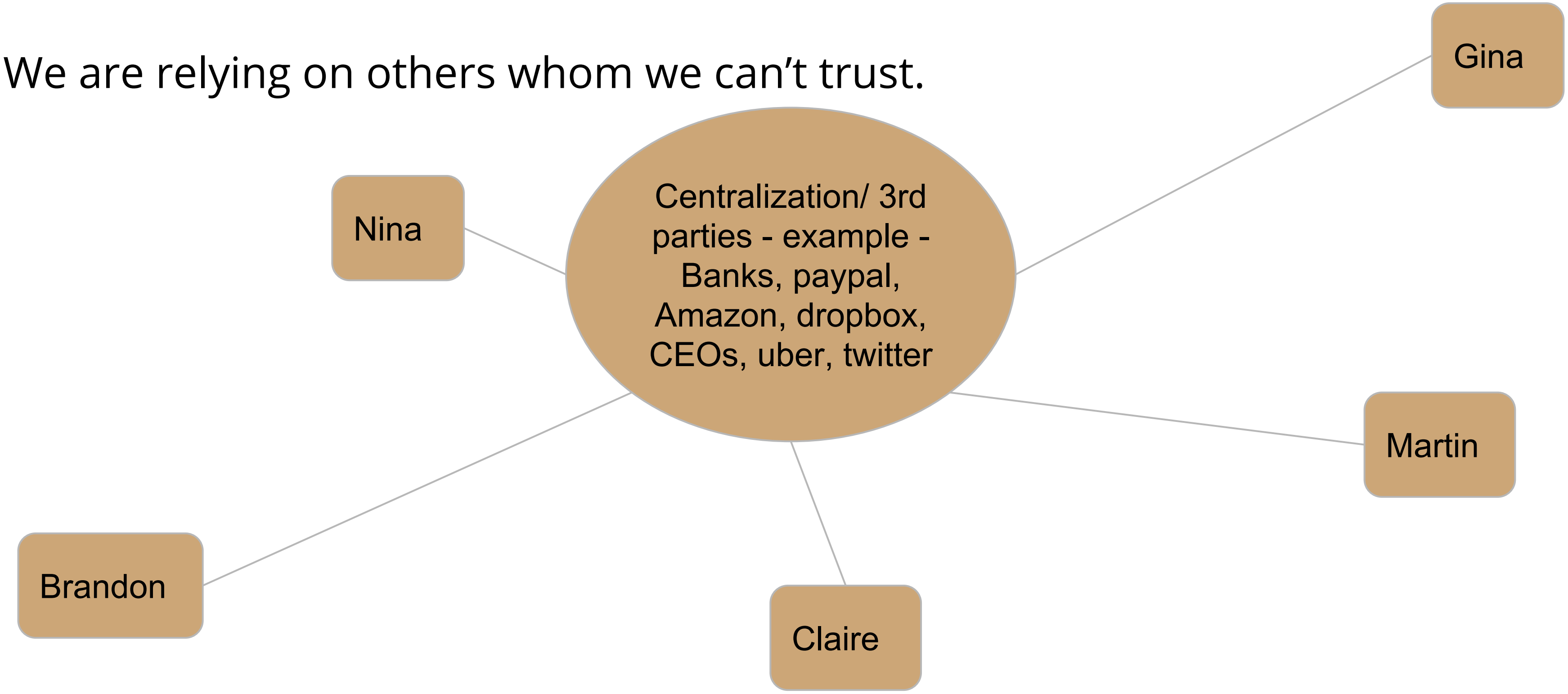


Blockchains are platforms for building bespoke economic coordination using distributed ledgers augmented with computationally embedded features such as programmable money (cryptocurrencies), programmable contracts (i.e. smart contracts), and organizations made of software (DAOs).

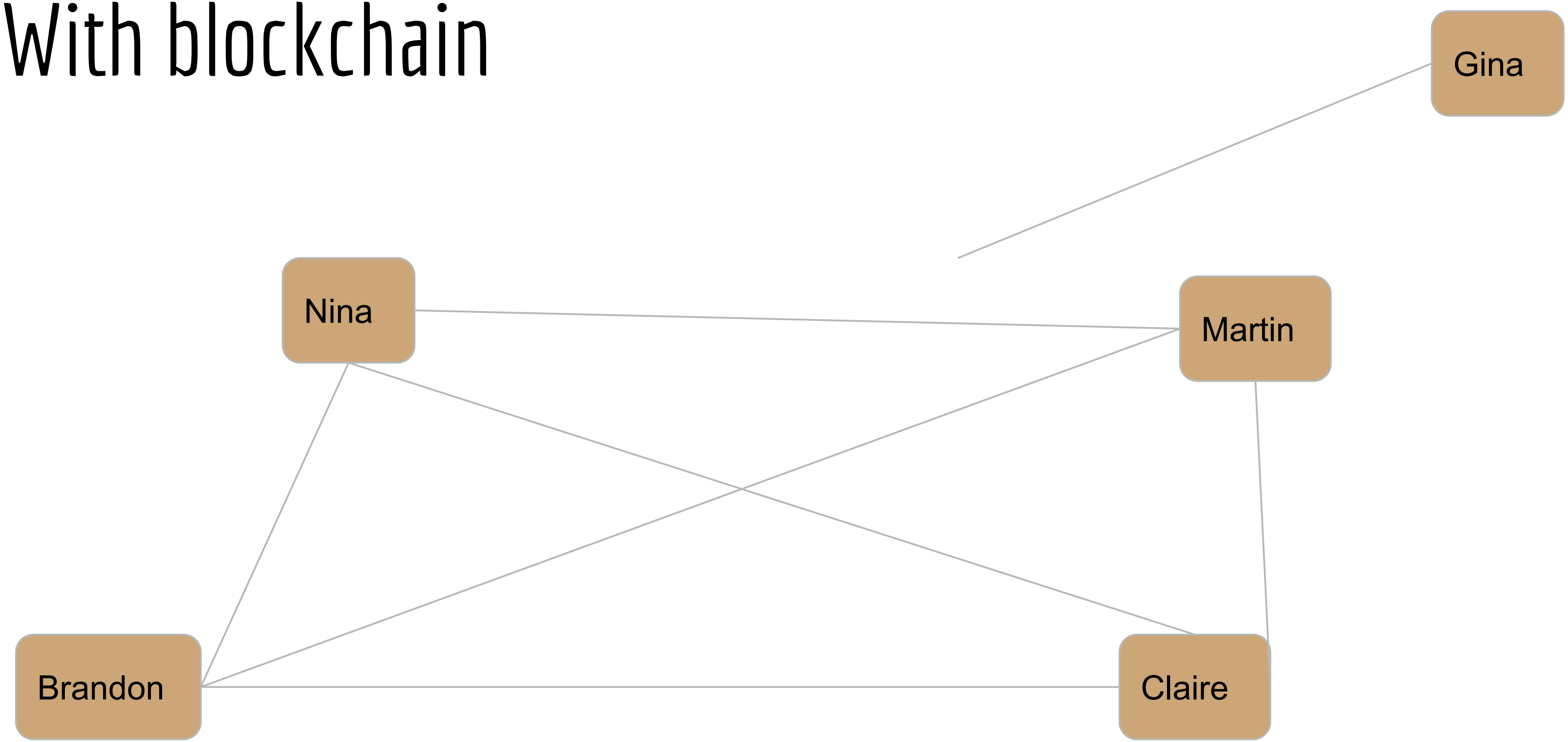
- In this paper we focus on what it means to have programmable money.

Right now.

We are relying on others whom we can't trust.

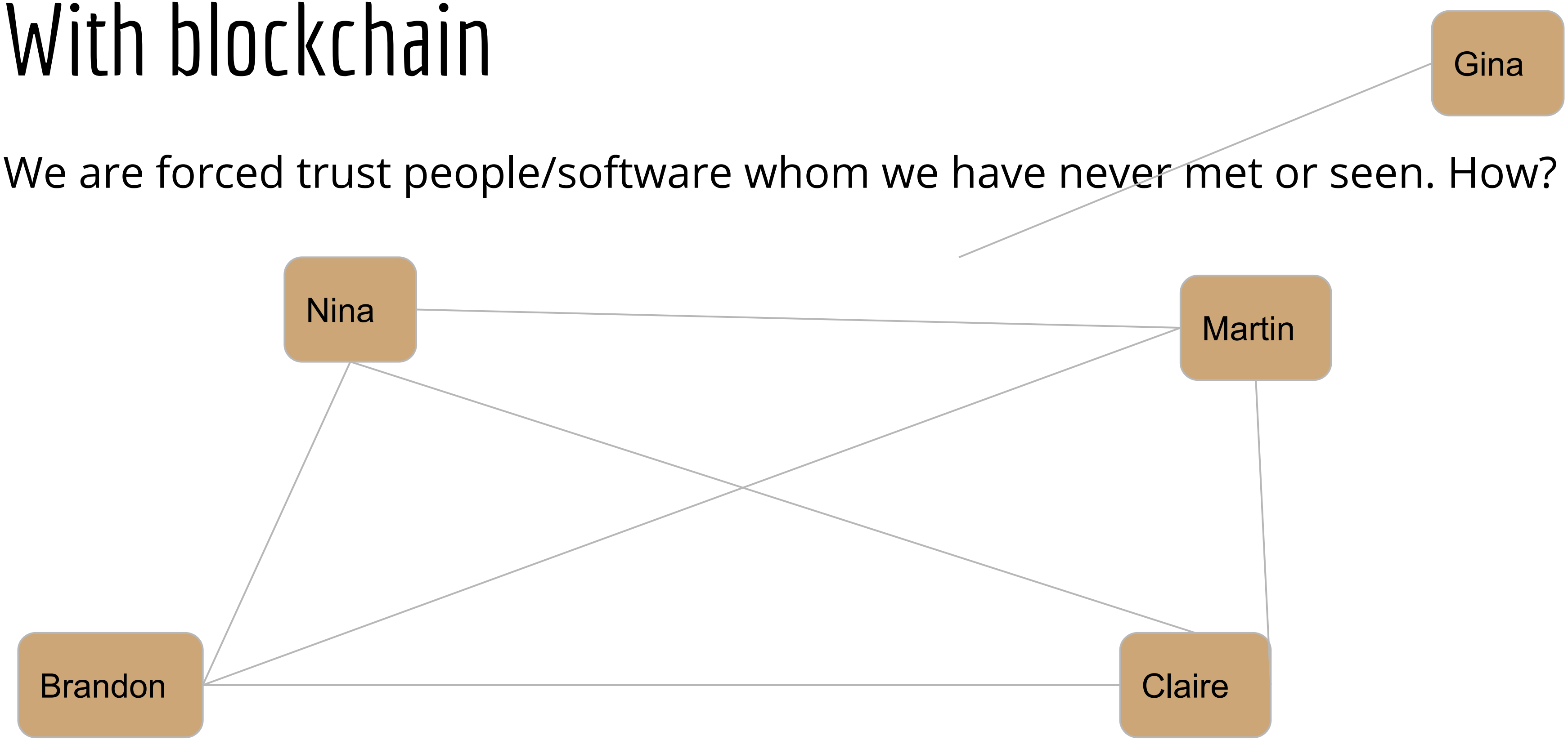

Gina
Nina
Centralization/ 3rd parties - example - Banks, paypal, Amazon, dropbox, CEOs, uber, twitter
Martin
Brandon
Claire

With blockchain

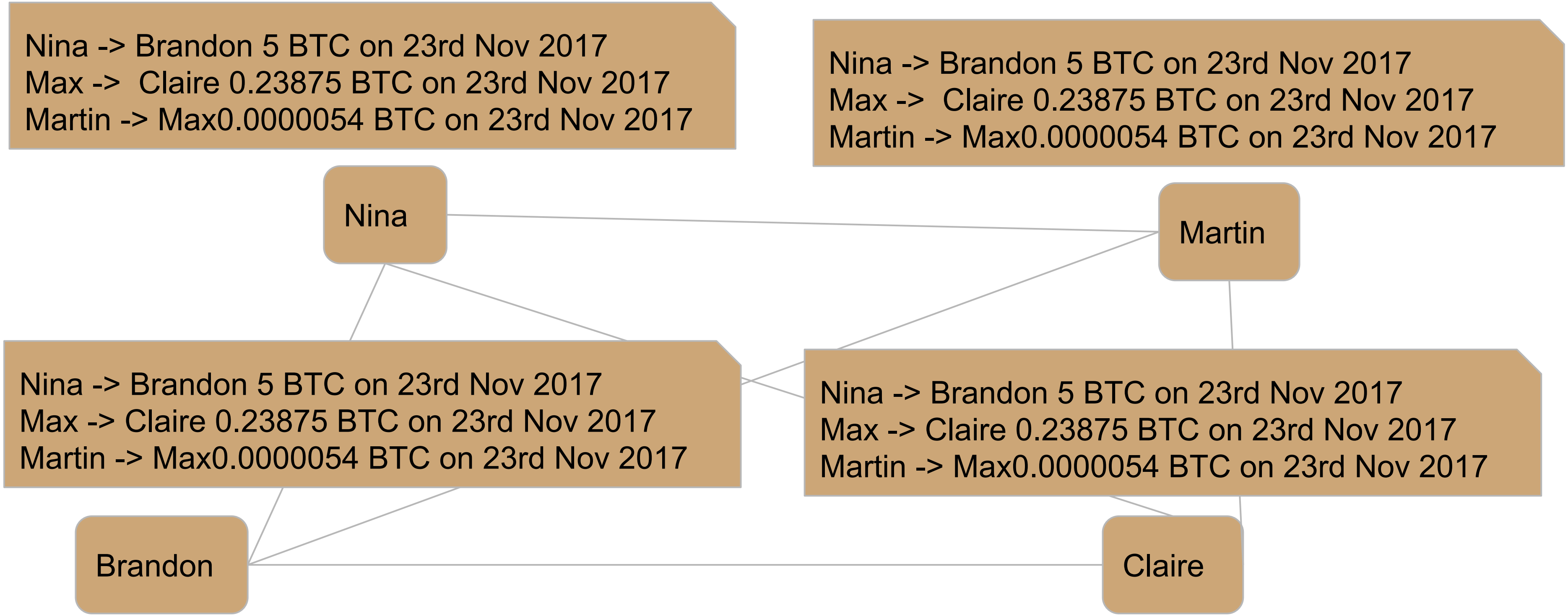


With blockchain

We are forced trust people/software whom we have never met or seen. How?



Same database everywhere.



Nina -> Brandon 5 BTC on 23rd Nov 2017
Max -> Claire 0.23875 BTC on 23rd Nov 2017
Martin -> Max0.0000054 BTC on 23rd Nov 2017

Nina -> Brandon 5 BTC on 23rd Nov 2017
Max -> Claire 0.23875 BTC on 23rd Nov 2017
Martin -> Max0.0000054 BTC on 23rd Nov 2017

Nina -> Brandon 5 BTC on 23rd Nov 2017
Max -> Claire 0.23875 BTC on 23rd Nov 2017
Martin -> Max0.0000054 BTC on 23rd Nov 2017

Nina -> Brandon 5 BTC on 23rd Nov 2017
Max -> Claire 0.23875 BTC on 23rd Nov 2017
Martin -> Max0.0000054 BTC on 23rd Nov 2017

With blockchain

How?

There is transparency of the data.

In a distributed ledger every party have a copy of the ledger.

We don’t need to know the name of the parties. Does the vending machine ask your name?

This gives privacy.

And all work, no politics.

What’s Bitcoin?

- Anonymous
- Decentralized
- Consensus
- One currency = All countries
- Scalable

About Bitcoin?

- A hash algorithm which is a cryptographic algorithm which converts an arbitrary amount of data into a fixed-length "digest".
- Impossible to determine what the input data was.
- SHA256 is used in Bitcoin, but there are many others including SHA3, RIPEMD160, scrypt etc

About Bitcoin?

- Public key cryptography - A "private" secret key is converted into a "public" key and used to prove ownership of the private key without giving away the secret. Additionally it is possible to encrypt data using the public key so that only the person holding the private key can decrypt it. It is possible to prove that the creator of the transaction owns the secret private key by using only the signature data and the public key.
- 2 ^160 private keys.

About Bitcoin?

- Merkle root - A tree data structure that uses one-way hashing to hold multiple pieces of data making it so that any data in the input of the tree can not be modified without changing the final value of the merkle root hash.

About Bitcoin?

- Bitcoin is a UXIO based contract
- A UTXO is an *unspent transaction output*. In an accepted transaction in a valid blockchain payment system (such as Bitcoin), only *unspent* outputs can be used as inputs to a transaction. When a transaction takes place, inputs are deleted and outputs are created as new UTXOs that may then be consumed in future transactions.

About Block of Bitcoin

- Block- The smallest verifiable and unforgeable unit on the blockchain. It contains various data. A block in Bitcoin has a header. The header contains the following:
    - Version
    - Previous block header hash
    - Merkle root hash of all transactions in the block
    - Time of creation
    - Difficulty
    - Nonce

  The body of the block is complete transactions.

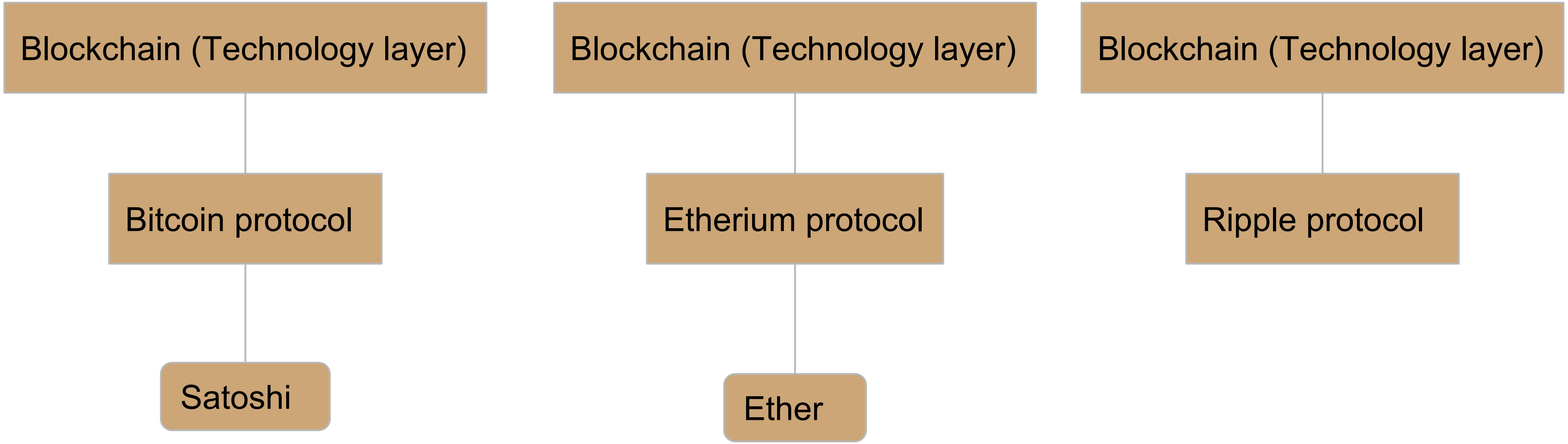
About PoW

A consensus system - requires participants (miners) in the block creation process to put in a certain amount of computational work to solve a difficult puzzle. The first miner to solve the puzzle gets a reward and their created block is added to the network's blockchain. How much work must be done is controlled by the "difficulty" specified in the block.

Diagrams

The Blockchain World

The blockchain can be the same or different.



Blockchain (Technology layer)

Bitcoin protocol

Satoshi

Blockchain (Technology layer)

Etherium protocol

Ether

Blockchain (Technology layer)

Ripple protocol

What’s Blockchain?

What’s Bitcoin?

Blockchain’s Future

A tsunami

Based on various data structures and AI techniques. Openbazaar, Github

Google, FB and twitter are nothing but marketing. Microsoft vs Ubuntu.

No Politics, No Banks, No Governments, No Countries.

Thank you blockchain