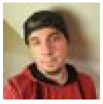
BUZZ CHRONICLES > BLOCKCHAINDEV
Saved by @BellOmuboye
See On Twitter

Twitter Thread by Oliver Jumpertz



Oliver Jumpertz
@oliverjumpertz

What actually is a Blockchain?

Bitcoin is breaking record after record, but there must be more to the technology than just crypto, or not? Well, we can take a look at the underlying technology first to understand what it actually provides to us.

■■■

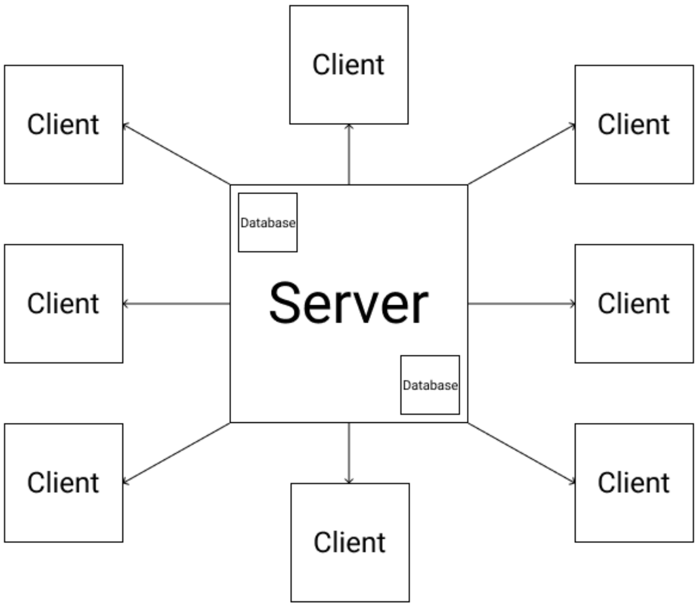
1■■ Foreword

This will be a high-level overview to give you an intro to blockchain technology. With further threads, we will dive deeper and deeper, so don't be sad if something you really looked forward to isn't included as detailed as you would have wished for, yet!

2■■ Client-Server Architecture

Before we dive into blockchain technology, we should take a look at how most of the internet works. We need this to understand the fundamental differences between a traditional model and the change blockchain technology brings.

The internet is mostly powered by a client-server architecture. For each service offered, its data is stored and owned by one entity, and distributed to a multitude of clients. It is stored in databases and returned to the users on request with or without further processing.



The server decides what is true. Information that has been stored once, can still be modified. No one can stop the owner of a website from modifying information within their database(s) or deleting it from their records.

If Twitter decides that one of your tweets shouldn't exist for some reason, they can delete it if they wish to (so can you). The same holds true for all other social networks and for everything else. If you think one of your blog posts underperforms, you can delete it.

Users always only get to see what the servers let them see and we trust the owners of the websites/services we use that they won't act against us. We actually have no choice other than to find someone else who we trust more when we are in doubt.

The same holds true for banks. Although they are regulated and legally obliged to act in your favor, you still need to trust them with your finances and have faith in their IT systems. You basically have no other choice.

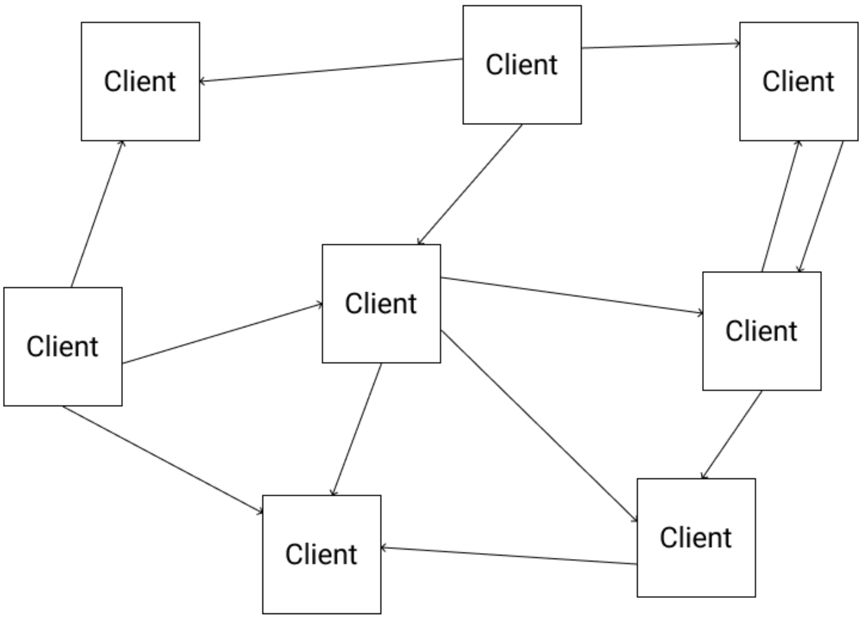
If you try to transfer money from your bank ...

... account to another one at another bank, it's still up to them to decide (within the bounds law forces on them) when to send the transaction. Some banks make extensive usage of deadlines, and delay your transactions to even out their balance sheets.

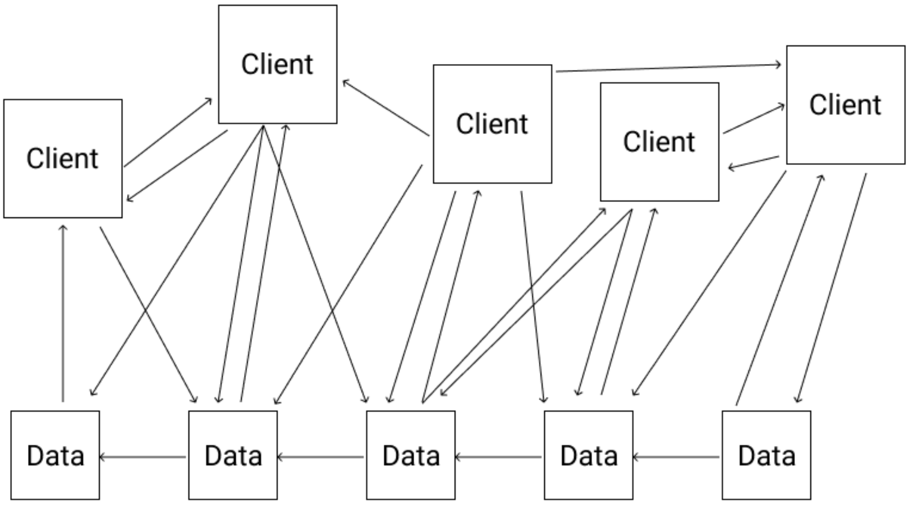
3■■ Blockchain Technology

Blockchain technology itself is nothing completely new. It's a combination of existing technologies creating something new and exciting, tackling very specific problems while being broadly applicable.

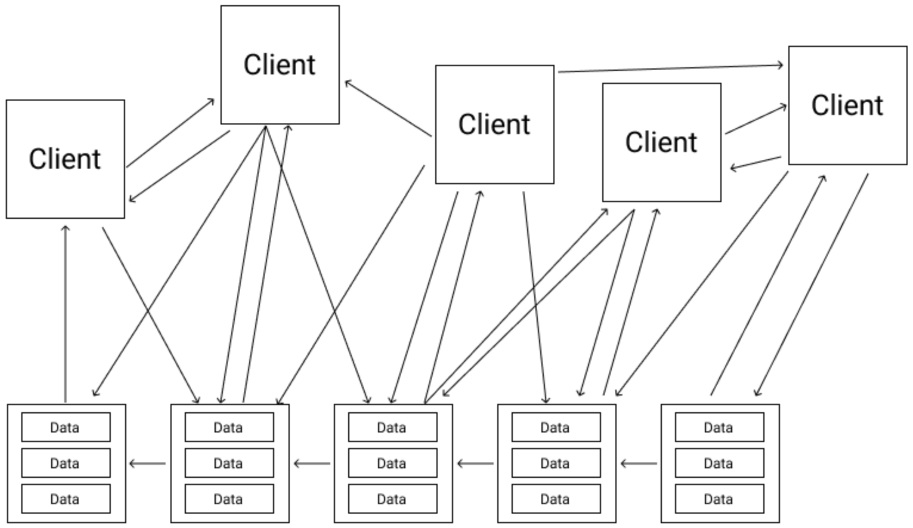
Generally speaking, you deal with a peer-to-peer network where no client talks to a central server but to many other clients.



This peer-to-peer network comes with a distributed database. Data is shared among all clients of the network. The data forms a chain where each block points at its predecessor in some form.



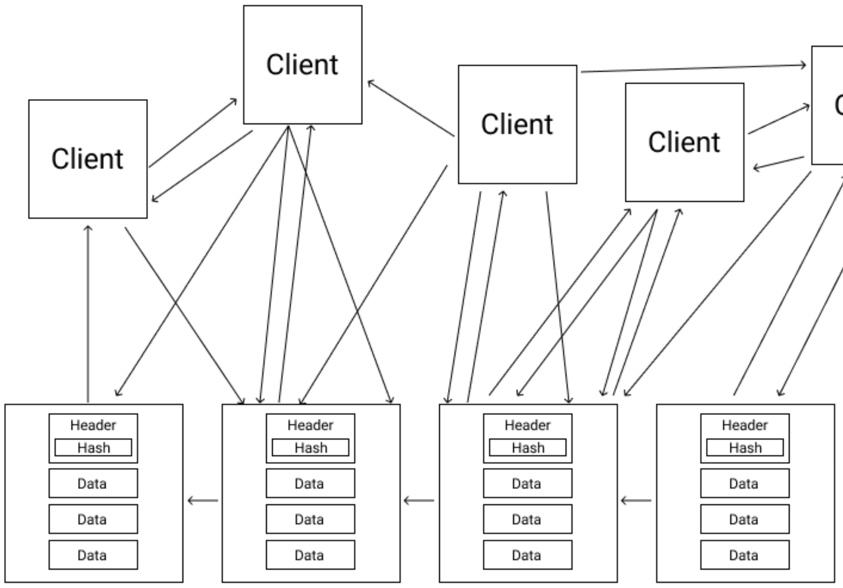
Placing individual entries into the chain would be inefficient which is why multiple entries are actually batched into blocks. This means that each block contains several data entries (thus the name of the technology).



To establish trust between all clients, or in other words, make sure that no one simply changes the chain and sends a fake one to your client, blocks contain a cryptographic reference. This reference often takes into account the content of the current and the ...

... previous block so that the correctness of a block and the whole chain can be verified.

The process of appending a new block to the chain is either called mining or forging, depending on the actual blockchain implementation.



The chain itself is designed to be immutable. Entries can't be changed and can't simply be deleted again, there is always a new entry - like an event log that states what happened when - publicly available.

4■■ Mining / Forging

As you already learned, mining or forging is the process of appending a new block to the chain.

There are multiple algorithms that deal with verifying blocks on a blockchain.

Two of those are:

- Proof-Of-Work
- Proof-Of-Stake

Proof-Of-Work is the algorithm used by Bitcoin. Miners have to guess random numbers that, combined with the previous block content, generate a defined result. This process is so compute-intensive that only the combined power of many miners ...

... can generate a result in approx. 10 minutes on average. One computer alone would take way more time to find just one result (~1 year).

Although this algorithm costs a lot of energy and resources, it is pretty safe, because attackers always have to compete ...

... with the whole network and it's not guaranteed when a miner may find the right answer to the problem at hand. Attacking a blockchain would mean constantly outperforming everyone else, which is nearly impossible.

Proof-Of-Stake is another algorithm that is not as compute-intensive and thus not as energy-intensive as Proof-Of-Work. Based on some criteria, a random node is selected to verify the next block and append it to the chain. That node doesn't have to calculate a complex ...

... result and thus doesn't need that much energy and so many resources anymore. You could say that this is an environment-friendly alternative with a lot of potentials.

5■■ What A Blockchain Offers

The general idea of a blockchain is to provide a publicly available, decentralized database. Everyone can participate and work with the network. Trust is established by the implementation itself because manipulation is very difficult, ...

... or even impossible.

No one can easily take control of a blockchain and change everything to their advantage. Small-scale manipulation can be spotted and negated by the network itself.

Users do no longer have to trust a central entity to manage something for them, ...

... the network does it.

And there is much more to a blockchain than only cryptocurrencies. You can build a whole social network on a blockchain where no censorship is possible, for example. Each entry ever made is persistent. No chance to delete a statement, ...

... or modify it after pushing it out anymore. Every modification is transparent. There is also no chance to let users vanish only because you want it to happen.

6■■ What's Next?

This was only a high-level overview to get warm with the general concept of a blockchain. We'll soon dive deeper into multiple specific concepts to grow our overall understanding of this particular piece of technology.

This thread is now over. Thank you for reading it and feel free to add your feedback as you like!