Over the last few months I keep thinking that the way blockchains are communicated to the public needs changing. We seen quite a few blockchains that didn't bring anything to the table the last few years.

As a though experiment I wanted to explore blockchains from a different view, the end user view. The following is exactly that.

Happy to hear any feedback about it.

Introduction

Blockchains are not unique in their possession of manytechnical specifications. In fact, most digital goods are similar. Laptops show RAM sizes, CPU models, battery capacity and hard drive space while cars show fuel consumption (MPG), horse power (HP), cubic capacity (CC) and cylinder count.

These specs have specific meanings in consumer minds. More RAM means more browser tabs, more disk space means more photos or movies, more house power means better acceleration etc.

Blockchains specs are currently very different. They are abstract terms, usually originating from academic articles, and are hard to understand for most users. But crypto networks are targeted at consumers too and consumer want very specific things, namely: faster

, cheaper

, easier

and … safer

.

Faster

A blockchain feels fast

when there are quick confirmations that transactions are going through. Usually, confirmations are not set irreversible and there's a second confirmation (called finality) that ossifies the transaction. This events are very rate but if it happens to someone in an unexpectable way, chances are label the blockchain as unsafe.

Tx inclusion:

Some blockchains are faster that others. In fact, the faster blockchains can process transactions in about 2 or 3 seconds while other systems need 15 seconds or more. The reason for this is that some blockchain have timeouts in node communication. Blockchains with timeouts (called BFT-like consensus) have a fixed amount of time tht nodes wait to hear from other nodes. These blockchains are faster and have instant finality but if enough nodes don't reply in time, they can't produce blocks and have to halted until enough nodes come back online. The other option (called Nakamoto-like consensus) is to not have a timeout and always follow the longest chain, it's not as fast as the first option and transactions are not instantly irreversible but they can support a lot more nodes and they always online.

Block finality:

It's possible that blocks and consequently transactions get reverted even if they showed as confirmed initially. As discussed above, some blockchains (ie. Nakamoto-like consensus) have to revert if they see a more appropriate version of the chain (more discussion on the trade-offs in the "Safety" section below).

Soft confirmations:

Most L2s blockchain provide users with really quick confirmation that their transactions will be included in the next block (called soft-confirmation). These L2s systems usually a few nodes priviledges responsibilities if they put up a significant collateral. One of their responsibilities is to commit to the transactions that will be included in the next block. If they start acting dishonestly their collateral might get slashed.

Safer

A blockchain feels safe

when users are confident that the chain is sufficiently validated and when transactions are not censored and they don't revert.

Transaction censorship:

Since the responsibility of deciding which transactions should be included in blocks is done voluntarily by nodes, they can

choose to censor a particular transaction. Blockchain with more nodes suffer less since if one node censor transactions the next possibly won't. Nodes are incentivized nodes to include transactions with transaction fees but there is no penalty if they don't and they are cases censorship is prevalent due to regulatory reasons (eg. OFAC and Tornado Cash) or ethical reasons (eg. Bitcoin Ordinals).

Node decentralization:

Blockchain with less nodes may be unable to process transactions for various reasons. For example, there might be a third party attacking them, the chain might face hostile takeover from token holders or there could be infrastructure problems with internet cables or cloud providers.

Block Finality:

Some blockchain systems might allow two concurrent versions of the chain to existing for some time until nodes decide which one is the valid one. For example, there could be two blocks that are proposed at the similar time and the network might take some time to decide which is appropriate one to follow. In the meantime, a user might follow one version of the chain which might not end up to be the correct one (ie. the one with the most staking votes or more proof of work attach to it).

Cheaper

A blockchain is cheaper

when there's enough blockspace supply to cover demand. In other words, when a chain can process more transactions per second (TPS) than the transactions that are submitted by the users, transactions fees are low.

Decentralization and TPS:

The less nodes there are to process transactions, the faster they can process them. This happens mainly because with fewer nodes transactions can propagate around network faster but it also means that the chain is more likely to go offline or censor transactions.

Sharding and TPS:

Blockchains that split their nodes in committees can process transactions in parallel. Sharding with committees allows processing more transactions in total but the more committees there are the less nodes each committee will have that affects the total chain security.

Demand and TPS:

One major factor that affects transaction costs is demand for blockspace from people that are looking to include transactions in blocks. Alternatively, a blockchain can have lower demand if it's restricted in its use (such as Bitcoin that doesn't support smart contracts and some Cosmos chains).

Layer 2 and TPS:

Layer 2s are can make transactions cheaper by processing them off-chain and only store a cryptographic proofs of the results on-chain. Since layer 2s have only a few nodes for better efficiency they have a greater chance that one censors transactions or something happens to all of then and the chain goes down.

Easier

Being easy to use

means less thinking for users. Arguably one of the harder problems with blockchains right now is that they are mentally draining. Features such as biometric wallets and wallets that spending restriction are necessary for adoption.

Seed-less wallets:

Meta-transactions are smart contracts that can send transactions in behalf of users. These transactions enable many new use cases such as wallets with biometric authentication instead of seed phrases and wallets that can enforce specific rules (eg. funds can't be drained all at once).

Gas-less transaction:

A common issue using a token from a new chain is you can't do anything without also bridging the native token too. This can be solved with meta-transactions as well that convert to native token on the fly.

Summary

Blockchains are no different to other products such as laptops and cars. They need to be: fast, cheap, easy and safe (since they usually deal with money).

Being fast is affected by transaction confirmation speed, soft-confirmations and finality. Being safe is determined by decentralization adn censorship. Being cheap is affected by various factors such as node decentralization, transaction demand, sharding and Layer 2s. And lastly, biometric wallets and gas-less transaction can make blockchains more easier to use.

If you found this post insightful you might like my other poston consumer blockchains.