You don't need a blockchain.

> This article was originally published at https://gist.github.com/joepie91/a90e21e3d06e1ad924a1bfdfe3c16902.

If you're reading this, you probably suggested to somebody that a particular technical problem could be solved with a blockchain.

Blockchains aren't a desirable thing; they're defined by having trustless consensus, which necessarily has to involve some form of costly signaling to work; that's what prevents attacks like sybil attacks.

In other words: blockchains *must* be expensive to operate, to work effectively. This makes it a last-resort solution, when you truly have no other options available for solving your problem; in almost every case you want a cheaper and less complex solution than a blockchain.

In particular, **if your usecase is commercial, then you do not need or want trustless consensus**. This especially includes usecases like supply chain tracking, ticketing, and so on. The whole *point* of a company is to centralize control; that's what allows a company to operate efficiently. Trustless consensus is the exact opposite of that.

Of course, you may still have a problem of trust, so let's look at some common solutions to common trust problems; solutions that are a better option than a blockchain.

- **If you just need to provide authenticity for a piece of data:** A cryptographic signature. There's plenty of options for this. Learn more about basic cryptographic concepts here.
- **If you need an immutable chain of data:** Something simple that uses a merkle tree. A well-known example of this application is Git, especially in combination with signed commits.
- **If that immutable chain of data needs to be added to by multiple parties (eg. companies) that mutually distrust each other:** A cryptographically signed, append-only, replicated log. Chronicle can do this, and a well-known public deployment of this type of technology is Certificate Transparency. There are probably other options. These are *not* blockchains.
- **If you need to verify that nobody has tampered with physical goods:** This is currently impossible, with or without a blockchain. Nobody has yet figured out a reliable way to feed information about the real-world into a digital system, without allowing the

person entering it (or handling the sensors that do so) to tamper with that data.

Some people may try to sell you one of the above things as a "blockchain". It's not, and they're lying to you. A blockchain is defined by its trustless consensus; all of the above schemes have existed for way longer than blockchains have, and solve much simpler problems. The above systems also don't provide full decentralization - and that is a *feature*, because decentralization is expensive.

If somebody talks to you about a "permissioned blockchain" or a "private blockchain", they are also feeding you bullshit. Those things do not actually exist, and they are just buzzwords to make older concepts sound like a blockchain, when they're really not. It's most likely just a replicated append-only log.

There's quite a few derivatives of blockchains, like "tangles" and whatnot. They are all functionally the same as a blockchain, and they suffer from the same tradeoffs. If you do not need a blockchain, then you *also* do not need any of the blockchain derivatives.

In conclusion: blockchains were an interesting solution to an extremely specific problem, and certainly valuable from a research standpoint. But you probably don't have that extremely specific problem, so you don't need and shouldn't want a blockchain. It'll just cost you crazy amounts of money, and you'll end up with something that either doesn't work, or something that has conceptually existed for 20 years and that you could've just grabbed off GitHub yourself.

Additions

I'm going to add some common claims here over time, and address them.

"But it's useful as a platform to build upon!"

One of the most important properties of a platform is that it must be *cost-efficient*, or at least as cost-efficient as the requirements allow. When you build on an unnecessarily expensive foundation, you can never build anything competitive - whether commercial or otherwise.

Like all decentralized systems, blockchains fail this test for usecases that do not benefit from being decentralized, because decentralized systems are *inherently* more expensive than centralized systems; the lack of a trusted party means that work needs to be duplicated for both availability and verification purposes. It is a flat-out impossibility to do *less* work in an optimal decentralized system than in an equivalent optimal centralized system.

Unlike most decentralized systems, blockchains add an extra cost factor: costly signaling, as described above. For a blockchain to be *resiliently decentralized*, it *must* introduce some sort of significant participation cost. For proof-of-work, that cost is in the energy and hardware required, but any tangible participation cost will work. Forms of proof-of-stake are *not* resiliently decentralized; the cost factor can be bypassed by malicious adversaries in a number of ways,

meaning that PoS-based systems aren't reliably decentralized.

In other words: due to blockchains being inherently expensive to operate, they only make sense as a platform for things *that actually need trustless consensus* - and that list pretty much ends at 'digital currency'. For everything else, it is an unnecessary expense and therefore a poor platform choice.

Revision #1
Created 11 December 2024 01:59:26 by joepie91
Updated 11 December 2024 15:56:33 by joepie91