'Blockchain not bitcoin'

Cryptocurrencies have captured the public's attention with their wild volatility, outspoken community, legal ambiguity, and mysterious origins. While most trends in crypto come and go, a popular narrative that won't seem to disappear is the 'blockchain not bitcoin' belief.

I've seen two primary interpretations of the 'blockchain not bitcoin' narrative:

1. Cryptocurrencies have no inherent fundamental value, but blockchain technology will be impactful.

2. Public blockchains aren't useful, but private enterprise implementations of blockchain technology will be valuable.

The narrative originated from various dynamics over time, including cryptocurrencies' ties to criminal activity, performance limitations (cost, speed, volume), and lack of control over the networks. The technology and core beliefs that underpin cryptocurrencies make intentional tradeoffs that gives rise to these dynamics.

Both interpretations stem from a fundamental misunderstanding of bitcoin and blockchains. More importantly, the narrative misses the significant innovation of the buzzworthy blockchain. The counter-narrative requires unpacking a few technical, historical, and computational characteristics of blockchains, money, and databases. We'll start with the definition of a blockchain.

Blockchain defined

At its core, a blockchain is a series of bundled, sequential inputs that create a collective record. A useful, yet overly simplistic, comparison is that a blockchain is a database with entries that can only be added, not changed or deleted.

The novelty of a blockchain is simply a new data structure. Blockchains keep a sequential digital record of data. Let's further delineate between public and private blockchains:

> Public blockchains are open and accessible to all participants. The protocol is open-source and widely shared, copies of the ledger are held by many, and any participant can add records to the ledger according to the software-based rules. Bitcoin falls into this definition.
>
> Private blockchains operate on a closed network. Only certain parties are granted permission to view or add records to the blockchain. The group of records, or ledger, is controlled by a single or small number of entities.

The significant innovation of blockchain technology came with the implementation of the public Bitcoin blockchain. We'll focus on the Bitcoin blockchain for much of this paper due to its popularity and clearly defined intentions.

Key Bitcoin characteristics

Bitcoin is a public blockchain that uses carefully constructed incentive mechanisms to create a network that has the ability to be (a) trustless, (b) permissionless, and (c) decentralized.

Let's unpack these key components:

(a) Trustless – no individual or entity needs to be trusted; both in terms of individual transactions and the macro rules of the protocol. The security and continued operation of the network relies on financial incentives and computer science.

(b) Permissionless – since participants don't need to trust any individual or entity, we can allow anyone to participate. The incentives are designed so that the network can operate with unknown and malicious users (i.e., bad actors). No individual or entity can be censored from participating according to the protocol.

(c) Decentralized – control does not reside with one entity. Power is shared among the network participants. Decentralization is often confused with the concept of being "distributed". Decentralization is about the dispersion of power, while distributed about the redundancy of the database or the number of nodes in a network. The dispersion of power makes the rules of the network difficult to change (again, this is a feature, not a bug).

These three characteristics allow for a shared agreement on a digital record without a central, trusted third-party. This had never been done at a global scale before Bitcoin and represented a paradigm shift in the ability to digitally store and transfer value. However, there is no free lunch, even in Silicon Valley, but especially in crypto. The innovation to remove of a trusted third-party has known tradeoffs. Widely cited tradeoffs are speed, cost, and throughput of the network.

A decentralized blockchain means each node (i.e., computer) must verify every transaction and share any new information with all other nodes in real time. There can be upwards of tens of thousands of nodes across the globe all performing the same computation, which is expensive. Transactions are probabilistically finalized based on the financial incentives, which only accrue over time. Also, there are physical limitations to how fast information can be processed and shared. Thus, to adopt a secure public blockchain, we must value a decentralized network over certain performance characteristics. This prioritization is what helped develop Bitcoin.

Bitcoin, using a blockchain, solved a social coordination problem in a digital era that allows for its trustless, permissionless, and decentralized operation. Most prominently, digital money has evolved as the killer use case for blockchain technology (hence, why commonly referred to as cryptocurrency). Let's further explore why trust and control are important, especially with money.

Trust, control, and money

Our modern economy is built on various degrees of trust. One of the most significant forms of trust is in money. Money is defined as a store of value, unit of account, and medium of exchange. Good money must be accessible, durable, fungible, portable, reliable, divisible, and importantly must retain value.

Fiat currency, which legal tender whose value is backed by the government or entity that issued it, is speculative in nature. In short, we accept U.S. dollars because we expect someone to accept U.S. dollars in the future. Fiat money relies on network-effects and artificial scarcity. For reference, gold is decentralized and relies on physical scarcity to retain value. However, gold lacks many of the characteristics of good money (i.e., portable, divisible, accessible).

Today, we typically rely on governments to issue fiat money. Governments are sometimes reliable in the short-term at performing this task (that's not very comforting). One of the biggest hurdles for fiat currency is the ability for money to retain value and remain durable (i.e., purchasing power can last over time). Retention of value is done by creating artificial scarcity.

In a not-too-surprising conflict of interest, most governments have the largest respective sovereign-denominated debt. This creates quite a temptation when a country is in massive debt and controls the printing press. The control and incentives of central banks are why we see hyperinflation in struggling countries. One entity with misaligned incentives controls the artificial scarcity for the foundation of an economy.

If a single entity controls the supply of money, they typically can also create rules about around the movement and who can (and can't) participate. This can make fiat currency inaccessible or immobile (i.e., cannot freely leave a country). On a smaller scale, think about the millennial-focused payment app Venmo. One company (PayPal) controls your balance, your ability to transfer that balance, and determines who can participate in the storage and transfers of digital assets. Would you keep your entire net worth on Venmo? For nearly everyone, the answer is no. Like fiat currency, a centralized authority can control nearly all aspects of fiat or virtual money.

This brings us to the initial part of our first critique, "bitcoin has no value". Cryptocurrencies can be seen as a superior form of money given the decentralized control and digitally enforced scarcity. Many smart people, including Warren Buffet, have denounced cryptocurrencies as valueless. This misunderstanding of bitcoin is rooted in an overconfident assessment of centralized control and trust in an institution to act in the best interest of its constituents. The generational trust is given to a central bank that has used various levers to be an arbiter for the general health of the economy, for which many U.S. adults have largely seen a positive impact. However, history shows fiat currencies can be easily abused by political power.

Another common, and valid, concern with cryptocurrencies is the wild volatility. With any emerging technology, there will be ups and downs as we move towards wide-scale adoption. Cryptocurrencies will not be as stable as the U.S Dollar in the short-term. With a fixed supply of bitcoin to be issued, incremental demand will unavoidably increase its price in the long-term. In the short-term, it is unclear if and when the flywheel effect will be fully put into motion.

A blockchain without a cryptoasset

To address the second part of the first critique ("blockchain technology will be valuable"), consider our definition of a blockchain: a series of records. The Bitcoin blockchain records who owns how much bitcoin.

The idea of removing a cryptoasset from a public, decentralized blockchain sounds appealing at first. However, having a blockchain without an asset is both impossible and impractical. It would be impossible to craft the necessary incentives for the proper operation and decentralized nature of a public blockchain in the long-term. There may be a myriad of short-term non-financial incentives but creating a lasting crypto-network assumes long-term participants.

If removing an asset from a blockchain were possible, the result would be an impractical shared, public database. Incentives aside, a public blockchain without an asset will be computationally expensive compared to a centralized database. Further, you can already store information and executable logic on

public blockchains, such as Ethereum, which also has a native asset. Go back to the Venmo example: what would Venmo be without money? A collection of emojis.

Blockchains without assets are often seen as the solution to all problems. In most situations, the use of a blockchain can lead to more complications. Before using a blockchain, start with the problem at hand and ask:

- Do you need to store records or maintain a database?
- Are there multiple individuals that can make additions to the record?
- Are individuals unknown and untrusted?
- Is the no trusted third-party to administer the database?

If the answer to one or more of the above questions is “no”, congratulations you probably don’t need a blockchain!

To summarize, public blockchains can create a scare and secure digital asset. These digital assets remove a centralized power which leads cryptocurrencies to be seen as a superior form of money. Further, you cannot separate an asset from its underlying public blockchain unless the blockchain operates in a closed, permissioned network. Next, we’ll discover why private blockchain implementations are the most commonly over-promised application of blockchain technology.

Interpretations #2

This brings us to our second interpretation: “public blockchains aren’t useful, but private enterprise blockchains will be valuable”. We should note that the public/private nature of a blockchain is not binary. Blockchains can move along a spectrum as the network evolves.

We’ve already seen why public blockchains can be valuable to create digital assets with its decentralized nature. We believe the second interoperation of the narrative focuses on perceived performance limitations of public blockchains.

To further quantify the limitations, bitcoin can be seen as slow (~60 minutes to finality), expensive (currently ~$5/transaction, but as high as $50/transaction), and unscalable (~7 transactions/second). While these are all generally true, they are a consequence of intentional tradeoffs made to ensure the security of a decentralization network. These factors will either be improved or abstracted away from the main blockchain (i.e., pushed to “Layer 2”) as technology advances. But for now, they are real disadvantages when compared to a centrally controlled network (i.e., the Visa for payment processing).

Enterprise blockchains

These tradeoffs have led companies to launch permissioned, or private, blockchains. The same sequential data structure is employed, but who can participate is controlled. Further, the consensus method (path to mutual agreement) on changes to the database is often controlled by one entity. This fundamentally removed the purpose of a public blockchain. The control is back in the hands of a single entity and the network is closed. This is a permissioned database!

Enterprise blockchains are often seen as a solution to legacy IT infrastructure when a permissioned database will solve the problem in a quicker and more cost-effective manner. Public blockchains allow individuals and entities to transact with anyone, anywhere, without a central third-party.

Private and public blockchains are similar to an intranet & the Internet. An intranet is an internal, permissioned internet. On the other hand, the Internet allows for information to be freely and openly transferred. It is clear which implementation of the underlying technology was successful. A closed network is not necessary when you can securely transact value on an open standard (i.e., protocol).

Growth of a private network

There are instances where enterprises want to create a consortium of businesses that can transact on a private blockchain. As power is distributed to various entities in the closed network, consensus mechanisms will need to be added (i.e., how do we come to an agreement). As the private network grows, the group will need to adopt similar consensus and security incentives as public blockchains, especially if participants are added that are untrusted and power shifts away from a single authority. Now you start to see similar negative performance tradeoffs, without the benefit of an open, standardized, and decentralized ledger. Additionally, creating a blockchain for each business relationship will cause a proliferation of peer-to-peer networks that won't be interoperable. It's comparable to creating an intranet with each business relationship when a business could simply communicate over an established, standard and secure protocol like the Internet.

As an aside, enterprise blockchains tracking physical goods take this effort a step further in the wrong direction. Practically, it's the "garbage-in, garbage-out" problem. A blockchain is only as good as its inputs. Tying physical goods to a blockchain requires physical inputs to be translated into digital records, the same as a traditional database. Putting the records in sequential order does not solve this problem. If less than a few entities already control the records, this can be achieved with a traditional database.

Private enterprise blockchains are either just a permissioned, internal database or a subscale semi-private blockchain that will eventually need all the same public incentives mechanisms as it grows. Enterprise blockchain applications make performance improvements by sacrificing the very innovation that came with the implementation of public blockchains: the ability to create a shared agreement on a digital record without a central trusted third-party.

The downfall of a narrative

In summary, a blockchain is a data structure; like all technologies, the implementation is key to its impact. Bitcoin and other public cryptoassets employ incentive structures that remove trusted third parties from the network. Public blockchains are primarily valuable for creating non-sovereign digital assets, but other public applications may come. These future applications cannot remove the asset from its underlying blockchain without surrendering trust and control.

With all emerging technology, it is important to consider the rapid evolution that will occur; we are still in the early days of public blockchains. Public blockchains' speed, cost, and scalability are showing promising signs of improvement, with many technical advancements and research making its way to production. Private enterprise blockchains are frequently just expensive permissioned databases capitalizing on the blockchain hype or will need to adopt the same incentive mechanism that requires performance tradeoffs. The linear improvement in data structure has already drawn attention away from the exponential improvement and value creation by public cryptoassets. Private blockchains completely miss the global decentralized network of digital value transfer and storage being built before our eyes.