timechain : a decade of misunderstanding blockchain

Gaurav Rana

Oct 9, 2018 · 6 min read

Abstract: The term "blockchain" has caused much confusion and damage due to its failure to accurately capture the core characteristics of decentralized byzantine fault tolerant systems. In this article, a restoration of an older term is proposed as replacement.

. . .

A decade ago, on October 31 2008, Satoshi Nakamoto announced on The Cryptography Mailing List that they had been working on "a peer-to-peer electronic cash system," named Bitcoin. It was gradually recognized that Satoshi had made a major conceptual and technological breakthrough. Their innovation allowed, for the first time in history, for actors across wide networks to exchange value without requiring trust in a centrally controlled entity. The underlying basis of the technology consisted of a ledger that could be appended but never retroactively modified. The lack of central control over the system and the immutability of the ledger form the core characteristics of this technology, which are more accurately categorized as byzantine fault tolerant systems (BFTs).

Over the years, there has been an explosion of experiments adopting Nakamoto inspired innovations to a wide variety of purposes. However, there have also been a number of unfortunate developments in the field. One of them has to do with the adoption of the term "blockchain" to describe the technology underpinning other supposed "distributed ledger technologies."

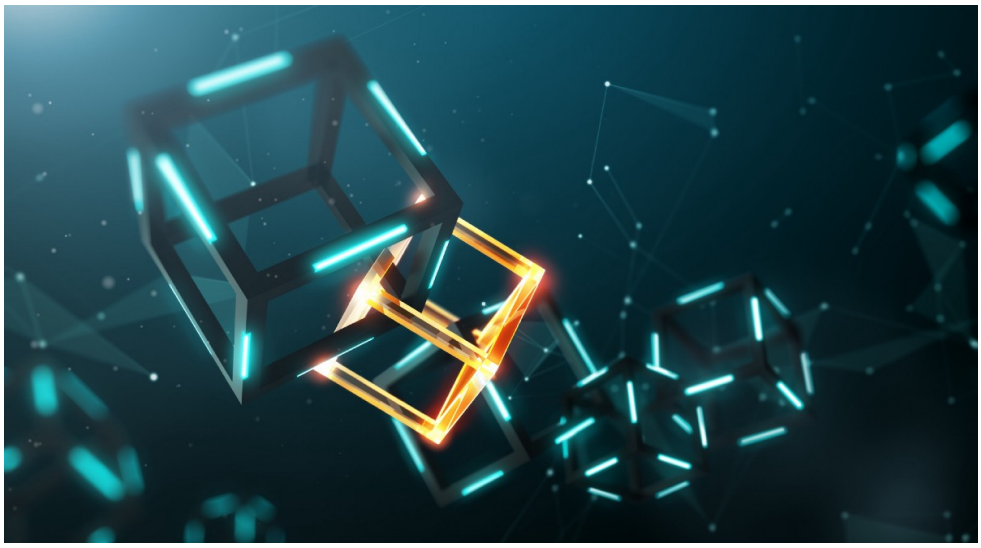
In this article, I will explain why "blockchain" is particularly poor nomenclature. Rather then providing clarity, it obfuscates. Instead of accurately delineating a sphere of technological activity that has great promise, it allows charlatans to pretend major

technologies that genuinely share the BFT ethos, if not their actual techniques. Explaining why the use of the term is not just a semantic issue but has significant practical consequences, I will propose the rehabilitation of an older term that more accurately describes the underlying keystone breakthrough.

what's wrong with "blockchain"?

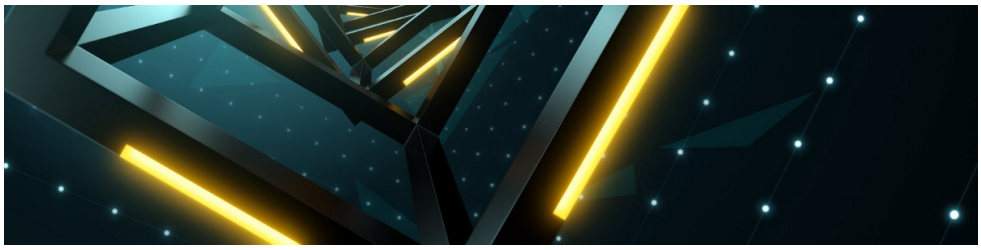
In a nutshell, the term "blockchain" merely refers to a data structure consisting of a chain of blocks.

The term does not capture the value system that make BFTs such powerful technologies, i.e. their lack of central control, their free-market, incentive based authoritativeness and, most of all, immutability.



a normal chain is only as strong as its weakest link

This ambiguity in definition has made it possible for entrepreneurs to claim usage of "blockchain technology" even when their systems are both centrally controlled and gratuitously mutable. Seemingly oxymoronic concepts such as pure "private blockchains" or "permissioned blockchains" have emerged.



a blockchain should be as strong as all of its links combined

Such technologies are gate guarded, disguised centralized Proof-of-Authority systems that almost always belie a fragile core. They violate the core BFT principles of openness, decentralization and immutability; you shouldn't claim byzantine fault tolerance if there's only one general or if the generals aren't byzantine-like in the first place. Yet, the use of the term "blockchain" has allowed creators of such technologies to pretend that they are working in the same tradition as Satoshi.

exclusion of newer technologies

On the other hand, the term "blockchain" excludes many newer technologies that share a commitment to decentralization and immutability, but do not use a chain of blocks as their underlying data structure. Directed Acyclic Graphs (DAGs) like hashgraphs, IOTA, nano, and the brand new Avalanche protocols are prime examples of collateral damage in this category.

Such technologies are thus denied participation in the tradition established by the inventors of the industry. This is unfortunate, for DAGs with right consensus controls share the core BFT principles to a much greater extent than "purely permissioned" or "purely private blockchains." They also represent some of the more exciting efforts to make the technology more scalable and energy efficient. For these reasons, it is necessary to devise a definition that classifies them together with byzantine fault tolerant systems while excluding those that fall short on decentralization or immutability.

a new term from old history

Instead of inventing a new term from whole cloth, it would be better if we could resurrect a term from the tradition that fits our needs.

Incidentally, the term "blockchain" has a much weaker presence in the historical record than is commonly supposed. Satoshi Nakamoto did use the term chain-of-blocks, global ledger, and block chain(with a space in between). However, there is zero

occurrence of the term “blockchain” in its conjugate form by Satoshi Nakamoto in the Bitcoin whitepaper, bitcointalk forum, emails, initial code, and their sourceforge entries. You can find the data and the analysis that support my claim here.

Nonetheless, they did use a different and very specific term to identify Bitcoin’s underlying technology as early as November 8, 2008. This term, in my humble opinion, far better describes decentralized byzantine fault tolerant systems. Although the term was used before any reference to “blockchain”, it has completely slipped past public consciousness and the resultant zeitgeist.

The term is **timechain**.

To give one example of Satoshi’s usage:

> *Nodes collect new transactions into a block, hash them into a hash tree, and scan through nonce values to make the block’s hash satisfy proof-of-work requirements. When they solve the proof-of-work, they broadcast the block to everyone and the block is added to the* **timechain**. *The first transaction in the block is a special one that creates a new coin owned by the creator of the block.— Satoshi Nakamoto, [bitcoin-nov08-tgz/main.h:719–724]*

why timechain?

To understand why timechain is a more accurate term , one with fewer false positives and false negatives than “blockchain,” we must first understand the importance of “authoritative order” or “authoritative chronology of events” in decentralized ledger technologies.

This may come as a surprise to a few, but there are at least two chains in Bitcoin: namely, the chain of blocks and, the chain of transactions. The latter, lesser-known chain is sufficient to trace back the entire transaction history of any given coin(s). The chain of blocks solidifies a particular chain of transactions in an authoritative order, thus preventing double spends. The chain of blocks and chain of transactions together constitute an immutable chain of events in time, or in short; a timechain. The reference to time in the terminology indicates that what has occurred cannot be erased. Events in history are as if set in stone, if not more.

DAGs, in their current implementations, include the chain of transactions but do NOT contain the chain of blocks. They have other means of ensuring the authoritativeness

and immutability of the chronology. For example, gossip based DAGs hold accountable "whom you got the transaction from" to the same extent as "what is in the transaction." It's like fulfilling the promise of "first seen, first commit rule" intimated by Satoshi, but instead, on steroids and with hard mathematical proofs. What they share in common with Bitcoin and other BFT systems is the chain of authoritative events built through time and with prohibitively irreversible chronology: the **timechain**.

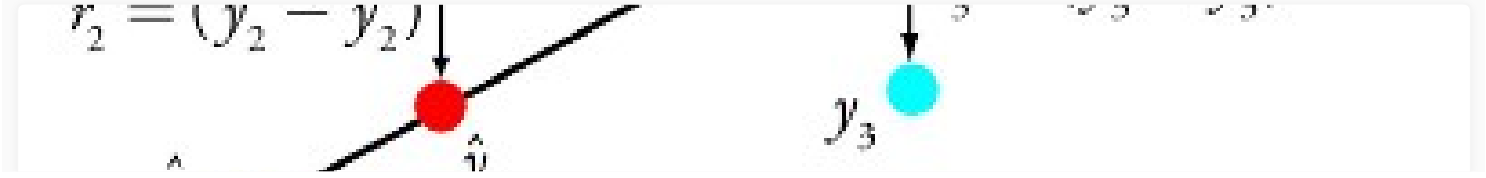
The term "timechain" commands a prerequisite of immutability. Simultaneously, it avoids a reference to blocks, thus making space for DAGs, and other future technology unrealized at the time of this post, while discarding technologies that masquerade as part of our revolution. This is the key reason to why "blockchain" as an all encompassing, industry defining, revolutionary term is flawed.

Finally, the term "timechain" originates with Satoshi and comes from a period before "blockchain" was used in its current, conjugate form. The use of the word is thus also a way of paying homage to the creators of the industry.

If nothing else, next time you come across a BFT, a DLT, or blockchain proposition, perhaps you should ask if it qualifies as a timechain.

Blockchain Bitcoin Ethereum Cryptocurrency Technology

Gaurav Rana
Medium member since Sep 2018
Decentralized Byzantine Fault Tolerant Systems. CTO @getbabb, prev CTO; @atlastogether, @everledger. Publ. Scientist; @techstars Alum.
Follow



More from Good Audience

TOP 10 Machine Learning Algorithms

garvitanand2
Feb 10 · 9 min read

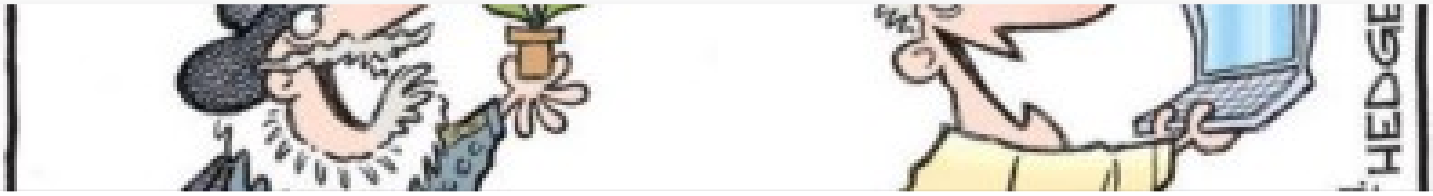
334

More from Good Audience

The biggest myths in cryptocurrency investing today and what would cause a new all time high

DK
May 29, 2018 · 20 min read

6K



More from Good Audience

My Crypto journey from 2011 to 2018

DK
May 18, 2018 · 13 min read

4.6K

Responses

Write a response...

Show all responses