COMMENTARY

OPEN ACCESS
ISSN Print: 2516-3949
doi: 10.31585/jbba-1-1-(5)2018

Why and How Blockchain?

Mark D. Wolfskehl[1] Ph.D.
CEO, Blockchain Innovations, Inc.
Correspondence: mark.wolfskehl@binv.us

Received: 19 April 2018 **Accepted:** 20 April 2018 **Published:** 23 April 2018

Competing Interests:
None declared.

Ethical approval:
Not applicable.

Author's contribution:
MW [1] wrote this commentary in entirety.

Funding:
None declared.

Acknowledgements:
None declared.

Abstract

We discuss the current state of blockchain in the technical industry and discuss blockchain's decentralization roots and its inclusion in the world of mainstream corporate technology. We include some technical background and issues in the context of the industry, feasibility, and future directions. We offer speculation as to how blockchain technology may serve various competing agendas. The purpose of this paper is to raise questions more than provide answers - to stimulate thought and discussion - in the context of the technology and its positioning in the centralisation vs. decentralisation spectrum of interests.

Keywords: *trends, analysis, opinion, technical, blockchain*

Blockchain was unleashed on the world in the form of Bitcoin in the hopes of transforming at least the financial sector of the world into a populist haven where anarchy rules and the average person does not have to become beholden to big banks, governments and other institutions for monetary needs.

In 2018 Blockchain is now mainstream where those same big banks, governments and every institution large and small, sees Blockchain as the cure for all its ills. I find this at least somewhat curious. Blockchain certainly does seem to hold potential for decentralisation of technological institutions of all sorts. This is something that would probably fit neatly along the lines of thinking of the original developer of Bitcoin. However, I think the fact that centralised institutions now find blockchain useful deserves a closer look.

Certainly, whenever there is a boom in any sector of the economy greed will rule, and people regardless of ideology will seek to cash in. But however, exciting the promise of Blockchain there is also a side of high cost. The Proof of Work algorithms central to most blockchain implementations extract a huge cost in computing power (this is the "work" of which is spoken), unusual hardware requirements, and energy consumption. Blockchain Innovations, Inc. is currently investigating how we might be able to retain or even increase the level of decentralized security provided by Proof of Work while removing, well, the work. By doing so we hope to allow the owner of the average PC without superhero-level hashing power the ability to participate and contribute to any blockchain without spending unsustainable amounts of money on graphics cards and electric bills.

It is understandable that the hashing power requirements that are currently blocking entry for "the average Joe" are easily met by large institutions. Irony aside though it is curious why such institutions would care about blockchain in the first place. Is your blockchain going to be behind a firewall? Is it going to be managed and controlled by one centralized organisation? When the application is going to be run in a centralized manner anyway, a rational individual would consider the added complexities of a blockchain implementation.

There is also a high cost for "programmer power" to implement blockchain solutions. One designs a complex blockchain solution that is broken down in a decentralized manner, throws large amounts of money at it, unusual hardware into running the software, and expends a lot of energy running a Proof of Work algorithm. In terms of "programmer power" we are not just talking about highly skilled employees who don't come cheap. There will also be a long-time lag from concept to implementation of a very complex solution. And in terms of business, doesn't time = money? The next step then is to run such a solution in a centralized data center by a single organisation. Make sense? In an age where efficient centralised server solutions are available off the shelf and are extremely cheap and easy to customise it does appear at least on the surface to have some aspects of irrationality from the economic perspective.

For those who wish to truly operate in a decentralised manner blockchain certainly make perfect sense. However, it is not my position to argue even that anyone considering a blockchain solution to be run in a centralized manner drop such plans. What I am suggesting is that the trend is curious and deserves some contemplation. Are there deeper reasons at play that are perhaps not immediately obvious?

One possibility is that one can very reasonably differentiate between blockchain as a software systems technology and cryptocurrency as a competitor for government-issued fiat. On the other hand, one might also argue that by filling the technology sphere with blockchain one obscures to oneself the fact that the basis of the technology has to date been almost exclusively in implementing cryptocurrency. However, marketing is marketing. And if the world sees the word "blockchain" more than the word "cryptocurrency" could this be viewed by "the big boys" as a good thing?

An interesting consequence though is that through this trend the number of blockchain projects can only be expected to skyrocket. This affects public projects as much as projects inside the data center, and the adoption rates of both are increasing. But perhaps this is not viewed as a problem? Because another possibility of the conscious and rational variety might be the hope that an application will develop that will take blockchain away from finance.

However, we have another trend in the technology industry today. That is one to make minimal investment and still turn around a product. One might term this the "lowest hanging fruit" approach. This is a short-sighted view that plagues the industry at the same time as the blockchain boom. And it ensures that the overwhelming majority of blockchain projects will remain in the realm of fintech for a long time to come. This in turn is going to cement blockchain's association with cryptocurrency. No significant shift will happen without a willingness to invest the time and money to reinvent (and re-code) from the bottom up.

But there are other possible explanations. Every large corporation today hires programmers. And the best programmers always want to be on top of the hottest technology. And what is the hottest technology today? Blockchain. Could this be why JP Morgan Chase developed a smart contracts system as a fork of Ethereum? It is easy to imagine some genius programmers lurking inside the closed doors begging for a chance to play with Ethereum.

This is pure speculation on my part. However, keeping the high demand developers happy for what must be an infinitesimal investment for a large bank makes perfect sense. What could be the harm? But once one has a successful project it is hard to just throw it away. And we see this in Chase's spinning off of the project now as a separate company.

On another level blockchain currently has a certain "hotness" about it, regardless of how we got here. At this tipping point one might say that the demand is such that people will jump at the opportunity to implement anything. This does require one to take the view that at least at some certain level humans are not rational creatures – not a controversial one to me personally. As we know supply must meet demand. So, I think we are going to be seeing an ongoing trend for a while where people hear the word "blockchain technology" and will immediately think of a place where blockchain must apply. Blockchain sells.

One thing is still curious, and that is that even removed from cryptocurrency the heart of blockchain is still anarchist in nature. Once put out there, it cannot be controlled. That was the point of Bitcoin in the first place. Could there be some hope amongst proponents of centralization that this nature can be changed?

The heart of the Proof of Work implementation of blockchain technology is really a very clever solution to Byzantine consensus. The best explanation I have seen to this effect is in Mastering Bitcoin by Andreas Antonopoulos [1]. However, the desire to have a "hive" of nodes cooperate in unison could also be potentially viewed as the very opposite of anarchy, perhaps even to the point of tyranny.

Does this mean that the nature of blockchain can be changed from an anarchist one, if one understands its true role in distributed systems? Distributed consensus is fundamentally a technology problem. And a solution to distributed consensus is just a tool. All tools can be used for good or for bad. But the type of consensus in Bitcoin – the emergent kind – comes from being fair and even handed. That means that (at least in theory) every node has an equal chance to have a say. So, while the "hive" can coordinate amongst itself, it is very unlikely that one individual can coordinate the hive. However, from this point of view the method of distributed consensus matters a great deal. I think this is the aspect of blockchain that is overlooked the most – for the very understandable reason that it is also the most technical. However, the fact and degree that it matters cannot be understated.

Proof of Stake is an almost drop-in replacement for Proof of Work that is currently being adopted by numerous systems. The very valid motivations previously mentioned of sustainability can easily be seen. However, it is the position of Blockchain Innovations and myself personally that Proof of Stake merely sidesteps the issue and fails to address the core problem of system security. Once a person or entity controls the largest stake can one not take over the network? Proof of Work is still the fairest solution, on a software architecture level, for emergent consensus that is widely available.

Some systems have gone back to older style messaging and leader selection models for obtaining Byzantine consensus. Such solutions are as complicated on a conceptual level as Proof of Work is unsustainable in hardware and energy. It is easy to convince oneself that Proof of Work is fair. It is not particularly dependent on network communication methods, aside from the simple need that all systems are eventually reached. After that a computational problem with random properties takes over the control mechanism in the form of a race. In the case of a protocol that is entirely dependent on a (typically very logically complicated) communications protocol fairness and even handedness is not easy to see at all. Vulnerabilities are highly likely to emerge over time. It could become very likely that even a single individual may take over the network – provided such an individual is extremely smart and insightful into the protocol.

So, we see that there exist hidden possibilities of centralization of the logical type. A warning to those with centralization interests is in order: the ability to take over a network is not without risk. Nobody can say that the takeover will be done by the intended party. The policy of maximal self-interest may still be to play fair.

Proof of Work to date appears to remain the fairest solution. But even Proof of Work is becoming de facto problematic. I have mentioned the sustainability issue a number of times. This can be stated in another manner: barrier to entry. We see that already the hardware and energy requirements in purely economic terms are hard for the "average Joe" to justify. And isn't Joe the one Satoshi Nakamoto originally had in mind to benefit the most from Proof of Work? This is a de facto issue of centralization that transcends the direct application of software architectural methods. Something must be done that addresses the barrier to entry without compromising on fairness. The solution currently under development at Blockchain Innovations addresses this issue along with the computation and energy sustainability issues while retaining the emergent consensus model embodied in Bitcoin.

In the end trends are trends and economics is economics. Making money is the game, and mutual benefit is the gain. If the forces of centralization and the forces of decentralization can approach the same technology and make advances at the same time society comes together. Peoples' fortunes across the spectrum increase. It is certainly preferable that apparently opposing forces compete on the economic playing field, one that is fundamentally peaceful.

Ultimately, what we are seeing is the emergence of an ironically symbiotic relationship in blockchain between those interested in centralization and those interested in decentralization. It is the intention of Blockchain Innovations to foster both "sides" by merely taking the attitude of contribution to the economy. By the same token, we think it is important to keep in mind that to truly be blockchain one needs to stick to the essential elements. So, we intend on the technology side to remain faithful to the principles and implementation aspects of decentralization embodied in the original Proof of Work implementation of Bitcoin. On the organizational level, we remain open and friendly to individuals and organizations regardless of placement on the spectrum of centralization vs. decentralization agenda.

People can hope. But ultimately nobody can truly know how blockchain will transform society in the long term. The exploration is exciting, and ultimately competition via peaceful means in an ever increasingly antagonistic (and so often violent) world is a good thing. We hope to see the advances continue.

References

[1] Antonopoulos, Andreas M., Mastering Bitcoin: Programming the Open Blockchain; Second Edition 2017; O'Reilly Media; Chapter 10: Mining and Consensus.