A Skeptical Look at Blockchains

By S. Keshav [*]

Blockchains are often (and uncritically) viewed as a 'unicorn' decentralized mechanism that can simultaneously provide security, fairness, verifiability, and privacy. These claims, unfortunately, do not hold up on closer examination, especially when a blockchain is embedded into the larger context of society. I demonstrate how permissionless *blockchains fall well short of their design claims. In contrast,* permissioned *blockchains do appear to meet these goals, but only by compromising on their degree of decentralization.*
JEL: Decentralization Conference

In the past few years, distributed ledgers (or *blockchains*) have drawn considerable attention for their potential to enable fair, secure, private, verifiable, and highly-decentralized systems; additionally, they permit very low transaction fees due to the disintermediation of trusted but rent-seeking third-parties (Underwood (2016)). Many experts claim that these technologies will cause fundamental changes to industries ranging from finance and real-estate to energy and transportation (Tapscott and Tapscott (2016)).

The thesis of this abstract is that, on closer examination, and especially when public (permissionless) blockchains are embedded into society, the reality is far less impressive. This strongly suggests that attention be paid, instead, to private (permissioned) blockchains, which are more centralized but also more robust.

We focus on Bitcoin, not only because it is the first, best-known, and most widely-used public blockchain, it is also a bellwether whose failure likely to drag down all other public blockchains with it. How well do its claims of functionality hold up under scrutiny?

Decentralization: Centralized systems demand trust in the center; decentralized systems diffuse the need for trust and, *ceteris paribus* are preferable. Although Bitcoin's design permits radical decentralization, it incentivizes the formation of stable coalitions, known as 'mining pools.' Hence, in practice, control of the chain rests in a handful of entities that are unregulated, free to collude, and potentially susceptible to coercion or corruption.

Fairness: Bitcoin, in theory, permits anyone to become a member of the system and 'mine' for token rewards. In practice, its hashing lottery is highly biased towards entities that own specialized hardware, out of reach of the general population. Moreover, the chain preferentially incorporates transactions

[*] School of Computer Science, University of Waterloo, 200 University Ave. W, Waterloo, ON N2L 3G1, Canada, keshav@uwaterloo.ca.

that pay higher transaction fees, making the platform inaccessible to poorer segments of society.

Security: Bitcoin's security claims rest on the assumption that honest miners control more than 50% of hashing power and that its cryptographic primitives are unbreakable. Both claims are potentially weak. Collusion between a handful of the top mining pools breaks security and can result in a near-instant and catastrophic loss of faith in Bitcoin. Moreover, with quantum computing, the cryptographic foundations of Bitcoin are also under attack. However, decentralization makes it challenging for the system to upgrade to quantum-safe cryptographic primitives.

Privacy: Bitcoin uses public keys as identities, which is pseudonymous and ostensibly private. In practice, tracking the flow of transactions between public keys makes it relatively straightforward to de-anonymize these entities Narayanan et al. (2016).

Verifiability: As long as hash functions cannot be tampered with using backdoors or quantum computing, Bitcoin's verifiability claims are indeed solid.

To summarize, four out of five of Bitcoin's top-line claims fail to hold up under scrutiny. Moreover, Bitcoin mining has an unacceptably large carbon footprint, and the technology has primarily been adopted by an unsavory assortment of libertarians, drug dealers, and arms merchants.

For these reasons, although there are numerous alternative blockchain proposals that address these lacunae, it may be best to abandon radical decentralization as a design goal and focus instead on *permissioned* blockchains that allow transactions amongst and on behalf of clients of a loose coalition of known, vetted, and regulated principals. By achieving consensus on transaction ordering without requiring cryptocurrency incentives and mining lotteries, they have a minuscule carbon footprint with strong security and verifiability. Moreover, they can permit fair access with low transaction fees. Being better aligned with legacy financial, legal, and corporate structures, they are more likely to bring blockchain's undeniable benefits to the masses. Thus they are more deserving of society's and our interest, analysis, investment, and adoption.

REFERENCES

Narayanan, Arvind, Joseph Bonneau, Edward Felten, Andrew Miller, and Steven Goldfeder. 2016. *Bitcoin and cryptocurrency technologies: a comprehensive introduction.* Princeton University Press.

Tapscott, Don, and Alex Tapscott. 2016. *Blockchain revolution: how the technology behind bitcoin is changing money, business, and the world.* Penguin.

Underwood, Sarah. 2016. "Blockchain beyond bitcoin." *Communications of the ACM*, 59(11): 15–17.