Blockchain and prudence

Subhashis Banerjee* Subodh Sharma†

February 5, 2022

Blockchain is a fascinating data structure that undeniably generates great curiosity in computer science, social and political sciences, and public policy. However, the hype around it, and its faith-based adoption for almost anything driven by unsubstantiated vendor and consultant claims, are bewildering and risky. They perhaps stem from both an inadequate understanding of the blockchain properties and imprecise articulations of application requirements.

In essence, a blockchain is a sequential append-only public bulletin board of transaction records with two main functional properties. First, what can get added is reconciled by multiple participating peers following a pre-decided consensus protocol. This process cannot be gamed under the assumption that a majority of the unrestricted number of peers are honest. Second, the bulletin board is immutable; once a record is added it is cryptographically ensured that it cannot be altered. Each participating peer normally has their own copy of the entire bulletin board, with identical content, and they can read and further copy at will.

A 'permissioned' or private blockchain has only pre-identified participating peers. Hence collusion is possible and integrity can only be ensured through regulations. Without political decentralization consensus does not imply safety, and this is no different from centralization in its threat model.

Despite claims to the contrary, the blockchain structure has nothing to do with the highly nuanced notion of privacy, or even the limited secrecy aspect of it. To ensure secrecy of the bulletin board records, one has to fall back on traditional and well established notions from cryptography – like encryption, key management and zero-knowledge proofs – and these techniques are not limited to blockchain. Decentralized consensus is orthogonal to the issue, and privacy is not an ensuing property of a blockchain.

'Consensus' is inapplicable when there is only one authority responsible for the integrity of the transactions, for example the ECI when a vote is cast in the privacy of a polling booth or a person is added or removed from a voters list. The claims of security based on blockchain are orthogonal to the verifiability requirements in voting, and despite the near consensus against their use, the multitude of proposals on using blockchains for elections are disconcerting. Also, voting is not the only example of inadequate analysis of applicability of blockchain, and there are proposals for using them for land records, asset registers etc. Most such proposals do not pass muster for reasons similar to voting. Indeed, a 2018 study found hardly any successful use cases.

The role of blockchain in RBI's digital currency proposal is similarly doubtful, and convincing methods independent of 'consensus' need to be developed to ensure the correctness and verifiability of transactions while protecting user privacy.

What may help in many of these applications is just the immutable public bulletin board part of blockchain, with or without encryption and zero-knowledge proofs. This may be simply achieved

*Computer Science, Ashoka University, Plot #2, Rajiv Gandhi Education City, P. O. Rai, Sonepat, Haryana 131029 (on leave from IIT Delhi). Email: suban@ashoka.edu.in

†Computer Science and Engineering, IIT Delhi, New Delhi 110016. Email: svs@iitd.ac.in

by the concerned authority periodically publishing the bulletin board in a publicly downloadable forum, and using hash chains verifiable by all to make alterations impossible.

Cryptocurrencies do make valid use cases for blockchains, though the political decentralization of participants is questionable. It also raises other concerns. Currency properties and monetary policies have evolved over thousands of years of bartering, and it is not clear that cryptocurrencies are consistent with them or that the larger macroeconomic implications of cryptocurrencies are well understood. Crypto assets derive their values from their potential to be exchanged for other currencies. However, since only a limited set of commodities are traded with crypto assets, and that too only by a privileged section of the world population, their price determination with respect to sovereign fiat currencies are uncertain. Apart from the crucial price stabilization issues, their potential to further inequality is also considerable.

Moreover, an asset becomes valuable when it is scarce and there is a demand. The scarcity of cryptocurrencies arise from the computational hardness of currency mining, of the process of solving a hash puzzle. And, there is clearly a perceived demand, not unlike gold. However, gold mining not only involves labour, material and energy, but there also are other requirements like environmental and other regulatory clearances, import regulation etc. In contrast, mining in cryptocurrencies is achieved by spinning the CPUs and thereby consuming electricity. The total carbon footprint is equivalent to that of a few megacities, and it does seem ungainly, energy-inefficient and unsustainable to mine assets this way. Surely, this requires regulation and taxation, especially for the potential environmental impacts and because only a few participate? It is amazing that the cryptocurrency research and deployment has not adequately addressed these concerns to develop sound theories for their regulation.

Blockchain is certainly an elegant concept whose properties and potential require careful research. However, the overall hype of treating them as solutions for everything with not-so-thoughtful use cases is perhaps techno-determinism at its worst.