Making the Blockchain Ecosystem Secure, Scalable, and Sustainable

Shin'ichiro Matsuo

Abstract

In place of the centralized computation of the Internet's current architecture, blockchain could be used to implement self-resilient or self-operating systems, as it upkeeps states with highly resilient mechanisms by design. Despite blockchain's potential to correct problems associated with the current Internet ecosystem, there are several issues that need addressing within the blockchain ecosystem. These include security; the tradeoff between scalability and decentralization; and sustainability.

Keywords: blockchain ecosystem, smart contract, proof-of-work mechanism

1. Potential and issues regarding the blockchain ecosystem

Whether you are interested in blockchain or not, there are several reasons for engaging with it. Cryptocurrency, smart contracts, and non-fungible tokens (NFTs) rely upon this distributed ledger-based technology, and it could have revolutionary implications for global networking and information technology (IT) companies, and the Internet at large.

The Internet, for instance, was originally designed to achieve global networking without a single point of failure (SPOF). However, the current problem for the ecosystem over the Internet is that tech giants have in effect become such SPOFs. Hence, there is a continued need for extensible trust without these risky flaws. In place of the centralized computation of the Internet's current architecture, blockchain could be used to implement self-resilient or self-operating systems, as it upkeeps states with highly resilient mechanisms by design.

Despite blockchain's potential to correct problems associated with the current Internet ecosystem, there are several issues that need addressing within the blockchain ecosystem. These include security, broadly understood; the tradeoff between scalability and decentralization; and sustainability.

2. Security and cryptography

Studies conducted on the formalization of blockchain security requirements have largely neglected to consider the entire technology and all its systems. While this does not necessarily imply insecurities, it means we are unable to demonstrate that blockchain does not contain vulnerabilities.

The presence of risk applies not only to blockchain specifications but also to its implementation. The attack in 2016 on a decentralized autonomous organization illustrated the possibility of exploiting vulnerabilities in the Ethereum blockchain code. Because of

the pervasive role that blockchain is expected to play as a social infrastructure tool, the impact of security incidents could increase dramatically. This means there is a need for vulnerability-handling procedures to ensure the quality of code and respond to attacks when they occur.

There also needs to be a standard operating model regarding the use of cryptography. When the IT industry transitioned from secure hash algorithm (SHA)-1 to SHA-2 several years ago, following a reported compromise of SHA-1, the Bitcoin and blockchain engineering community for the most part lacked the experience, mechanisms, and operations to do likewise.

With quantum computing looming as a long-term threat, the digital signature schemes used in blockchain technologies could also become insecure. Efforts to develop post-quantum cryptographic techniques are underway. The U.S. National Institute of Standards and Technology (NIST), for instance, has selected post-quantum finalists covering public-key encryption and digital signatures. Because long-term operations are assumed with blockchain applications, it is important to transition to equally long-term, secure cryptographic techniques. Cryptographic agility, which means a level of flexibility when the underlying cryptography is compromised, should be implemented into blockchain technology, operations, and governance mechanisms.

3. Scalability vs. decentralization

The blockchain ledger is processed according to a specified rule of processing speed. (In the case of Bitcoin, 1-MB block of data is added every 10 minutes.) This upper bound on the maximum number of transactions per unit time effectively puts a limit on scalability, which advancing computing power cannot overcome.

One solution is to increase the size of the block by changing its specifications. However, this would increase the amount of data stored at all user nodes. This could result in only wealthy individuals or parties having the resources to operate the nodes, which in turn decreases their number. A solution involving fewer nodes would therefore contradict the original "decentralization" philosophy of permission-less blockchain, making such blockchains less secure.

The trade-off between scalability and decentralization is related to design philosophy. Reducing the number of nodes or setting multiple nodes in the same cloud computer (to achieve greater scalability) may destroy one of the prime merits of public blockchain, namely, the removal of centralized operators. It is, therefore, crucial to consider the cost-merit balance of introducing such a semi-decentralized blockchain when we expand its applications.

4. Sustainability

From an environmental perspective, there is concern about whether the proof-of-work (POW) blockchain consensus mechanism used by Bitcoin is sustainable given the tremendous amount of energy consumed in mining these digital assets. The alternative proof-of-stake (POS) mechanism is much more energy-efficient; however, POS faces numerous implementation challenges, including confirmation delays.

From a business perspective, public blockchain systems such as Bitcoin are considered self-resilient because their protocols implement fees for operations through self-issuing crypto assets. A capital growth theory analysis indicates that blockchain systems are usually sustainable, although stakeholders unconstrained by certain standard rules of business (such as those involving taxes, energy costs, or risk of bankruptcy) could undermine a chain's viability. Similarly, if we were to see a so-called selfish mining attack on the POW mechanism, it could lead to the collapse of a chain, another limit on sustainability. It is also worth mentioning that the use of blockchain by itself, for instance in NFTs or self-executing contracts, does not guarantee outcomes that could be characterized as fair. Achieving fair outcomes calls for appropriate design considerations.

What that also means is that in addition to further analysis, we are likely to need regulations in this field. If we are interested in a new type of public, self-resilient Internet infrastructure mentioned at the start of this article, we may need to upgrade blockchain.

Shin'ichiro Matsuo
Senior Scientist, Head of blockchain research, Cryptography and Information Security Laboratories, NTT Research, Inc.

He is the head of blockchain research at NTT Research. He is also a research professor at Georgetown University, Washington, D.C., USA, and works as a director and blockchain research lead of CyberSMART research center at Georgetown University. He has been engaged in research on cryptography and cryptographic protocols for over 23 years. He was a program chair of Scaling Bitcoin workshop 2019 and program committee member of many blockchain-related academic conferences such as IEEE Security & Privacy on the Blockchain, International Workshop on Cryptocurrencies and Blockchain Technology (CBT), Stanford Blockchain Conference and Crypto Economics and Security Conference. He is also a co-founder of BSafe.network, which is the global and neutral academic research testbed dedicated to blockchain research. As editor and project leader, he oversees two technical reports on the security of blockchain technology at ISO TC307.