

Economic Incentives and Blockchain Security

Abstract

Much like steam engines and the internet, blockchain has emerged as a disruptive technology and a foundation for tomorrow's businesses and ecosystem.

Blockchains meld technology and economics to provide unprecedented security guarantees. As individuals seek to reduce uncertainties, economic incentives can drive human behavior, and act as the enablers of personal security, either perceived or real. Since cryptographies are hackable, a truly secure, decentralized, and automated blockchain protocol can be established only when significant security guarantees, using inherent economically incentivized consensus mechanisms, are combined with cryptographic guarantees.

Since hacks are a reality and cannot be completely prevented when the economic gain is large, we decided to explore the possible consequences for the network if a private or permissioned blockchain is compromised as they currently do not employ economic incentives:

- 1. Blocking consensus:** Transactions are validated and added to the secure ledger when a majority of nodes, sign a block (deterministic blockchain) or add them to the blockchain (probabilistic blockchain). In a common private network with 10 to 20 nodes, transactions will fail even if only 4 to 7 nodes are compromised. Therefore, in a high-volume, high-value use-case such as equities settlements, there could be significant damage, especially as participants begin to panic, and there is a likelihood that trading will be halted on an exchange platform.
- 2. Manipulating consensus:** If consensus is compromised:
 - a. Transactions can be censored long enough to cause significant financial harm, especially where time is of essence such as in high frequency trading use cases.
 - b. 'Bad' transactions can be accepted as valid, 'good' transactions can be manipulated, and malicious ones can be created to favor one or more counterparties.
- 3. Transaction censoring by manipulating the order of the leader node:** In Practical Byzantine Fault Tolerance (PBFT) or PBFT-like consensus models, each new block or transactions group is created and broadcasted to the network from a temporary 'leader' node. If the leader node fails to produce blocks within a predetermined time interval, the consensus protocol selects a new leader to propose new blocks. Although there are multiple algorithms that can determine the new leader node, if the leader selection can be 'guessed' based on known parameters, the leader can be compromised to favor malicious nodes instead of honest ones. Such attacks can lead to similar consequences as mentioned above when it comes to censoring or manipulating transactions.
- 4. Manipulating smart contract code by a non-census number of nodes:** Smart contract code can be manipulated inside its container to create transactions that conflict with other transactions on different network nodes. This can lead to rejection of blocks as the proof-of-correct-execution on the different nodes will contradict information that is stored in other network nodes. Such circumstances

result in transaction censoring, delays, and cancellations in transaction execution, ultimately causing inefficiencies, long-term financial harm and stakeholders' distrust in the network.

5. Manipulating or spoofing proof-of-correct-execution:

This scenario is a variant of the previous scenario, where the smart contract container is not compromised but the generated transactions are censored and replaced by malicious transactions. As a result, an incorrect 'world state' among the network's nodes leads to the same outcomes as in the previous scenario.

6. Corrupting notary nodes in DLT networks: Notary solutions in distributed ledger technology (DLT) implementations promise to sign on any transaction sent to them if three conditions are satisfied – the inputs specify the notary, no other transaction previously signed by the notary consumes any of the same inputs, and the transaction is valid. If a notary is compromised, it might for example either refuse to sign transactions that it should sign and censor truthful transactions, or sign malicious transactions that may cause double spending.

7. Manipulating data oracles: Smart contracts rely on data supplied by sources, known as 'data oracles'. If this data is manipulated through a Man in the Middle (MiM) attack, at the source or before it reaches the smart contract, it can block actions or trigger them at the wrong time. This can cause, significant operational or financial damage in addition to participants losing trust in the network. Such a scenario is inherent to any blockchain with a (quasi) Turing-complete compute framework, irrespective of whether it is private or public.

8. DDOS attacks on honest nodes: A private blockchain hosted on a private network behind a firewall, is not at a significant distributed denial-of-service (DDOS) attack risk, unless it is communicating through public IPs over the internet. Under such circumstances, a DDOS attack can paralyze the entire network and prevent transactions from being confirmed if honest nodes are brought down or stalled, or if the attack is followed up by a MiM attack, spoofing the public IP to incoming packets and rerouting traffic.

Building a Reliable Blockchain Protocol by Applying Inherent Economic Incentives

The guiding security principle for blockchain protocols must be the reduction of risks that cause significant process or financial harm to network participants and platform stakeholders, whether the network is private or permissioned.

To state this differently, every blockchain should incorporate a design principle in which the marginal cost of malicious behavior of network nodes must be equal to, or better yet, significantly higher than, any possible marginal gain derived from such malicious behavior.

One way to achieve this goal is to build economic incentives into the network protocol. For instance, trusted network nodes should be asked to deposit a bond into an escrow account to build this additional layer of economic security. The value of the bond should be proportional to the economic value that the node is gaining from the platform, for a certain length of block history. This means that a node not only underwrites the overall value of the block or equivalent DLT groups it signs, but rather it does so for a certain length of platform operating time. Doing so significantly mitigates the risk of long-range attacks on the network, and is in line with the method followed by many proof-of-stake consensus algorithms such as Casper¹ or Tendermint².

The argument that a node needs to underwrite the value of several blocks or groups of transactions it validates seems to be straightforward, as nodes should be held accountable for any transactions they validate. In fact, given the real time nature of today's transactions, waiting for a legal entity to rule in favor of a damaged party could take much too long. All participating nodes should agree to abide by the rules laid out in the protocol and its consensus algorithm. Failure to prevent malicious behavior during a node's operation should lead to forfeiture of a node's bond to the benefit of the other network participants, in real time and in a decentralized manner.

Another factor to be considered is the additional security requirement for underwriting a history of blocks. This seems to be counterintuitive in the existing financial regulatory framework. Currently, markets demand unconditional settlement finality of transactions, which relieves counterparties of their liabilities only when all the assets in a transaction have been settled. However, settlement finality in

the real world is always probabilistic as settlement records, and no matter what form they are kept in, stand a chance of being manipulated maliciously. Therefore, it is important to account for the possibility of such a scenario in a blockchain context and to apply the economic incentives' security principles to it as well. As a result, if one node or a sufficient majority-consensus of nodes manipulate transaction history and are found out, they will be penalized through a similar mechanism to the one mentioned above.

Up to this point, we have only spoken about economic incentives with regard to risk mitigation but not as a revenue incentive for stakeholders. While an economic revenue incentive is always required for a public blockchain, it's a nice-to-have feature for a permissioned or private blockchain because the business motives for the private network's participants are significantly different from those of a public network. However, this does not prohibit adding additional revenue incentives through native currency tokens to the consensus algorithms such that network users pay for the upkeep and maintenance of the network, one transaction at a time.

Nurturing Blockchain Platforms

Economic incentives add critical economic security guarantees to technology in a private or permissioned blockchain scenario. To ensure this, beyond the typical technical evaluation, we always need to analyze new platforms from a game theory perspective, such that all stakeholders reach their Nash equilibrium³ and their expected actions benefit the entire ecosystem. Such an analysis is typically not carried out at the moment. Hence, currently most private or permissioned blockchain platforms security levels are insufficient for enterprise risk departments, which usually lack the relevant experienced blockchain talent and expertise, to sign-off on blockchain production implementations, especially due to the many unknowns involved in these deployments.

The current situation is an opportunity for service providers to fill in the gap and enable their clients to design proper economically incentivized consensus algorithms for blockchain production systems, and guide them, from ideation to POC and finally to production.

References

- [1] LinkedInEthereum Blog, Introducing Casper "the Friendly Ghost", August 1, 2015, <https://blog.ethereum.org/2015/08/01/introducing-casper-friendly-ghost/>, accessed June 13, 2017
- [2] The Blockchain, Tendermint Consensus without Mining, <http://www.the-blockchain.com/docs/Tendermint%20Consensus%20without%20Mining.pdf>, accessed June 13, 2017
- [3] PNAS, Equilibrium points in n-person games, <http://www.pnas.org/content/36/1/48.full>, accessed June 14, 2017

About The Authors

Dr. Andreas Freund

Dr. Andreas Freund is the TCS 2017 Distinguished Engineer for his contributions to blockchain technology, digital identity and building the TCS Co-innovation Network (COIN™) blockchain ecosystem, a seasoned business leader and Six Sigma Black Belt. He has a proven international record of over \$500M in enterprise value enhancements, leading multiple successful business and technology transformations, M&A, restructuring and continuous improvement initiatives. He now specializes in creating exponential organizations and innovations through rapid digital strategy development and implementation spanning Fortune 500 to private equity companies with a focus on blockchain technology and its business models.

Gal Mordechai

Gal Mordechai is a Senior Strategic Business Manager at Tata Consultancy Services' (TCS) Next Generation Strategy Practice and focuses on blockchain and its impact on organizations and business processes. In his role, Gal assists clients from various industries to understand blockchain technology and its disruptive power, develop new business strategies and use cases around it and design executional roadmaps to utilize its cross-industry effect on clients' business models and operations.

Experience certainty. IT Services
Business Solutions
Consulting

Contact

Visit the [Consulting & System Integration](#) page on www.tcs.com

Email: global.consulting@tcs.com

Blog: [#Enterprise Insights](#)

Subscribe to TCS White Papers

TCS.com RSS: http://www.tcs.com/rss_feeds/Pages/feed.aspx?f=w

Feedburner: <http://feeds2.feedburner.com/tcswhitepapers>

About Tata Consultancy Services Ltd (TCS)

Tata Consultancy Services is an IT services, consulting and business solutions organization that delivers real results to global business, ensuring a level of certainty no other firm can match. TCS offers a consulting-led, integrated portfolio of IT and IT-enabled, infrastructure, engineering and assurance services. This is delivered through its unique Global Network Delivery Model™, recognized as the benchmark of excellence in software development. A part of the Tata Group, India's largest industrial conglomerate, TCS has a global footprint and is listed on the National Stock Exchange and Bombay Stock Exchange in India.

For more information, visit us at www.tcs.com

All content / information present here is the exclusive property of Tata Consultancy Services Limited (TCS). The content / information contained here is correct at the time of publishing. No material from here may be copied, modified, reproduced, republished, uploaded, transmitted, posted or distributed in any form without prior written permission from TCS. Unauthorized use of the content / information appearing here may violate copyright, trademark and other applicable laws, and could result in criminal or civil penalties. Copyright © 2017 Tata Consultancy Services Limited