Tiramisu: Layering Consensus Protocols for Scalable and Secure Blockchains

2022 IEEE International Conference on Blockchain and Cryptocurrency (ICBC) | 978-1-6654-9538-7/22/$31.00 ©2022 IEEE | DOI: 10.1109/ICBC54727.2022.9805562

Anurag Jain
IIIT Hyderabad
anurag.jain@research.iiit.ac.in

Sanidhay Arora
University of Oregon
sanidhay@uoregon.edu

Sankarshan Damle
IIIT Hyderabad
sankarshan.damle@research.iiit.ac.in

Sujit Gujar
IIIT Hyderabad
sujit.gujar@iiit.ac.in

***Abstract*—Cryptocurrencies are poised to revolutionize the modern economy by democratizing commerce. These currencies operate on top of blockchain-based distributed ledgers. Existing permissionless blockchain-based protocols offer unparalleled benefits like decentralization, anonymity, and transparency. However, these protocols suffer in performance which hinders their widespread adoption. In particular, high time-to-finality and low transaction rates keep them from replacing centralized payment systems such as the Visa network. Permissioned blockchain protocols offer attractive performance guarantees, but they are not considered suitable for deploying decentralized cryptocurrencies due to their centralized nature. Researchers have developed several multi-layered blockchain protocols that combine both permissioned and permissionless blockchain protocols to achieve high performance along with decentralization. The key idea with existing layered blockchain protocols in literature is to divide blockchain operations into two layers and use different types of consensus to manage each layer. However, many such works come with the assumptions of honest majority which may not accurately reflect the real world where the participants may be self-interested or rational. These assumptions may render the protocols susceptible to security threats in the real world, as highlighted by the literature focused on exploring game-theoretic attacks on these protocols. We generalize the "layered" approach taken by existing protocols in the literature and present a framework to analyze the system in the BAR Model and provide a generalized game-theoretic analysis of such protocols. Using our analysis, we identify the critical system parameters required for a distributed ledger's secure operation in a more realistic setting.**

I. Introduction

Bitcoin [1] promised to transform the financial system by proposing a decentralized peer-to-peer currency. *Miners* maintain this system by honestly following the underlying consensus protocol through appropriate incentives/rewards. In Bitcoin, and similar cryptocurrencies such as Ethereum, every miner validates transactions and tries to append a set of valid transactions to the set of validated transactions, i.e., append a block on the blockchain. These miners compete against one another in a "mining" game. Typically, these miners have to produce "Proof of Work" (PoW) to write new transaction data to the blockchain.

As of December 2021, Bitcoin's and Ethereum's network processes up to 4 and 15 transactions per second (TPS), respectively [2], [3] whereas Visa's global payment system handles 1,700 TPS [4]. Besides, using such cryptocurrencies for real-time retail payments is not feasible as the protocols only provide *eventual consistency*. Each transaction requires a certain number of block confirmations to be confirmed; Bitcoin needs at least 60 mins to confirm a transaction.[1]

Researchers have proposed several multi-layered protocols to improve blockchain technology's practical performance for better applicability [5], [6], [7], [8]. These protocols combine both permissioned and permissionless protocols to achieve scalability while maintaining decentralization. With inspiration from these works, we abstract out this layered approach and formalize these layers for different functions of the system, which lead us to a general framework we term as *Tiramisu*.

We highlight that these works do not provide a game-theoretic analysis to ensure incentive compatibility, i.e., all the above protocols assume miners are either honest or byzantine. However, the miners may be rational or self-interested players. That is, they may deviate from the prescribed protocol to gain additional *rewards* because it may not be a strategic miner's *best response* to follow the protocol honestly. A system is said to be *incentive compatible* if it rewards each player greater for playing truthfully as compared to all other possible strategies. We remark that designing such incentive-compatible blockchain protocols that are robust to strategic deviations is a significant challenge. It is also a new area of research with limited prior work [9], [10].

Motivation. Overall, we observe that building a scalable, consistent, and fully decentralized practical blockchain protocol remains elusive. Cryptocurrencies like EOS [11], DFINITY [6], Solida [5], etc. have a committee-based blockchain protocol. Among these, PeerCensus [7], and Hybrid Consensus [8] inherently use a layered approach that demonstrates its potential benefits by achieving higher throughput and faster block confirmations. We highlight none of these works provide a game-theoretic analysis to ensure incentive compatibility and thus, security in the presence of *rational* miners – the ones maximizing their rewards. Hence, the scalability guarantees provided by these protocols might not hold if the protocol is not incentive compatible.

Tiramisu: Overview. We believe that with a layered approach, one can create protocols that offer the best of both worlds: throughput and decentralization. We dub this approach as "Tiramisu" after the layered dessert.

More concretely, Tiramisu consists of two layers: Access Control Layer (ACL), and Consensus Later (CSL). In ACL, we run a permissionless consensus protocol to obtain authorized

The work done when Sanidhay was student at IIIT Hyderabad
978-1-6654-9538-7/22/$31.00 ©2022 IEEE

[1] It is also referred to as time to finality.

nodes. Then, with CSL, these nodes form a committee to run a BFT consensus protocol on the state of the system. We identify three conditions, which we call *NIC Conditions*, in our game-theoretic analysis that ensure incentive-compatible implementation of any Tiramisu protocol. As our framework is general, one can use any permissioned blockchain protocol in CSL, as long as it satisfies NIC Conditions. As standard, our security analysis assumes that ACL is secure. This assumption is based on inherent security guarantees of the underlying consensus protocol that must be carefully employed in the protocol design.

A. Contributions.

Our contributions are as follows:

- We abstract out the essentials of a layered approach to combine multiple protocols for improved performance of blockchain ecosystem and propose a framework, namely *Tiramisu*.
- Along similar lines, we present general conditions on protocol parameters, rewards, and the fraction of honest nodes to ensure an incentive-compatible instantiation of a Tiramisu framework. Our analysis considers three types of nodes: rational, honest, and Byzantine.
- Under the reasonable assumption that the protocol designer uses a secure protocol in ACL, we provide a rigorous security analysis formalism for Tiramisu such that the overall system is secure.
- Analysis with the Tiramisu framework also helps identify the optimal parameters for a multi-layered blockchain protocol to ensure maximal performance within safe operation.

II. Tiramisu: A Layered Approach

In Tiramisu, we split the operation of the blockchain into two independent layers, the Access Control Layer (ACL) and the Consensus Layer (CSL), respectively. ACL manages nodes in the network via a permissionless consensus protocol. Whereas CSL employs a permissioned consensus protocol among the authorized nodes from the first layer. These nodes will run a byzantine agreement protocol to verify transactions and reach a consensus on the state of the system.

A. Access Control Layer (ACL)

ACL is responsible for providing sybil-resistant node identities to CSL. The identity of these *nodes* are simply a derivative of the public key of a public-secret-key pair $\langle pk, sk \rangle$, owned by a participant. Each node is identified by its public address.

In this layer, participants maintain a separate blockchain to obtain sybil-resistant identities. Participants in this layer run any permissionless blockchain consensus protocol by choice of protocol design, denoted by Π_{ACL}. Note that Π_{ACL} must satisfy some pre-defined conditions. Towards stating these pre-defined conditions, we first describe a *democratized resource*. These network resources must be directly proportional to the fraction of control that they gain over the protocol Π_{ACL}. Typically Π_{ACL} can be a proof-of-X base protocol like Proof-of-Work or application-specific alternatives like Proof-of-Location [12].

Operation. Π_{ACL} is run to determine the identities of the nodes participating in CSL. Each block in the blockchain of this layer must contain a single public address representing the identity of the node that wishes to join the CSL. Once a block reaches finality, ACL uses a pre-defined interface to interact with CSL and propose the identity present in this block to join the committee in CSL. Observe that any participant will only invest their network resources for the identities of the nodes that they wish to get promoted in CSL. The key insight behind the sybil-resistant nodes is that the democratized resources are hard to obtain and may not be scaled at will. Observe that the probability of a node joining the CSL is directly proportional to the amount of democratized resources owned by the participant, denoted by $\alpha_{participant}$.

B. Consensus Layer (CSL)

This layer is responsible for handling transactions and reaching a consensus on the state of the system. The nodes in this layer are controlled by participants. This layer maintains a shared state of the system by running any Byzantine agreement protocol or BFT protocol, denoted by Π_{CSL}. One can use any BFT protocol suited for the permissioned blockchain setting as long as it satisfies the network model. The shared-state can only be modified by pre-determined operations. This shared-state can consist of anything related to the purpose of the protocol like running a cryptocurrency, notarization platform, smart-contract platform, etc.

We now claim that the Tiramisu protocol satisfies the properties of *safety* and *liveness* associated with distributed ledgers []. BFT protocols structure their execution into a sequence of views, each with a designated leader process. These protocols guarantee safety and liveness by ensuring that all correct nodes eventually overlap in a single view, with the right leader, for enough time to reach consensus.

Claim 1. *A Tiramisu protocol session achieves safety and liveness if* Π_{CSL} *does so.*

We describe the three conditions on protocol parameters that ensure incentive compatible deployment of a Tiramisu protocol.

NIC Conditions. We identify three conditions that ensure that following a Tiramisu protocol honestly is the Nash Equilibrium, (i.e., it is Nash Incentive Compatible NIC). *NIC-Conditions* are based on the following requirements: (i) to ensure that Π_{CSL} is secure, (ii) to ensure that rational nodes attain non-negative utility when they deviate from following the honest strategy, (iii) to ensure that each rational node must obtain positive utility. In particular, NIC conditions are:

1) **Faithful Fault Tolerance Condition** $n_{\mathcal{B}} < n_f$
2) **Maximum Payload Condition** $\phi \leq \frac{\kappa_{\mathcal{R}} \cdot \delta_{min}}{c_{val}}$
3) **Minimum Reward Condition** $TR \geq \phi \cdot c_{val} + \frac{c_{mine}}{n_{TX}}$

Theorem 1 (Informal)**.** *The Faithful Fault Tolerance Condition, Maximum Payload Condition and Minimum Reward Condition are sufficient to ensure that the protocol is NIC.*

We refer the reader to the full version of our paper at [13] for more details.

REFERENCES

[1] S. Nakomoto, "Bitcoin: A peer-to-peer electronic cash system," https://bitcoin.org/bitcoin.pdf.

[2] *Blockchain Charts*, 2020, https://www.blockchain.com/charts/transactions-per-second.

[3] *Ethereum Daily Transactions Chart — Etherscan*, 2020, https://etherscan.io/chart/tx.

[4] *VisaNet Booklet*, 2021, https://usa.visa.com/dam/VCOM/download/corporate/media/visanet-technology/visa-net-booklet.pdf.

[5] I. Abraham, D. Malkhi, K. Nayak, L. Ren, and A. Spiegelman, "Solida: A Blockchain Protocol Based on Reconfigurable Byzantine Consensus," in *21st International Conference on Principles of Distributed Systems (OPODIS 2017)*, ser. Leibniz International Proceedings in Informatics (LIPIcs), J. Aspnes, A. Bessani, P. Felber, and J. Leitão, Eds., vol. 95. Dagstuhl, Germany: Schloss Dagstuhl–Leibniz-Zentrum fuer Informatik, 2018, pp. 25:1–25:19. [Online]. Available: http://drops.dagstuhl.de/opus/volltexte/2018/8640

[6] M. M. Timo Hanke and D. Williams, "Dfinity technology overview series consensus system." CoRR abs/1805.04548 (2018), 2018. [Online]. Available: https://arxiv.org/pdf/1805.04548.pdf

[7] C. Decker, J. Seidel, and R. Wattenhofer, "Bitcoin meets strong consistency," in *In Proceedings of the 17th International Conference on Distributed Computing and Networking Conference (ICDCN)*. ICDCN, 2016. [Online]. Available: https://tik-db.ee.ethz.ch/file/ed3e5da74fbca5584920e434d9976a12/peercensus.pdf

[8] R. Pass and E. Shi, "Hybrid Consensus: Efficient Consensus in the Permissionless Model," in *31st International Symposium on Distributed Computing (DISC 2017)*, ser. Leibniz International Proceedings in Informatics (LIPIcs), A. W. Richa, Ed., vol. 91. Dagstuhl, Germany: Schloss Dagstuhl–Leibniz-Zentrum fuer Informatik, 2017, pp. 39:1–39:16. [Online]. Available: http://drops.dagstuhl.de/opus/volltexte/2017/8004

[9] S. Siddiqui, G. Vanahalli, and S. Gujar, "Bitcoinf: Achieving fairness for bitcoin in transaction fee only model," in *Proceedings of the 19th International Conference on Autonomous Agents and Multiagent Systems, AAMAS '20, Auckland, New Zealand, May 9-13, 2020*, A. E. F. Seghrouchni, G. Sukthankar, B. An, and N. Yorke-Smith, Eds. International Foundation for Autonomous Agents and Multiagent Systems, 2020, pp. 2008–2010.

[10] A. Jain and S. Gujar, "Block rewards, not transaction fees keep miners faithful in blockchain protocols," in *GTiB@WINE 2020*, Beijing, China, 2020.

[11] *Documentation/TechnicalWhitepaper.md*, 2020, https://github.com/EOSIO/Documentation/blob/master/ TechnicalWhitePaper.md.

[12] D. Chatzopoulos, A. Jain, S. Gujar, B. Faltings, and P. Hui, "Towards mobile distributed ledgers," *IEEE Internet of Things Journal*, 2021.

[13] A. Jain, S. Arora, S. Damle, and S. Gujar, "Tiramisu: Layering consensus protocols for scalable and secure blockchains," 2022. [Online]. Available: https://arxiv.org/abs/2203.10765