IJCRT.ORG ISSN : 2320-2882

INTERNATIONAL JOURNAL OF CREATIVE RESEARCH THOUGHTS (IJCRT)

An International Open Access, Peer-reviewed, Refereed Journal

Zero-Trust Architectures Integrated With Blockchain For Secure Multi-Party Computation In Decentralized Finance

Syed Khundmir Azmi[*]

Aark Connect, USA

Abstract

This paper focuses on integrating Zero-Trust Architecture (ZTA) and blockchain technology to improve the security and reliability of Secure Multi-Party Computation (MPC) in Decentralized Finance (DeFi). Traditional security models are unsuited to the decentralized and trustless nature of the DeFi model where MPC can take place providing privacy-preserving financial operations whilst still absorbing sensitive data which is exposed. By pairing together ZTA's "never trust, always verify" philosophy and blockchain's immutable, transparent ledger, we propose a many layered architectural schema that would provide for continuity in verification, decentralized policy enforcement and tamper proof auditing. The integration addresses important security issues like the misbehavior of nodes, input corruption, and collusion, and encouraged scalability, compliance, and resilience. Practical feasibility of the approach is demonstrated by case studies of projects such as Chainlink DECO and Threshold Network. Besides its application in finance, the proposed model provides potential implications for DeFi and other privacy-sensitive fields that require clinicians' trust when storing and accessing data.

Keywords: Zero-Trust Architecture, Blockchain, Secure Multi-Party Computation, Decentralized Finance, DeFi Security, Privacy-Preserving Computation

1. Introduction

1.1. Overview of Decentralized Finance (DeFi)

Decentralized Finance (DeFi) has emerged as a revolutionary paradigm, harnessing the power of blockchain technology to disintermediate conventional financial intermediaries, and build open, permissionless, and composable financial ecosystems. By leveraging smart contracts on distributed ledgers, DeFi platforms provide a wide range of services, such as lending, borrowing, trading, and asset management, without the need for centralized institutions (Chen & Bellavitis, 2020).

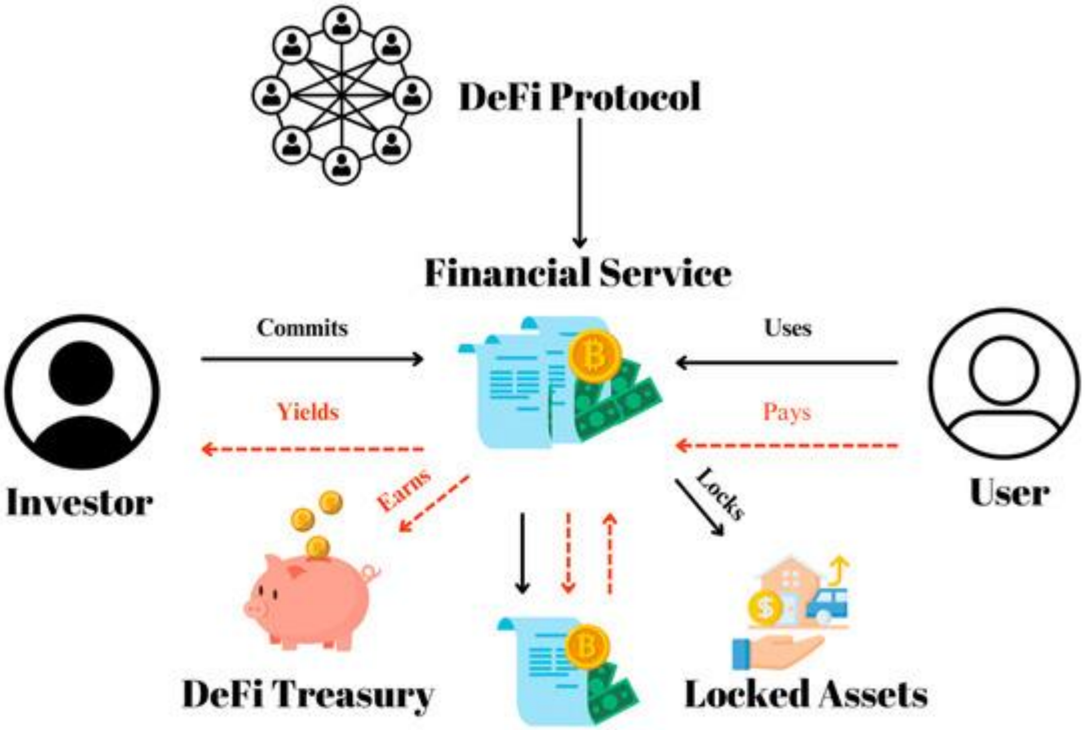

Figure 1: Decentralized Finance (DeFi) common mechanism and revenue strategy

The value of the total value locked (TVL) of de-thriving applications has held its peak at tens of billions of dollars, reflecting its market adoption and ability to change the way global finance operates (Qin et al., 2021). However, this unprecedented innovation and growth has significantly outpaced the development of viable security frameworks, making billions of dollars in digital assets extremely vulnerable to exploitation.

1.2. Importance of Security in Multi-Party Computation

A central feature of the functionality that enables many advanced DeFi applications is Secure Multi-Party Computation (SMPC). SMPC enables several parties to share one function over their private input while concealing the private input from one another. In DeFi it is essential for purposes such as decentralized dark pools, private evaluation of creditworthiness, collective management of valuable assets, as well as secure oracles. The security of the SMPC protocols should be paramount, because if it were compromised, it might expose large amounts of sensitive financial data, collusion or manipulation of the computed result in catastrophic financial losses and loses trust in the whole decentralized system.

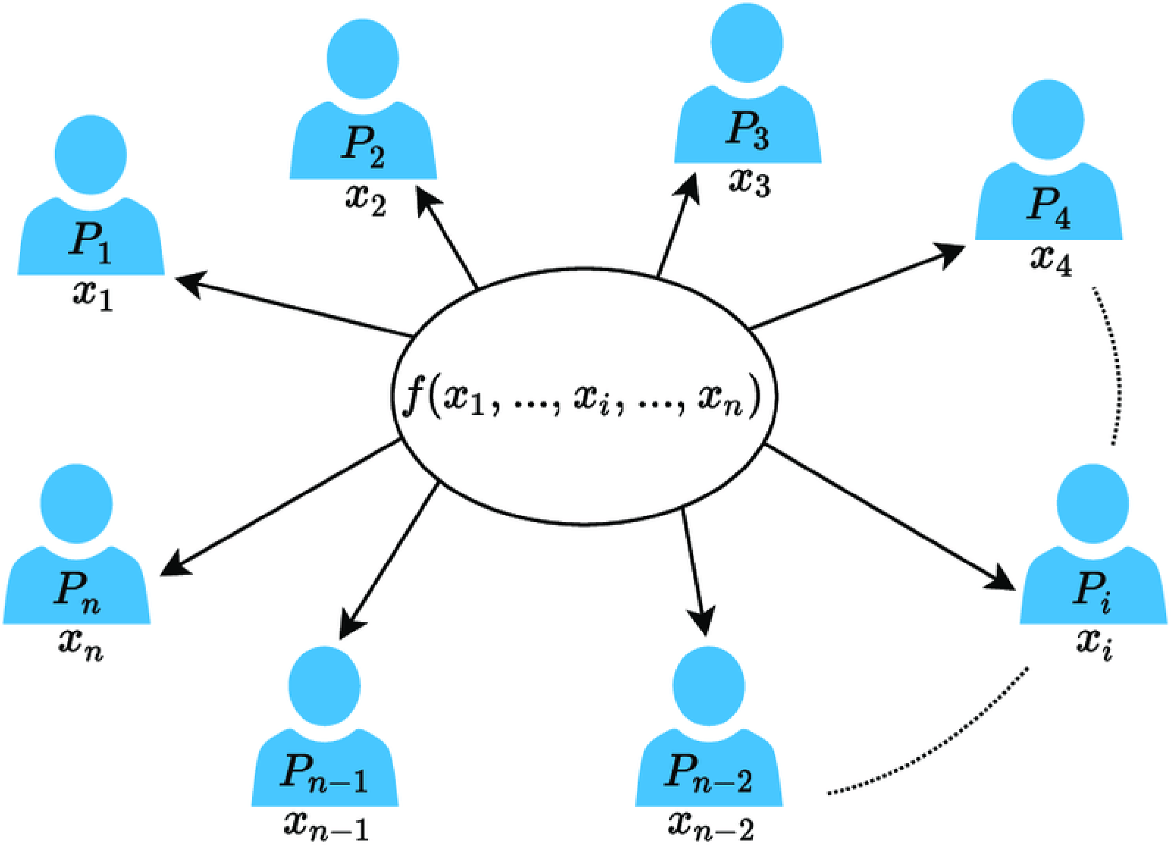

Figure 2: Secure multi-party computation (Example)

1.3. Introduction to Zero-Trust Architecture (ZTA)

The traditional perimeter-based security model, which assumes trust within a network boundary, is fundamentally incompatible with the decentralized and transparent nature of blockchain and DeFi environments. Zero-Trust Architecture (ZTA) addresses this inadequacy by operating on the principle of "never trust, always verify." A ZTA mandates that no entity, whether inside or outside the network perimeter, is granted implicit trust. Instead, all access requests have to be authenticated, authorized, and encrypted prior to granting them, and as guided by strict identity and context-aware policies (Rose et al., 2020). This model is especially appropriate for dynamic and distributed systems such as DeFi, that postulate participants are anonymous and untrusted by default.

1.4. Significance of Integrating Blockchain Technology

While ZTA offers a powerful security framework, its application to a trustless multi-party environment such as DeFi needs a decentralized and tamper-proof mechanism to manage identity, enforce policies, and record transactions. Blockchain technology has these features inherently available. Its immutability guarantees audit trails are unforgeable, its consensus mechanisms allow a single source of truth when it comes to policy definitions and its smart contracts can automate the enforcement of zero trust policies (e.g. access grants, attestation checks), in a transparent and deterministic way. Therefore, the pairing of ZTA with blockchain represents a synergetic security model: as the blockchain implements the decentralized "trust layer" for the execution of policies, ZTA implements the strong "security principles" of access control, together enabling verifiably secure SMPC in high-stakes de-fi applications. This paper delves into this integration, suggesting a new architecture, and testing its effectiveness in addressing the current security threats in the DeFi space.

2: Fundamentals of Zero-Trust Architectures

2.1. Definition and Core Principles of Zero-Trust

Zero-Trust Architecture (ZTA) is a strategic cybersecurity initiative that removes the concept of trust from the network architecture of an organization. Rooted in the principle of 'never trust, always verify', ZTA requires that no entity - be it inside or outside of the network perimeter - is granted implicit access to resources. Every access request should be fully authenticated, authorized and then encrypted prior to granting the request (Rose et al., 2020). This is a fundamental change from the more traditional approach to security models that view the world as a series of perimeters (a "castle and moat" model, for example) and assume that all internal users and devices are to be trusted.

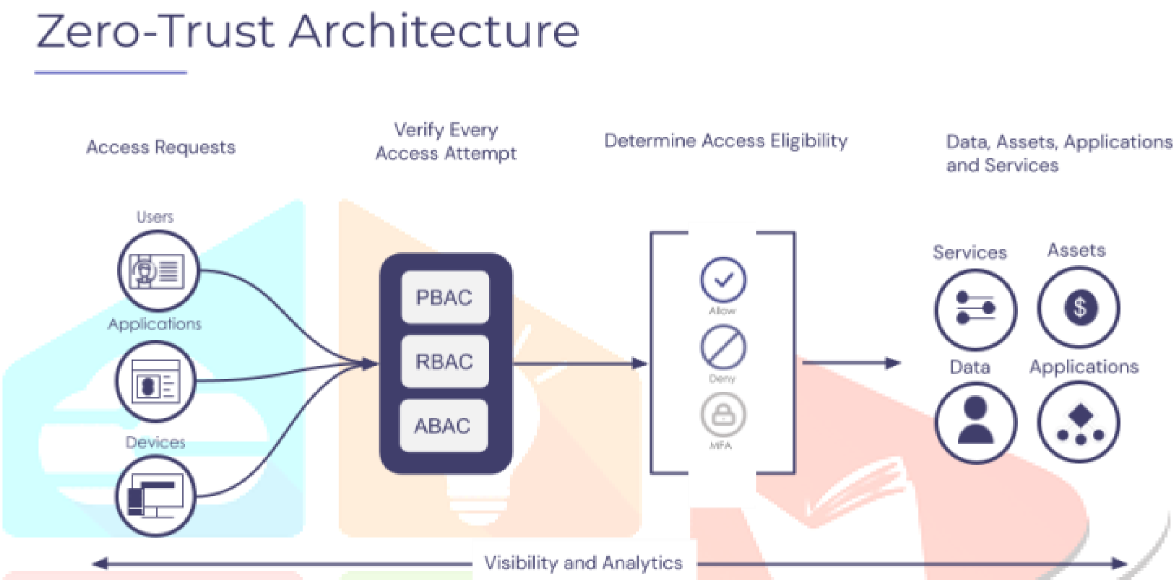

Figure 3: Zero Trust Architecture

The fundamental principles of ZTA, as defined by the National Institute of Standards and Technology (NIST), are to assume a hostile environment, that a local network location is not automatically trusted, and that access had better be sternly enforced based on dynamic policy evaluation (Rose et al., 2020).

2.2. Historical Context and Evolution of ZTA

Zero Trust was officially coined by Forrester Research analyst John Kindervag in 2010, though Zero Trust can really be applied to concepts that have been around for much longer - the concepts of least privilege and need-to-know access (Kindervag, 2010). The formalization and adoption of ZTA was given a significant boost with the publication in 2020 of the NIST SP 800-207 that delivered a formal framework and architecture recommendations, transitioning the concept from a marketing term form towards a defined standard for enterprise security (Rose et al., 2020). More recently, ZTA has been developed to solve the security issues of distributed systems, such as IoT networks and cloud-native environments, so it's become very relevant for decentralized architectures such as blockchain.

2.3. Key Components of Zero-Trust Models

The implementation of a Zero-Trust model is facilitated by several interdependent technological components that work in concert to enforce the core principles.

2.3.1. Identity Verification: Scarcity of trust identity is the foundation of ZTA. Every application workload, device, and user (referred to as a "subject") should require verification for identity before granting any access request. This will extend to usernames and passwords being replaced with MFA (Multi-Factor Authentication), biometrics, and device health attestation. In a decentralised context, this can correspond to the concept of cryptographic identity verification with the help of public/private key pairs, by means of which digital signature is a strong and cryptographically verifiable proof of identity.

2.3.2. Least Privilege Access: The principle of least privilege ensures that subjects receive only minimum access as low as needed to accomplish the subject's specific function for the lowest duration possible in order to accomplish the function. This is usually enforced by micro-segmentation and attribute based fine grained access control (ABAC) policies. Micro-segmentation separates workloads into secure zones, isolating workloads and providing visibility and stopping lateral movement of an attacker that breaches the network once in place. ABAC policies consider access requests taking into account dynamic attributes (user role, device security posture, hour of the day, location, etc.), rather than static roles, as is the case in static and role-based policies.

2.3.3. Continuous Monitoring: ZTA is not a one and done with authentication event but rather a continuous check and validate scenario. This gives the ability to dynamically modify access rights; for instance, if a user's device is discovered to be running vulnerable software in a mid-session the access might be revoked or downgraded automatically. This element plays an important role in getting into a breach mindset and reducing the impact potentially caused (Rose et al., 2020).

3. Blockchain Technology in DeFi

3.1. Overview of Blockchain Fundamentals

Each module does the following: At its core, a blockchain is described as a distributed, immutable and transparent digital ledger that records transactions in an unchangeable, and permanent fashion. The chain of blocks contain a cryptographically hashed batch of transactions. Each block contains the hash value of the previous block, forming a cryptographically interlinked chain whereby any data from the past is extremely resistant to tampering (Tapscott & Tapscott, 2020). Consensus mechanisms, such as Proof-of-Work (PoW) or Proof-of-Stake (PoS) are core protocols that can become a successful network of distributed nodes to agree on the validity of transactions and current state of the ledger without a central authority (Antonopoulos & Wood, 2023). This is the combination of cryptographic linking, decentralization and consensus that is the trustless foundation that Decentralized Finance is built upon.

3.2. Role of Blockchain in Decentralization

Blockchain is the power technology behind decentralization in DeFi. It does it by committing the ledger to a network of nodes in a peer-to-peer network; each computer keeps an identical copy of the entire history of transactions. This architectural choice removes single points of failure and control forcing any single entity to unilaterally modify the ledger or censor transactions (Zheng et al., 2023). Decentralization is further operationalized with the use of smart contracts-self-executing code encompassing the blockchain network which automatically enforces the terms of an agreement. This means that smart contracts essentially replace traditional financial intermediaries (e.g., banks, brokers), programmatically instead harvesting a logic of loans, trades and investments in a DeFi, thus the operation is done exactly as programmed, transparently and without human intervention (Qin et al., 2021).

3.3. Benefits of Using Blockchain in Financial Transactions

The digital transformation of finance caused by the implementation of blockchain represents a whole number of ground-breaking benefits that have the capability to reimagine the foundations of classical banking institution structures by maximizing trust, effectiveness, and innovation. Its transparency and auditability are guaranteed as all authenticated transactions are indelibly stored on a public ledger that can be accessed and audited by any party for real-time protocol and transaction auditing purposes to reduce the potential avenues of hidden fraud while also boosting user confidence (Chen & Bellavitis, 2020).

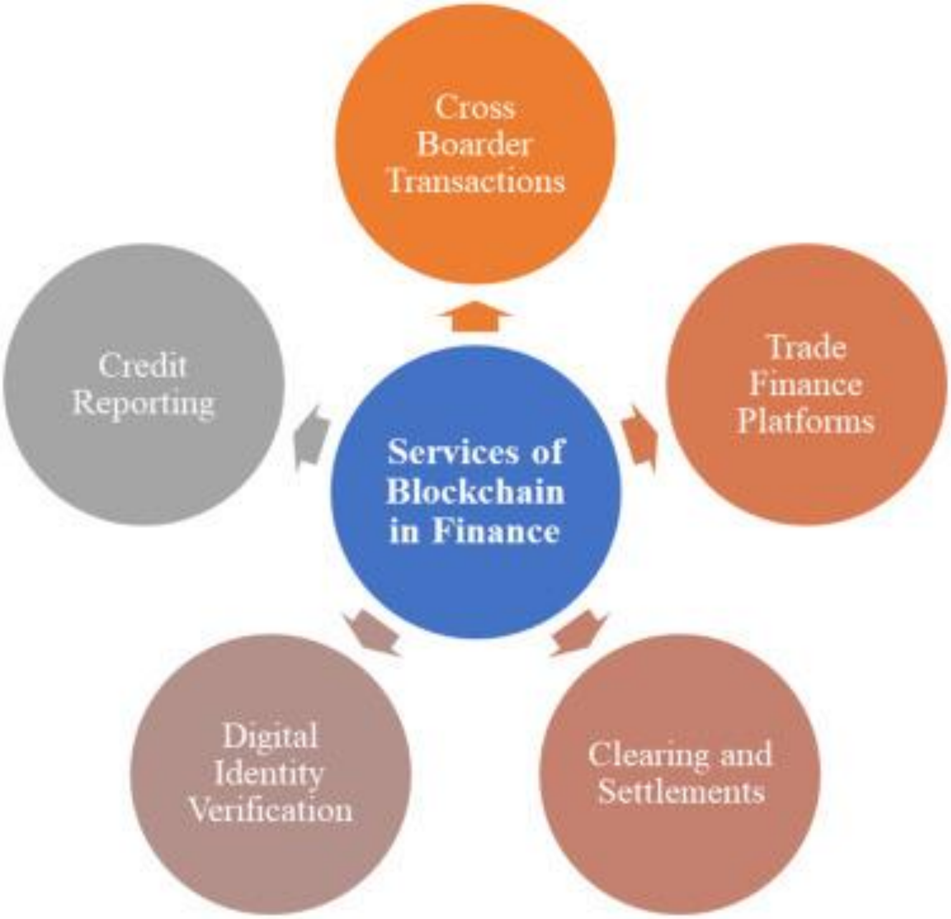
Cross Boarder Transactions
Trade Finance Platforms
Clearing and Settlements
Digital Identity Verification
Credit Reporting
Services of Blockchain in Finance

Figure 4: Benefits of Using Blockchain in Finance

Furthermore, its unalterability and finality of transactions in blockchain technology ensures that once confirmed, a transaction cannot be reverted thereby preventing the occurrence of fraudulent chargebacks and also ensuring the finality of settlement which is essential for the stability in the financial sector (Werner et al., 2021). In addition to this, due to its decentralized nature, blockchain offers censorship resistance so that it can't be easily blocked or reverted to by governments or corporations which can be an advantage in areas with unstable or authoritarian financial systems. Finally, its programmability via smart contracts supports the creation or financial instrumentation that promotes composability, automation and the usage of what is often termed "money lego" during which new financial innovation would be accelerated with the integration and expansion of new financial instruments and products (Schar, 2021).

3.4. Challenges and Limitations of Blockchain in DeFi

While blockchain technology promises to revolutionize the way we conduct business and finance, it also presents a number of challenges that are stalling its mass adoption in the decentralized finance (DeFi) space now. Consequently low transaction throughput and high latency that emerges in major public blockchains like Ethereum of cause severe congestion and prohibitively high transaction fees at peak times, virtually making micro-transactions and HFT economically impractical (Gudgeon et al., 2020), which is one of the major challenges. Besides scalability, another key constraint is linked to the security threats that smart contracts have been provoking; although the blockchain is extremely secure, smart contracts are tied to the most exploited attack vector in DeFi: susceptible traps such as reentrancy attacks, logic attacks and oracle attacks have cost the stakeholders billions of dollars (Qin et al., 2021; Zhou et al., 2023). Another area of concern is the fact that, as a lot of DeFi runs on transparent blockchains, there is no privacy about transactions and wallet balances - even if they are pseudonymous - which is likely to be of concern to individuals and institutions, as it discloses their trading strategy or their financial position (Kappos et al., 2022). Additionally, regulatory uncertainty still puts DeFi's long-term sustainability under a shade with its decentralized and borderless capabilities, taxation, anti-money laundering (AML) and Know Your Customer (KYC) requirements being hard to comply and questions around legal responsibility and enforcement remaining unanswered, representing a formidable obstacle to widespread institutional adoption (Zetsche et al., 2020).

4: Multi-Party Computation (MPC) in Finance

4.1. Definition and Importance of MPC

Secure Multi-Party Computation (MPC) is a very basic cryptography protocol, which provides the ability to jointly compute a function over private input data by a set of different parties while ensuring confidentiality of their inputs. The key security guarantee of MPC is that no one gains any information regarding the secrets of others whereas anything other than what can be deduced from the result of the computation itself (Evans et al., 2018). Such capability is revolutionary in the world of finance.

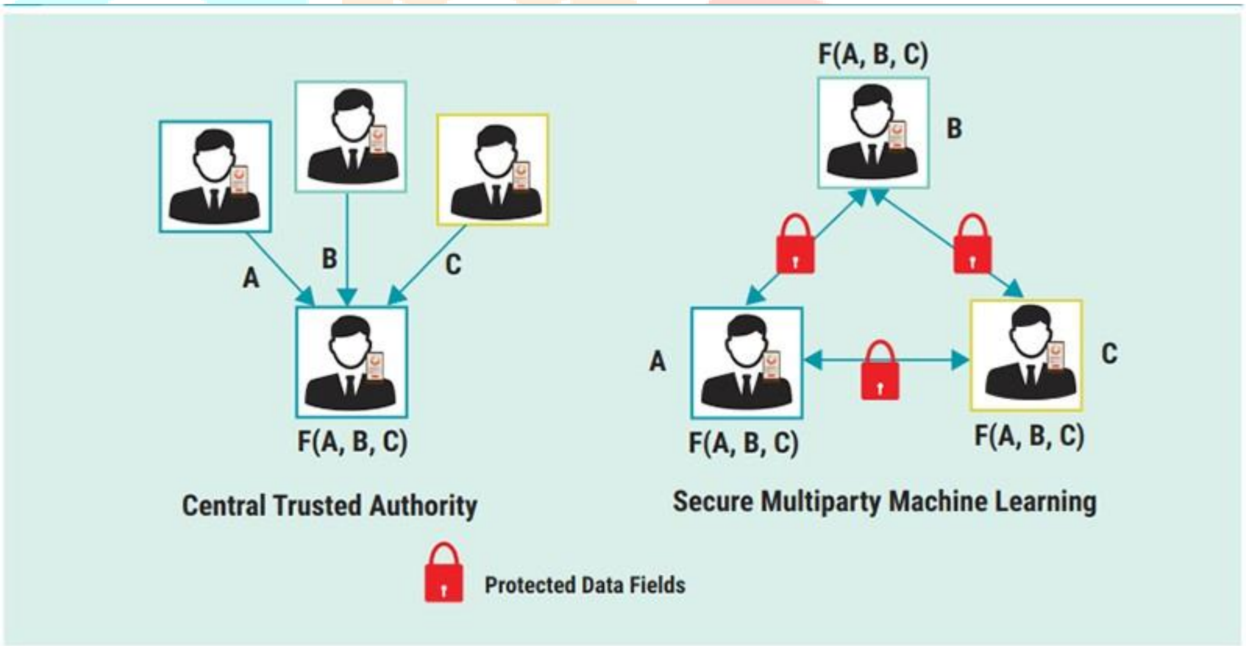

Figure 5: Central trusted Authority and secure multiparty ML

Through this peer-to-peer platform, mutually distrusted entities, whether they are rival financial institutions, individual traders or individual data providers, can analyze and gain value-added information from their data to each other without having to disclose sensitive commercial or personal information to a central trusted entity or to the others. This circumvents the classical data utility versus data privacy. Making MPC an integral component of privacy-preserving finance, just as it has been in other applications in recent times.

4.2. Use Cases of MPC in Decentralized Finance

The application of Multi-Party Computation (MPC) in the power of decentralized currency finance (DeFi) creates a new space for advanced, secure, and privacy-preserving financial products that address certain limitations of existing blockchain systems. In decentralized exchanges (DEXs), MPC makes it possible to match orders and complete trades without revealing the entire order book and trading intentions of the parties, to prevent them from being front-run by others and avoid negative influence on the market as a whole. In addition, in private credit and lending, borrowers are able to privately calculate credit scores across various data sources (including traditional credit history and chain data) without sharing personal or financial sensitive information with lenders or MPC operators, making it both privacy saving and fair. MPC also enhances the reliability of secure oracles by enabling different oracles to compute tamper-resistant aggregate median asset prices without disclosing their own inputs, greatly mitigating manipulation risks and eliminating the single points of failure (Breidenbach et al., 2021). Moreover, for institutional-grade funds, MPC can enable decentralized funds to conduct collective decision-making processes like portfolio rebalancing pricing where investors can vote/authorize trades weighted by their holdings - a key necessity for large investors needing confidentiality (Baum et al., 2020). Taken together, these use cases point to the promise of MPC to contribute to trust, security, and privacy for DeFi while driving adoption by retail and institutional actors.

4.3. Security Challenges Associated with MPC

While Multi-Party Computation (MPC) protocols are theoretically secure, when applied to the decentralized finance (DeFi) scenario, they face a series of practical concerns that can compromise their adoption in an adversarial environment. One key concern is input corruption and freezing where a malicious participant may feasibly fail to provide its input after observing inputs of other participants, preventing the computation from crystallizing altogether, or purposefully providing corrupted input for manipulating the output (Cramer et al., 2020). Even worse, there lies the threat of collusion since many MPC protocols rely on the assumption that the malicious parties only constitute a minority, in a permissionless, anonymous, DeFi world, it is intrinsically hard to guarantee no collusion among node operators and there is a risk of reconstruction of private inputs. In addition to such adversary, another common attack is that MPC systems, as any cryptographic software, have the ability to suffer from the drawbacks of the bugs or it being not implement correctly following formal models and thus will be open to attacks in unexpected manners and hence disclose sensitive information. Finally, the computationally intensive nature of MPC makes it susceptible to denial-of-service (DoS) attacks, whereby adversaries can overwhelm node operators by initiating large volumes of MPC sessions, effectively crippling availability and disrupting DeFi applications dependent on continuous, secure computation. These challenges underscore the gap between the theoretical security of MPC and its resilience in real-world DeFi deployments, highlighting the need for further research and robust engineering practices to ensure reliability at scale.

4.4. Integration of ZTA and Blockchain in MPC

The integration of Zero-Trust Architecture (ZTA) with blockchain technology presents a robust framework to mitigate the security challenges of MPC in DeFi. This integration creates a layered security model:

4.4.1. Blockchain as the Policy and Audit Layer: The blockchain acts as a decentralized, immutable authority for managing the rules of the MPC network. Smart contracts can be used to:

Enforce Node Eligibility: Establish and verify a process (e.g. staked collateral, proven identity) for determining eligibility of a node to join an MPC committee; limiting the risk of Sybil attacks and sub-standard participants

Manage Access Policies: Encode ZTA principles such as least privilege in the MPC protocol itself The smart contract can then dynamically assign nodes to computation according to their attested security posture and permissions required.

Provide Auditable Logs: To transparent and tamper-proof audit trail for compliance and forensic analysis, record MPC executions metadata and pass it on-chain (e.g., participants, function computed, success/failure).

4.4.2. ZTA Principles for Continuous Verification: ZTA components are applied to the MPC node network:

Identity and Device Attestation: Each node thus has to continuously not only give its identity but also demonstrate that its software/hardware environment is valid, so that the MPC pool can build an environment trust relationship between each member and network. This works to reduce the risk of accidentally input corruptology by attackers nodes.

Micro-Segmentation: The MPC nodes can be micro-segmented to only allow communication as much as is required for the protocol and preventing a lateral movement in case one of the nodes is compromised.

Continuous Monitoring: Node behavior during computations can be inspected for anomalies (e.g. significant latency, departing from the protocol). Smart contracts can be programmed to slash the stake of, or kick out nodes with malicious behaviour, as attested by a consensus of honest nodes.

This synergistic integration guarantees that trust is not entrusted in any single entity and is interspersed and verified by cryptographic proofs (known as blockchain) and continuously-enforced security policies (known as ZTA) hence creating a secure and resilient environment to apply MPC in DFi.

5 Integrating Zero-Trust with Blockchain for Secure MPC

5.1. Architectural Framework for Integration

The integration of Zero-Trust Architecture (ZTA) with blockchain for Secure Multi-Party Computation (MPC) necessitates a layered, synergistic architecture that moves beyond traditional models. This framework consists of three core layers:

5.1.1. Blockchain Policy and Audit Layer: This is the very foundation "trust anchor." A smart contract on a blockchain (commonly called a Policy Administration Point (PAP), and Policy Decision Point (PDP) in ZTA parlance) is the decentralised authority. It codifies the rules for participation such as eligibility criteria for nodes (e.g. a minimum amount of stake, attestation of identity) logic for assigning MPC tasks and punishment for misbehaviour. Its immutability enhances the policy integrity.

5.1.2. Zero-Trust Enforcement Layer: This layer is made up of the network of MPC nodes themselves which each could be a Policy Enforcement Point (PEP). Before participating in any computation, each node would need to cryptographically prove its identity and provide attestation proving its security posture (e.g. software versions, secure enclave measurements) to the blockchain policy contract. Communication between nodes is micro-segmented and encrypted by following the principle of least privilege.

5.1.3. MPC Execution Layer: This layer is made up of the network of MPC nodes themselves which each could be a Policy Enforcement Point (PEP). Before participating in any computation, each node would need to cryptographically prove its identity and provide attestation proving its security posture (e.g. software versions, secure enclave measurements) to the blockchain policy contract. Communication between nodes is micro-segmented and encrypted by following the principle of least privilege.

5.2. Mechanisms for Ensuring Security and Trust

The security of the integrated model is enforced through several key mechanisms:

5.2.1 Decentralized Identity and Attestation: Each MPC node operator must possess a decentralized identifier (DID) and verifiable credentials (VCs) that attest to their identity and their machine's compliance with security standards (e.g., running specific trusted execution environments like Intel SGX). The blockchain smart contract verifies these credentials before granting permission to participate.

5.2.2 Staking and Slashing: Nodes are required to stake a rather large amount of cryptocurrency in the form of a security bond. The smart contract automatically "slashes" (confiscates) part (or all) this stake if the node is proven (by cryptographic or by consensus of honest nodes) to have behaved maliciously, for example, by giving incorrect inputs, or refusing to provide outputs or outputs. This economic disincentive makes interpret individual behavior of nodes consistent with network security.

5.2.3 Continuous Behavioral Monitoring: In real-time, both other nodes in the MPC committee as well as off-chain "watchtower" services can monitor the performance and outputs of the nodes. Anomalies (i.e. latent discrepancies in outputs and outputs not adhering to the expected protocol) are flagged and can be submitted to the blockchain as fraud proofs to be arbitrated (Breidenbach et al., 2021).

5.2.4 Dynamic and Verifiable Policy Enforcement: All access decisions are made according to the logic written in smart contract. It offers a very simple reference to an auditable, transparent and deterministic enforcement mechanism that cannot be changed (arbitrarily) by a single party, according to which the zero-trust "never trust, always verify" constraint is automatically enforced for every activity (Rose et al., 2020).

5.3. Case Studies Demonstrating the Integration

While full-scale integration is still an emerging field, several projects and research initiatives demonstrate its principles:

Chainlink DECO: DECO is a privacy-preserving oracle protocol, whose base on MPC (here, more precisely, zero-knowledge proofs), enables users to prove facts about their web-based data (e.g., bank account balance) without disclosing the data purchased. The DECO node network can be combined with a blockchain and to control the identities of the nodes and slashing criteria, in order to enforce a zero trust mechanism, in which the oracles need to continually demonstrate they are running the protocol properly (Breidenbach et al., 2021).

Keep Network / Threshold Network: This network offers a decentralized cryptocurrency custody protocol by MPC. The node of staking and slashing currently implemented in the neurons network by using Ethereum smart contracts, to secure MPC nodes (also named, "operators"). For reluctance to act vengefully on their operators' misdeeds, operators should stake KEEP tokens, which are burnt in case of misdeeds - introducing an economic incentive for being truthful and truly enforcing a zero-trust principle on the behaviour of nodes.

5.4. Benefits of this Integrated Approach

Zero Trust Architecture (ZTA) and MPC The fusion of Zero Trust Architecture (ZTA), blockchain, and MPC is a form of security that provides great value to DeFi, as the concept fundamentally transforms our idea of trust and resilience in open financial systems. Improved security and resilience through removal of implicit trust and dividing application policy enforcement between decentralized infrastructures, reducing reliance on central authorities and economy of scale, and making the system immune to single points of failure, insider and node-specific attacks. At the same time, trust and transparency can be verified as all security policies, enforcement mechanisms and penalties are programed in smart contracts on the blockchain, so the participants can audit autonomously the system's guarantees as well as behaviour of the node operators, hence moving from blind trust to crypto-verifiable and verifiable trust. Moreover, with integrations, the compliance and governance can also run automatically with regulatory requirements like KYC and AML integrated right into policy contracts; for example, a node could be required to present verifiable credentials issued by the regulator to trigger compliance workflows that maximize user privacy while also meeting legal requirements. Finally, this model can ensure scalable security for open networks with the potential to provide a framework for large-scale participation by allowing anyone to become the operator of a node, while still providing robust security guarantees through cryptographic proofs and incentive mechanisms consumers of the network instead of having closed, permissioned, trust lists. Together this triad consisting of ZTA, blockchain, and MPC offers a blueprint for securing next-generation DeFi ecosystems in a way that is transparent, scalable, compliant and inherently resilient.

6: Future Directions

Future research attempts should concentrate for the increased performance and applicability of the integrated model. One of the main avenues is alleviating the performance bottleneck of the blockchain by vitalizing the implementation of the policy contracts, on Layer-2 scaling solutions (talking about Optimistic; or Zero-Knowledge (ZK) Rollups) for achieving high throughput, low latency required for mainstream DeFi adoption. Concurrently, the node attestation's security can be substantially elevated by using powerful Hardware-based trusted execution environments (TEEs) such as Intel SGX, and cryptographically verifiable computation integrity. Furthermore, the use of advanced cryptographic methods is also important; this consists of introducing Fully Homomorphic Encryption (FHE) for end-to-end encrypted computations and using more efficient non-interactive zero-knowledge proofs (zk-SNARKs) for small and efficient fraud proofs as well as for improved privacy solutions, mitigating the overhead for on-chain verification. Beyond DeFi, there are dramatic wider applications for the architecture's big principles of verifiable, decentralized trust. It can be used for healthcare data pipelines which are sensitive, but that should not share patient data between collaborators; transparent and tamper-proof supply chain management with multi-stakeholder logistics optimizations; and novel digital identity/privacy-preserving voting systems. Ultimately, it seems that the confluence of ZTA, Blockchain, and advanced cryptography offers a flexible construct for developing the new generation of resilient, privacy-preserving, and decentralized applications for the digital economy.

Conclusion

Deploying Zero-Trust Architecture in Decentralized Finance and integrating it with blockchain technology is a transformative proposal towards safeguarding Multi-Party Computation. By providing self-determined and tamper-proof policy and ongoing identity validation and behavioral analysis, this model will adequately bridge gaps in permissionless environments that expose critical vulnerabilities. It replaces explicit trust with cryptographic recognitions and economic incentives for accountability, transparency, and resilience to attacks. There are still issues pertaining around scalability and implementation, but it is technologies such as layer-2 solutions or trusted execution environments that are expected to increase the performance and adoption into the future. This synergy not only makes DeFi as secure as possible, but it will also serve as a blueprint for privacy-preserving and compliant and decentralized systems across a number of sectors like healthcare, governance, and digital identity. Future work on integration of these work streams will be instrumental to bringing global, at scale and secure financial ecosystems.

Reference

1. Chen, Y., & Bellavitis, C. (2020). Blockchain disruption and decentralized finance: The rise of decentralized business models. Journal of Business Venturing Insights, 13, e00151. https://doi.org/10.1016/j.jbvi.2019.e00151
2. Qin, K., Zhou, L., Afonin, Y., Lazzaretti, L., & Gervais, A. (2021). CeFi vs. DeFi--Comparing central to decentralized finance. arXiv preprint arXiv:2106.08157. https://arxiv.org/abs/2106.08157
3. Rose, S., Borchert, O., Mitchell, S., & Connelly, S. (2020). Zero trust architecture (NIST Special Publication 800-207). National Institute of Standards and Technology. https://doi.org/10.6028/NIST.SP.800-207
4. Baum, C., Chiang, J. H., David, B., Frederiksen, T. K., & Gentile, L. (2023). SOK: Mitigation of Front-Running in Decentralized Finance. In Lecture notes in computer science (pp. 250–271). https://doi.org/10.1007/978-3-031-32415-4_17
5. Matt Luongo, Corbin Pon (2019) The Keep Network: A Privacy Layer for Public Blockchains
6. Baum, C., David, B., & Dowsley, R. (2020). Insured MPC: Efficient secure computation with financial penalties. Financial Cryptography and Data Security.

7. Breidenbach, L., Cachin, C., Coventry, A., Ellis, S., Juels, A., Maghakian, J., ... & Zhang, F. (2021). Chainlink 2.0: Next steps in the evolution of decentralized oracle networks. Chainlink Labs. https://research.chain.link/whitepaper-v2.pdf
8. Cramer, R., Damgård, I., & Nielsen, J. B. (2020). Secure multiparty computation. Cambridge University Press.
9. Evans, D., Kolesnikov, V., & Rosulek, M. (2018). A pragmatic introduction to secure multi-party computation. Foundations and Trends® in Privacy and Security, 2(2-3), 70-246. https://doi.org/10.1561/3300000019
10. Antonopoulos, A. M., & Wood, G. (2023). Mastering Ethereum: Building smart contracts and dApps. O'Reilly Media.
11. Chen, Y., & Bellavitis, C. (2020). Blockchain disruption and decentralized finance: The rise of decentralized business models. Journal of Business Venturing Insights, 13, e00151. https://doi.org/10.1016/j.jbvi.2019.e00151
12. Gudgeon, L., Werner, S., Perez, D., & Knottenbelt, W. J. (2020). DeFi protocols for loanable funds: Interest rates, liquidity and market efficiency. Proceedings of the 2nd ACM Conference on Advances in Financial Technologies (pp. 92-112). https://doi.org/10.1145/3419614.3423254
13. Kappos, G., Yousaf, H., Piotrowska, A., Kanjalkar, S., Delgado-Segura, S., & Meiklejohn, S. (2022). An empirical analysis of anonymity in Zcash. USENIX Security Symposium, 4631-4648.
14. Qin, K., Zhou, L., & Gervais, A. (2021). Quantifying blockchain extractable value: How dark is the forest? 2022 IEEE Symposium on Security and Privacy (SP).
15. Schär, F. (2021). Decentralized finance: On blockchain- and smart contract-based financial markets. FRB of St. Louis Review.
16. Tapscott, D., & Tapscott, A. (2020). Blockchain revolution: How the technology behind bitcoin and cryptocurrency is changing the world. Penguin.
17. Werner, S. M., Perez, D., Gudgeon, L., Klages-Mundt, A., Harz, D., & Knottenbelt, W. J. (2021). SoK: Decentralized finance (DeFi). arXiv preprint arXiv:2101.08778. https://arxiv.org/abs/2101.08778
18. Zetsche, D. A., Arner, D. W., & Buckley, R. P. (2020). Decentralized finance (DeFi). Journal of Financial Regulation, 6(2), 172-203. https://doi.org/10.1093/jfr/fjaa010
19. Zhou, L., Xiong, X., Ernstberger, J., Chaliasos, S., Wang, Z., Wang, Y., Qin, K., Wattenhofer, R., Song, D., & Gervais, A. (2023). SoK: Decentralized finance (DeFi) attacks. 2023 IEEE Symposium on Security and Privacy (SP).
20. Zheng, Z., Xie, S., Dai, H., Chen, W., Chen, X., Weng, J., & Imran, M. (2023). An overview on smart contracts: Challenges, advances and platforms. Future Generation Computer Systems, 105, 475-491. https://doi.org/10.1016/j.future.2019.12.019
21. Kindervag, J. (2010). Build security into your network's DNA: The zero trust network architecture. Forrester Research Inc.
22. Rose, S., Borchert, O., Mitchell, S., & Connelly, S. (2020). Zero trust architecture (NIST Special Publication 800-207). National Institute of Standards and Technology. https://doi.org/10.6028/NIST.SP.800-207
23. Alamsyah, A., Kusuma, G. N. W., & Ramadhani, D. P. (2024). A Review on Decentralized Finance Ecosystems. Future Internet, 16(3), 76. https://doi.org/10.3390/fi16030076
24. Emin Muhammadi (February 4, 2024) Secure multi-party computation (Example in Golang) https://eminmuhammadi.com/articles/secure-multi-party-computation-example-in-golang
25. X-PHY Editorial (June 6, 2022) Zero Trust Architecture https://x-phy.com/zero-trust-architecture/
26. Mohd Javaid, Abid Haleem, Ravi Pratap Singh, Rajiv Suman, Shahbaz Khan, A review of Blockchain Technology applications for financial services, BenchCouncil Transactions on Benchmarks,

Standards and Evaluations, Volume 2, Issue 3, 2022, 100073, ISSN 2772-4859, https://doi.org/10.1016/j.tbench.2022.100073.

27. Ulf Mattsson, MSE (17 March 2021) Privacy-Preserving Analytics and Secure Multiparty Computation