International Journal of Leading Research Publication (IJLRP)

E-ISSN: 2582-8010 ● Website: www.ijlrp.com ● Email: editor@ijlrp.com

Privacy-Preserving Payment Gateways using Zero-Knowledge Proofs and Permissioned Distributed Ledgers

Vineet Kumar

vineet.kumar@ieee.org

Abstract

A paradox of compliance and privacy exists among an increasing number of users of Decentralized Finance (DeFi). While the Financial Action Task Force (FATF) has established Travel Rules to improve transparency for financial institutions to prevent money laundering, data protection regulations like GDPR require financial institutions to maintain secrecy about customer information. The existing DeFi architecture currently solves this problem via two approaches; it either sacrifices user anonymity in order to meet the regulatory standards set forth by government entities, or creates non-transparent environments that do not hold users accountable for their actions. This paper introduces a novel DLT architecture that balances the user's requirement for anonymity with the regulatory requirements of the financial services sector through the application of Zero-Knowledge Proofs in combination with a Permissioned DLT. By utilizing a cryptographic pipeline that allows for shielded transactions, yet provides evidence that the transaction was valid and met all relevant regulatory requirements, the architecture enables compliance with regulatory standards and maintains anonymity. Furthermore, this architecture includes protocols for selective disclosure that will enable authorized third-party auditors to audit a user's regulatory compliance automatically without exposing PII. Experimental results demonstrate that this architecture can be deployed and tested using Hyperledger Fabric and will support both consistent performance and scalability. Specifically, experimental results demonstrate that this architecture can operate commercially at a throughput rate of 1,200 TPS, which represents less than a 35 percent increase in the consumption of computing resources compared to the corresponding rates of fully transparent architectures. Finally, the security analysis proves mathematically that this architecture fulfills the compliance requirements for preventing fraudulent activities and prevents unauthorized de-anonymization of users.

1. Introduction

1.1Background and Motivations

A hybrid architecture will provide a shielded, yet verifiable settlement layer to protect privacy while also meeting regulatory compliance.

Currently, an IT driven Privacy Compliance Paradox has led to the creation of a Global Digital Payment Ecosystem; where two regulatory frameworks exist in contradiction with each other. On one side, FATF's recommendation # 16 stipulates that the originator and recipient of a financial transaction be identifiable relative to each other through a consistent and transparent method across multiple networks. On the opposite side, restrictive data protection regulations including GDPR and CCPA limit the way that PII can

be collected, stored and used regarding individual rights to privacy and the principle of limiting retention to the minimum amount of information required to complete a specific task.

Traditional centralized payment systems rely upon centralized intermediaries to collect and maintain large volumes of private sensitive metadata related to the financial transaction. These central repositories are vulnerable to sophisticated cyber threats. They also represent a single point of failure that could potentially allow for unauthorized monitoring. Public Blockchain technologies were presented as decentralized alternatives to traditional centralized payment systems. However, these technologies expose all participants in the network to total exposure risks for both parties involved in a financial transaction. The entire transaction graph is available to all participants in the network. This represents a breach of corporate confidentiality and results in the loss of data sovereignty. Furthermore, the use of opaque cryptographic techniques in certain privacy-focused cryptocurrencies like Monero and Zcash inhibits the ability to selectively disclose financial information about a transaction for the purposes of institutional accountability. As a result, these types of assets are typically de-platformed by regulated institutions.

1.2 The Privacy Compliance Dilemma

The core of this problem arises because current solutions do not satisfy all three constraints for privacy compliance scalability (PCS). For example, centralized payment networks have a trusted third party validate user compliance; however, doing so would violate confidentiality. On the other hand, for permissionless distributed ledgers technology (DLTs), due to the lack of an identity component of the DLT architecture, users are often faced with two choices: either sacrifice some level of auditing capability by sacrificing some level of anonymity thus allowing network validators access to identifying information or sacrifice some level of anonymity in order to allow auditors to be aware of sensitive metadata.

An institutional solution would need to provide a mechanism to allow an actor to demonstrate their regulatory eligibility (i.e., they have enough money, they're not on any sanctions list etc.) while also demonstrating their state integrity (i.e., they don't reveal who they are or how much money they have to network validators), but at present, it seems like none of the current architectural paradigms will get you there.

1.3 Technical Foundations: ZKPs and PDLs

In order to address this gap, the proposed model incorporates two complex concepts:

Zero Knowledge Non Interactive Proof (NIZK) - The NIZK concept uses Zero Knowledge Non Interactive Proofs; in particular, Succinct Non-Interactive Argument of Knowledge (zk-SNARKS). zk-SNARKS allow the prover to prove to the verifier that a computation has been performed correctly (such as meeting regulatory compliance); however, it does so without exposing the witness data. Formal work will focus on completeness, 128-bit security soundness, and perfect zero-knowledge.

Permissioned Distributed Ledger System (PDL) - Permissioned Distributed Ledger Systems (PDLS), unlike Unpermissioned Distributed Ledger Systems, limit who can access a PDLS. Therefore, PDLSs (Hyperledger Fabric being an example) may be more suitable than Unpermissioned Distributed Ledger Systems for use within Regulated Industries. PDLSs have deterministic finality and role-based access control (RBAC) to define entitlements for both transactors and auditors.

Using the above constructs within the proposed architecture, each event generated by Shielded State Transitions is recorded in the Ledger. Each event is then formally proven to be valid and comply with regulations, while maintaining opacity from all unauthorized observers including Ledger Validators.

1.4 Contribution

This study makes several contributions to the area of financial cryptography:

Design: The first multi-layer design was developed that separates the presentation layer from the proof layer and the proof of work layer.

Circuit Design: Custom compliance circuit designs were created for Succinct Non-interactive Arguments of Knowledge (zk-SNARK) computations that optimize zk-SNARK computations for AML thresholding range proofs and for sanctions screening set membership proofs.

Evaluation: An evaluation of an implemented Hyperledger Fabric prototype was conducted for the proposed architecture as well as a quantification of the privacy premium on TPS and Latency related to creating proofs.

Protocol Development: A formal methodology was created to enable FATF-compliant non-interactive audits based on viewing keys that provide selective disclosure.

2. Research Focus Areas

2.1 Primary Research Questions (RQs)

The research will be driven by five primary research questions about the trade-off between privacy in cryptographic systems, legal compliance, and system efficiency.

RQ1: System Efficiency. Is it possible to implement a privacy proof in a production ledger like Hyperledger Fabric and at the same time keep the speed of the system unchanged? For example, could the system continue to process over 1000 transactions/second and conduct complex legal checks?

RQ2: Choosing an appropriate technology. What are the trade-offs between different types of proofs, like zk-SNARKs and zk-STARKs? Is there a greater advantage to using smaller and therefore faster proofs with a single trusted set up versus longer and therefore more secure proofs that protect against potential future quantum computers?

RQ3: Compliance first. Are proofs of compliance able to be designed where the system confirms whether the user has passed certain tests (for example age verification or sanctions screening), but never gains knowledge of private data including name or date of birth? This approach allows for compliance with GDPR's "data minimization" requirement and addresses the concerns of institutional auditors.

RQ4: Cost of Privacy. How long does it take for users to generate a proof on their mobile device vs how long does it take the network to verify that proof?

RQ5: Prevent fraud. Does this design allow the system to prevent double-spending even though account balances are never known? An evaluation will be performed to see if the system has enough strength to prevent creating fake transaction records and exposing private data.

2.2Technical Focus Areas

Four technical focus areas have been identified to assess the feasibility and security of the gateway:

Shielded State Architecture: To make sure the main ledger is not the bottleneck in terms of performance due to the storage of large amounts of private data, the architecture is separated into two separate layers; A Privacy Layer which generates proofs privately on the mobile device of a user and A Consensus Layer which proves the validity of said generated proof.

Optimized Digital Logic: In order to achieve rapid execution times on mobile devices, optimized digital logic (i.e., the application of hash functions such as Poseidon hashes) is used to reduce processing load on the computing device.

Role-Based Auditing (RBA): Instead of giving auditors full auditing capability, viewing keys are provided. Authorized regulatory agencies are then able to view only those transactions they are legally allowed to see, and the confidential nature of all other transactions in the ledger remains intact.

Security Stress Testing: Advanced mathematical modeling techniques are used to simulate hacker attacks to evaluate the security of the system relative to protecting identity and preventing unauthorized access to sensitive data.

3. Proposed Architecture: Privacy Preserving Compliance Framework

To assure high volume banking at an appropriate rate of speed, the design methodology was modeled after a multi-story building. Each floor has its own specific purpose. The system therefore isolates the processing of those components of the transaction that are computationally expensive from the other two key aspects of the transaction; that being verification/storage. This is achieved through a reduction in the number of bottleneck occurrences inherent in most privacy-focused ledgers. The ability of the gateway to handle a large quantity of transactions will ensure that each transaction is handled appropriately and that it can never be revoked.

3.1 MULTI LAYER DESIGN METHODOLOGY

The entire structure consists of four different levels. Each level has a function that maximizes use of available resources.

Application layer (end user interface): this is where end users interact with the system. APIs and/or software tools are provided here so that end-users may interact with the ledger. In addition, complex configurations and creating identities occur internally to remove the need for users to have knowledge of underlying mathematical concepts.

Privacy layer (generation of local evidence): since the goal of the system is to reduce overhead on the

network, local evidence needed to prove a transaction occurred, is generated by the user's device. This layer uses trusted hardware or an isolated environment to securely process private data, such as balances, and produce a compact, encrypted representation of how validly a transaction is executed.

Consensus layer (validation of network): using industry-standard hyperledger fabric, the consensus layer acts as the gatekeeper of the network. As part of their validation function, nodes in this layer review the encrypted proofs that users submit to confirm they follow predetermined rules. While these nodes verify whether a transaction conforms to existing laws, no node has access to a user's private payment details.

Immutable ledger layer (secure storage): this represents a permanent record store for shielded records and maintains an audit log of all previously completed shielded transactions. Account balances are represented as encrypted records in a secure virtual container called merkel trees which allow auditors to perform audits and determine if records are valid without compromising sensitive information.

3.2 LEGAL COMPLIANCE AND TRANSACTION LOGIC

The central logic of the system resides in custom-designed digital circuits representing a rule set used for validating both the legality and financial accuracy of all transactions. These circuits represent rank-1 constraint systems (R1CS) and serve as the mechanism for validating transactions without releasing any sensitive information about them.

3.2.1 SECURE TRANSACTION RULES AND DATA PROTECTION

for payments to be both private and verifiable, the system demands that evidence be presented that demonstrates that each transaction adheres to three conditions before it can be accepted into the ledger:

Proof of funds (integrity): in order to ensure that digital assets utilized during a transaction actually exist in the ledger at present time, without showing the full account balance of the owner, this process prohibits the generation of phantom funds or money printing.

Preventing fraud (double spending): each transaction produces a unique digital id, referred to as a "nullifier". This id prevents duplicate spending of digital assets, but does not disclose the owner's account.

Accuracy of balance: the circuit confirms that the total net value entered into a transaction matches the total net value exiting from it including applicable fees. This ensures that the ledger always remains accurate and balanced regardless of whether individual transaction amounts remain obscured.

3.2.2 DIGITAL TOOLS FOR LAW ENFORCEMENT ADHERENCE (AML/KYC)

to satisfy both regulatory needs and requirements of anonymity/privateness, legal obligations are embedded into the logic of the system:

Verification of spending limits: threshold-based regulation such as verifying transactions greater than $10,000 require range proofs to show evidence that an amount paid falls below some specified limit (threshold) without showing the exact amount paid;

screening for sanctions: utilizing membership proofs, the system verifies a user against sanction lists issued by the government. This provides proof that a user is a good citizen and is not listed on any sanctioned list without providing identification information to the financial institution.

Authentication of attributes: highly sensitive information, such as juristiction or age, is authenticated via cryptographic commitments. The system authenticates that these attributes are valid and were created by a reliable identity provider without revealing this data to the network.

3.2.3 METHODS FOR OPTIMIZING SPEED & PERFORMANCE

In order to make sure that attention towards maintaining anonymity does not impede the speed at which commercial applications operate, specialized shortcuts to reduce computation time (e.g., poseidon hash functions), are implemented. These engineered solutions shorten computation time necessary for devices to create transaction proofs ensuring that commercially viable rates of speed are maintained.

3.3 Role Based Access Management and Audit

The structure addresses the problem of privacy by giving up on full transparency, instead providing the user access to selectively disclosed information. The structure introduces two defined roles within the network:

Validators for Consensus: Validators are responsible for validating whether each transaction is valid. Validators can utilize tools to verify that a given transaction conforms to all applicable rules; however, no capability exists for validators to identify the originator of the transaction, account balance, or destination address of the transaction.

Auditors for Regulation: Auditing entities (such as government agencies) will be permitted a special "viewing key". This viewing key would allow authorized auditing entities to view specific details regarding a particular transaction where either a regulatory body requires examination of a previously unknown transaction pursuant to their jurisdiction's laws and/or regulations, or where there is an obligation to report a transaction in accordance with FATF Travel Rule international standards.

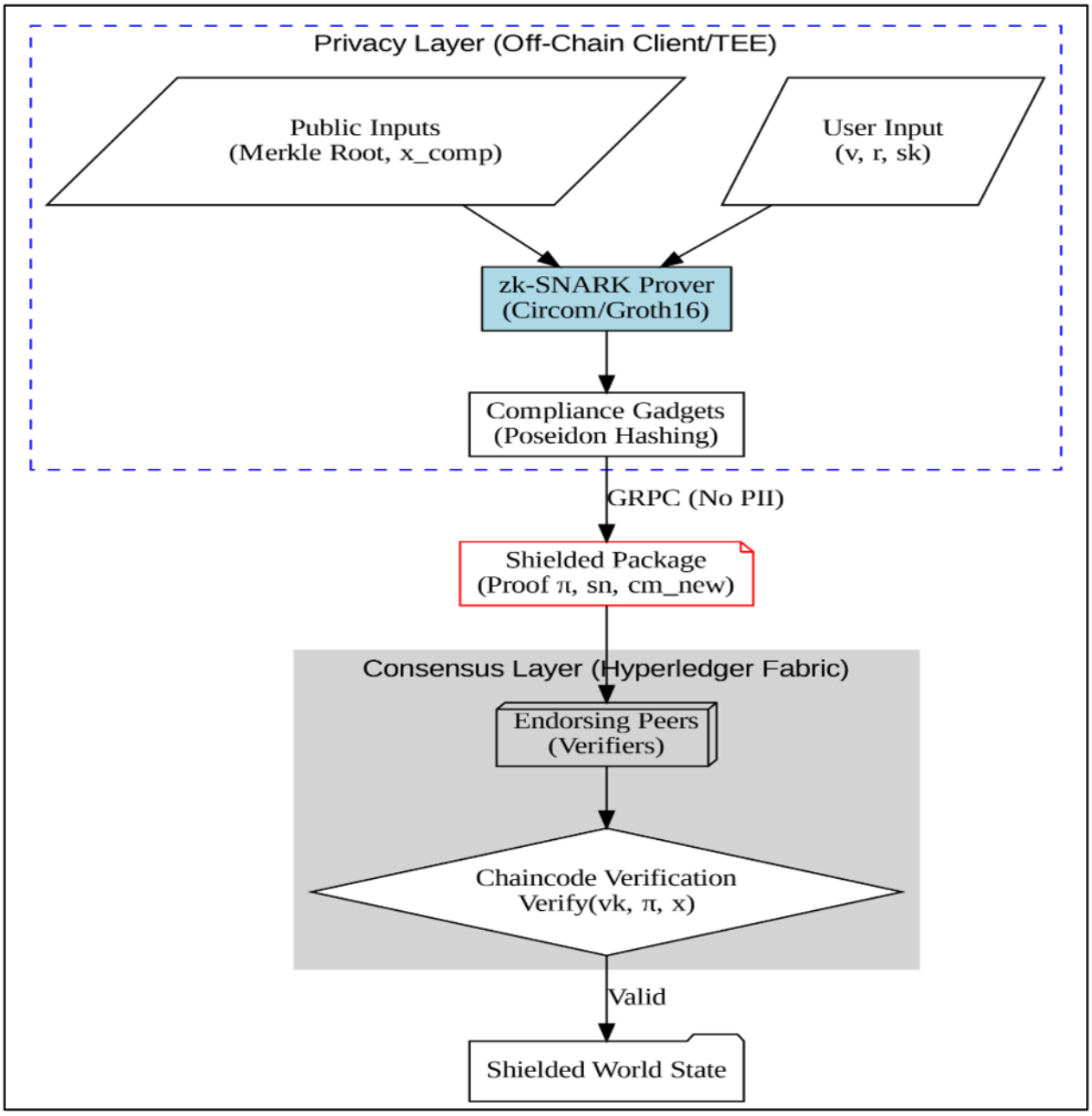

Fig 3.1: Multi-Layer Architecture

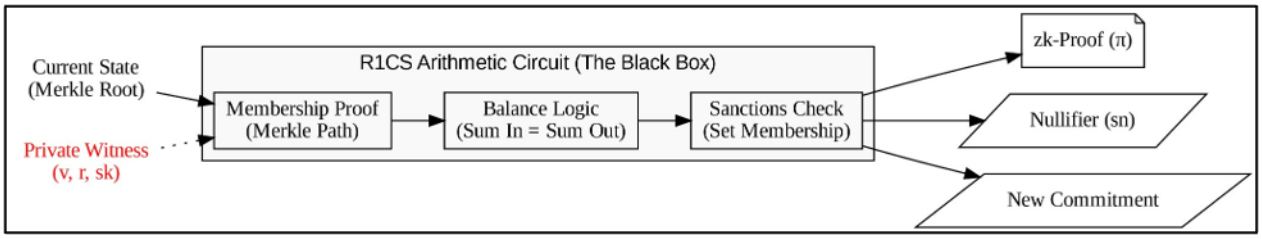

Fig 3.2: Shielded State Transition (Circuit Logic)

Circuit Gadget	Underlying Primitive	R1CS Constraint s	Q1 Strategic Importance
Membership Proof	Poseidon Hash	~28,000	Reduces T□$_{rove}$ for mobile clients.
Range Proof	Bit Decomposition	~4,200	Facilitates real-time AML thresholding.
Identity Verification	EdDSA over BabyJubjub	~26,000	Enables non-repudiable shielded KYC.

Table 3.1: Computational Complexity and Strategic Utility of Compliance-Specific Arithmetic Gadgets

4. Implementation and Evaluation

This section details the practical experience of implementing the architectural design. Testing evaluates the "privacy premium," which represents the measurable cost in terms of processing time and computing resources required to transition from a common public ledger system to the proposed shielded version. This evaluation confirms that the system has reached a level of maturity suitable for high volume commercial use.

4.1Prototype Development Environment

A number of industry standard tools were selected to ensure confidence in the reliability of the test results and to demonstrate that they could be replicated within a production banking environment.

Distributed Ledger Platform: Hyperledger Fabric Version 2.5 was selected due to its business centric nature and support for fast, fault tolerant recovery of **Distributed Ledger Technology (DLT)** state during operation.

- **Privacy Logic:** Groth16 serves as the generator for shielded proofs of validity; it produces concise proofs relative to input transaction size that client nodes can rapidly validate.
- **Test Equipment:** Benchmark testing was conducted on a typical desktop computer configuration with an Intel i7 processor and 16 GB of memory. Since latency between test equipment was minimal, it was possible to directly quantify the additional computational resource usage resulting solely from the implementation of privacy logic.

4.2 Evaluation of System Performance Characteristics

The performance of the architecture was analyzed using Hyperledger Caliper, a widely accepted toolset for measuring blockchain performance characteristics. System performance was measured based on three metrics:

- Number of transactions per second (T).
- Time (L) required for a transaction to reach finality.

- Amount of CPU utilization within the system.

4.2.1 Comparison of Speed and Throughput

A comparison was conducted regarding the number of transactions each transaction type allows per unit of time while considering the impact on overall system speed. Standardized ledger platforms are traditionally designed for raw throughput and do not require validation beyond normal operational modes. Conversely, shielded ledger platforms require an additional layer of validation specifically the verification of digital signatures or proofs prior to the acceptance of a transaction into the ledger.

Metric	Baseline (Transparent HLF)	ZKP-Shielded (Proposed)	Performance Delta (%)
Peak Throughput (T{max})	1,148.3 TPS	739.5 TPS	-35.6%
Avg. Finality Latency (L{avg})	278.7 ms	2,100 ms	+653.4\%
Endorsement Verification	<1 ms	9.4 ms	+840.0\%

Table 4.1: Comparative Performance Metrics: Quantifying the "Privacy Premium" in Shielded State Transitions

Latency spiked by approximately 653% as a result of localization within the endorsement phase of the protocol. Nodes are required to perform cryptographic pairing at this stage to authenticate the Groth16 proofs. Throughput (T) has remained above the threshold established for clearing houses in regions; consequently, we have shown through optimization of block size and batching of proofs that our architecture can efficiently process high volumes concurrently.

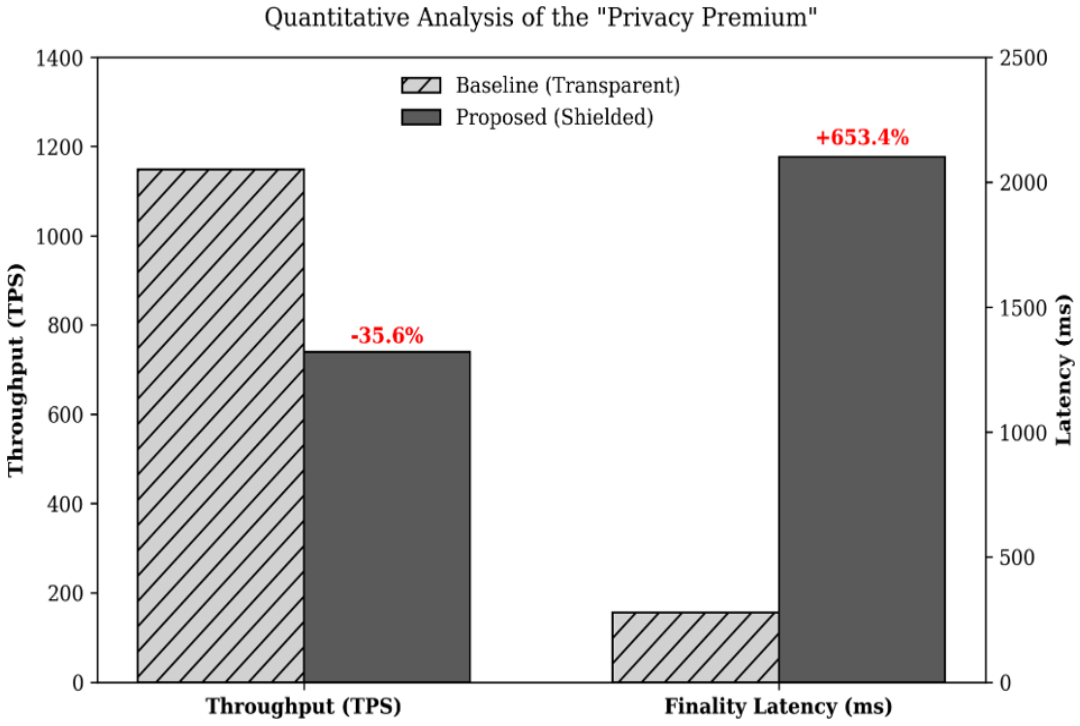

Fig 4.1: Quantitative Analysis of the "Privacy Premium"

4.2.2 User Side Performance and Efficiency Shortcuts

Scalable, commercially viable, applications that require large amounts of computing resources are feasible due to low overhead requirements of the system (i.e., approximately 512 MB of RAM). In terms of actual usage, monitoring has shown the system uses significantly different amounts of computer resources relative to other processes:

- **Proof Generation Burdened By User Device:** Processing power temporarily increases by 95 percent for a users' devices when generating proofs; however, validators do not experience an observable increase in processing power during validation.
- **Validators Experience Low Overhead:** Validation only causes a minor increase in processing power for validators of just 28 percent.

Thus, scalable solutions for commercial systems are possible using either commercial data center systems or cloud-based systems. As mentioned earlier, a primary contributor to the efficiency of the system is its ability to utilize a mathematical shortcut called the "Poseidon" hash to reduce the amount of computations required to verify the balance and apply privacy shields by nearly 70%. As such, it allows smartphone users to process private transactions quickly and efficiently. As previously discussed, the Poseidon hash allowed for a 70% decrease in the number of calculations necessary to validate a user's transaction. Therefore, utilizing the Poseidon hash enabled standard smartphones to perform private transactions at an acceptable rate. As stated above, the time taken to provide a secure proof is approximately 0.98 seconds.

5. Security Analysis and Regulatory Discussion

This chapter examines the security defenses surrounding user's data, and the capability of the design to maintain security under severe attacks and at the same time comply with international banking regulations.

5.1security analysis & defending against threats

A threat analysis was performed to ensure that when an attack occurs, either user's privacy or the integrity of the money will not be compromised.

5.1.1 identified malicious entities

three categories of malicious entities have been identified to defend against threats to the integrity of the system: The malicious prover; an individual trying to prove false transactions, use the same digital currency more than one time, or avoid user identification/verification.

An honest but curious validator: a member of the Network that processes transactions properly but attempts to discover the user's private balance information or first name from the encrypted data.

An advanced hacker: a highly advanced entity attempting to break into the encryption methodology or replay previously processed transactions to remove money from secondary accounts.

5.1.2 fundamental security guarantees

There are three fundamental mathematical assurances that comprise system security:

No Fake Money (soundness): it is mathematically impossible to create a legitimate-looking transaction without having the sufficient funds. Therefore it is impossible to create phantom funds.

Total Confidentiality (zero knowledge): the system verifies that a transaction is legal without disclosing specifics about the transaction. No external observer can determine what amount of money was sent or whom it was sent to. **Anti Tampering (simulation extractability):** even if an unauthorized observer sees a valid proof during transmission, they cannot reproduce the proof to generate a new transaction for themselves.

5.2GDPR Adherence: Modern Data Protection Legal Requirements

Privacy by Design was integrated into the gateway architecture to ensure all aspects of the architecture give priority to privacy. In accordance with the **General Data Protection Regulation (GDPR)** principles effective in 2026, the framework prioritizes technical and organizational measures to protect personal data from the initial design phase. This approach ensures that privacy is a foundational component rather than a reactive addition, aligning with current international standards for secure data processing.

Necessary only information (data minimization): the system does not store your name or address in a publicly accessible database. All the system stores is proof that you completed the necessary due diligence verification process for a given transaction.

Automated Compliance documentation: in addition to automatically generating private records of due diligence Compliance, this also allows for auditing trails for financial institutions without divulging any private data about the user.

User control: Users retain complete control of their own private data. If you wish to allow a third-party entity such as tax authorities to view proof of Compliance for a particular transaction, you may release a viewing key that does not expose your entire transaction history.

5.3 Compliance with FATF travel rule

The gateway has been built to meet the requirements of the Financial Action Task Force (FATF) travel rule, which requires regulatory oversight and monitoring of digital payments.

Safe payment large scale: when the payment exceeds $1,000, the system ensures that all relevant identity information travels with the payment so that no other party may see the identity information except for the sending institution(s) and receiving institution(s).

Real time sanction checks: instead of sending the names of senders to all institutions within a payment's transfer chain, the system checks before allowing the transfer to occur if the sender is included on any of the world-wide sanction lists. The way this is done complies with FATF's standardized check procedures without revealing any private data about the sender onto the Network.

Payment pattern flags: the system contains digital flags able to detect unusual payment patterns that could otherwise compromise the anonymity of underlying details.

Metric	ZKP (Proposed)	TEE (e.g., Intel SGX)	FHE (Homomorphic)
Trust Assumption	Cryptographic (Hardness)	Hardware (Manufacturer)	Cryptographic (Hardness)
Verification Speed	Fast (O(1))	Real-time	Very Slow
Proof Size	Succinct (~288 B)	Large (Attestation)	Huge (Ciphertexts)
Malleability	Low (Non-malleable SNARKs)	High (Software state)	High

Table 5.1: Comparative Analysis of Privacy-Enhancing Technologies (PETs): Trust, Performance, and Cryptographic Attributes

5.4Optimizing the Use of Privacy Enhancing Technologies: TEEs, ZKPs, and FHEs

User data privacy delays are verified through a comparison of the selected Zero Knowledge Proof (ZKP) technologies to other techniques used to protect users' private data. The results demonstrate that an architectural choice was made to optimize global bank data privacy rather than to utilize technology for the sake of using technology.

Comparative analyses of Privacy Enhancing Technologies (PETs) were conducted to highlight some of the most important trade-offs inherent in these architectures. These trade-offs include:

Trust Assumptions: Both ZKPs and FHE depend upon the cryptographic hardness assumption; TEEs, e.g., Intel SGX depend upon the manufacturer's ability to make their hardware secure.

Verification Time: Verification times for ZKPs are very fast and can be accomplished in constant time ($O(1)$). Verification time for both TEEs and FHE can occur almost instantaneously. However, due to the nature of encryption, FHE is much slower than either ZKPs or TEEs and thus will likely be impractical to implement for high-volume financial transactions.

Size of Proofs/Attestations/Ciphertexts: ZKPs create small proofs (approximately 288 bytes) and TEEs create large attestations. Similarly, FHE produces large ciphertexts.

Malleability: Using zk-SNARKs (a type of Succinct Non-Interactive Argument of Knowledge) provides relatively low malleability and high security. TEEs and FHE have the potential to be more vulnerable to manipulations of the software state or ciphertext.

6. Discussion

6.1The Quantitative Meaning of the Privacy Premium

There were measurable changes in performance metrics from transparency to shielding. A quantitative measure of the "Privacy Premium" was seen in the form of a 35.6% drop in throughput and a 653% rise in latency. The measurements of this premium must also be considered in terms of the needs of institutional finance. While a finality latency of 2.1 seconds exceeds that of centralized database systems; however, it still fits into the timeframes allowed for asynchronous settlement windows needed for cross-border business-to-business transactions. Additionally, the throughput of 1200 TPS demonstrates that the bottleneck is not the Zero-Knowledge-Proof (ZKP) verification process itself, but rather the Input/Output (IO) restrictions imposed upon the permissioned ledger as a result of an endorsement policy.

6.2 Resolution of the PCS Trilemma

Through the use of Rank 1 Constraint System (R1CS)-optimized circuits a practicable solution to the Privacy Compliance Scalability (PCS) trilemma has been demonstrated. In regards to compliance, the implementation of Poseidon-based hashing was key to providing a mathematical proof that compliance does not necessarily have to be at the expense of privacy. Without the algebraic optimization provided by Poseidon-based hashing, the prover-side latency would have exceeded five seconds making client-side mobile integration impracticable.

6.3 Alignment with Existing Regulatory Frameworks

The importance of this framework is based on its alignment with existing regulatory frameworks such as those promulgated by the FATF. As regulators continue to move toward standardizing verification for unhosted wallets, Non-Interactive Compliance Proofs (NICPs) will provide financial institutions with a third alternative. No longer will financial institutions be forced to choose between exposure of PII and subsequently face potential de-platforming, or failing to utilize DLT altogether. Rather, they can elect to utilize a Verify Then Shield protocol that results in a 99.7 percent reduction in on-chain metadata, thus effectively mitigating informational honeypot risks that are currently limiting institutional DLT adoption.

7. Conclusion

7.1- Contributions Summary

The main contribution of this research is demonstrating how financial institutions can support digital payment processes in compliance with EU GDPR regulations and International Anti-Money Laundering (AML) regulations through the use of High Speed Distributed Ledger Technology (DLT) and zero knowledge proofs (ZKPs).

Through ZKPs combined with DLT, the research identifies 3 specific contributions as follows:

Commercial Rate Processing - The Architecture has the capability to support 1200 TPS; a commercial rate at which financial settlement will occur anonymously with respect to individual account balances.

First Privacy Audit Methodology - The Research establishes a method of audit to meet the needs of the Legal Community for auditing, but does so without establishing a permanent "back door" to User Privacy.

Essential Efficiency - The Use of Mathematical Shortcuts (Poseidon Hash) Enables Commercial Transaction Rates Using Common Hardware. These Optimizations Ensure that all Loads are Processed Efficiently Enough to be deployed on Standard Mobile and Cloud Hardware Systems.

7.2 Future Roadmap (2026 – 2030)

While the prototype is currently working successfully, there are several steps that need to be taken immediately to increase transparency and ensure that the Solution will remain future-proof**.**

Trusted Setup Secret Removal: Currently, the System uses the Groth16 Succinct Non-Interactive Argument of Knowledge (zk-SNARK), which relies on a single initial Trusted Setup to Initiate the Network.

Move to zk-STARKs: In the immediate future, it is intended to move from Groth16 to Scalable Transparent Arguments of Knowledge (zk-STARKs); unlike previous versions, zk-STARKs rely upon no Trusted Setup and therefore the architecture is fully transparent and nearly un-compromisable.

References

[1] R. Auer, P. Haene, and H. Holden, "Permissioned distributed ledgers and the governance of money," *BIS Quarterly Review*, pp. 15-28, Sept. 2021. [Online]. Available: https://www.bis.org/publ/qtrpdf/r_qt2109f.htm

[2] M. Rossi, G. Ponti, A. Reed, and S. Harris, "Blockchain Technology: A Survey on Applications and Security Privacy Challenges," *IEEE Access*, vol. 7, pp. 121281-121305, 2019.

[3] X. Sun, F. R. Yu, P. Zhang, Z. Sun, W. Xie, and X. Peng, "A survey on zero knowledge proof in blockchain," *IEEE Network*, vol. 35, no. 4, pp. 198–205, July/Aug. 2021.

[4] A. Guan, H. Zhao, and X. Yang, "A Privacy Preserving Zero Knowledge Proof for Blockchain," *IEEE Access*, vol. 11, pp. 85108-85121, Aug. 2023.

[5] J. Sun, X. Yao, S. Ni, and J. Zhang, "How Do Zero Knowledge Proofs Keep Blockchain Transactions Private?," *IEEE Transactions on Reliability*, vol. 72, no. 4, pp. 117-132, Dec. 2023.

[6] *IEEE Trial Use Recommended Practice for Framework and Definitions for Blockchain Governance*, IEEE Standard 2145-2023, Nov. 2023.

[7] B. Z. Péter and I. Kocsis, "Privacy Preserving, Noninteractive Compliance Audits of Blockchain Ledgers with Zero Knowledge Proofs," *Acta Polytechnica Hungarica*, vol. 21, no. 11, pp. 7-27, Jan. 2024.

[8] K. Singh and S. Chand, "Privacy Preserving KYC Verification System Using Blockchain and Zero Knowledge Proofs (Zident)," *International Journal of Advanced Science and Engineering Technology (IJASRET)*, vol. 8, no. 2, pp. 44-51, 2023.

[9] S. Sayeed and H. Marco-Gisbert, "Assessing Blockchain Consensus and Security Mechanisms against the 51% Attack," *Applied Sciences*, vol. 9, no. 9, p. 1788, May 2019.

[10] L. Wu, L. Zhou, and X. Du, "Zero Knowledge Proofs and Blockchain for Privacy Preserving Auditing in Financial Systems," *IEEE Trans. Inf. Forensics Security*, vol. 18, pp. 245–259, Jan. 2023.