A Privacy-Preserving Enforced Bill Collection System Using Smart Contracts

Prof. Umar Mulani, Diksha Shinde, Kadam Ankita, Sameera Gaikwad, Sanket Abnave
Department of Computer Engineering,
K J College of Engineering and Management Research, Pune(India)

Abstract - The paper presents a privacy-preserving enforced bill collection system that ensures both user anonymity and accountability using smart contracts and accountable ring signatures. The system extends the existing Isshiki system, which allows users to anonymously access services, by introducing an enforcement mechanism that guarantees payment via pre-deposited funds. If a user ignores the invoice, the smart contract automatically transfers the deposit to the bill collector, ensuring fair compensation. The proposed system is designed for decentralized blockchain environments, specifically using Ethereum smart contracts to enforce payment while maintaining privacy. The solution is efficient, reducing gas costs by leveraging elliptic curve digital signatures (ECDSA).

Keywords *- Privacy-preserving, smart contracts, accountable ring signatures, enforced bill collection, Ethereum, anonymity, traceability.*

1. Introduction

In modern service systems, balancing privacy and accountability is critical, especially in billing processes. The Isshiki system provides a foundation by allowing users to access services anonymously using group signatures while enabling a bill collector to trace users for invoicing. However, the Isshiki system lacks an enforcement mechanism for bill payment, allowing users to avoid payment by ignoring invoices. This paper proposes an extension of the Isshiki system using smart contracts and accountable ring signatures to enforce bill collection automatically, ensuring users cannot bypass payment.

2. Motivation

While privacy-preserving systems are crucial in maintaining user anonymity, it is equally important to ensure that service providers receive due payment. The absence of an enforcement mechanism in existing systems like the Isshiki framework creates a loophole where users can exploit services without paying. The motivation for this paper is to fill this gap by introducing a smart contract-based system that not only protects privacy but also guarantees payment enforcement, ensuring fairness for service providers.

3. Literature Survey

1. In this paper[1],This text discusses the use of Bitcoin's blockchain for smart contracts—automatically enforced agreements without intermediaries. Despite Bitcoin's primary role as a currency, its consensus mechanism supports such contracts. However, inconsistent treatment, informal descriptions, and undocumented features hinder research. The paper presents a formal framework to clarify existing smart contracts and enhance automatic verification, while also identifying key challenges for wider adoption on Bitcoin.

2. In this paper[2],This work introduces the first fully dynamic lattice-based group signature, allowing users to join and leave freely. It improves on previous static schemes by reducing signature size and meeting strong security requirements, including deniability.

3. In this paper[3], This paper tackles the issue of fairness in cryptocurrency transactions, ensuring both parties either exchange items or neither does. It introduces "strong timeliness" for fair exchanges, important for resource-constrained users, and proposes two blockchain-based protocols for fair payment-for-receipt exchanges, comparing their security and efficiency.

4. In this paper[4], This paper presents an anonymous trust-marking scheme for cryptocurrencies, enabling trusted entities to assign tokens to addresses while keeping their identity hidden. It works with Bitcoin, Ethereum, and NEM, offering a solution inspired by the Coincheck incident.

5. In this paper[5], This paper introduces SmartJudge, a mediator smart contract that enables secure two-party interactions without a trusted third party. It reduces costs by consulting verifier contracts only in disputes, achieving cost savings of 46–50% for cross-blockchain trades and 22% for digital goods exchanges compared to current methods.

6. In this paper[6], This paper introduces Onionchain, a protocol suite that provides both privacy and traceability in blockchain systems, inspired by Onion routing. It includes a case study on Vehicular Ad Hoc Networks (VANETs) and offers security analysis and validation of its effectiveness and cost- efficiency.

7. In this paper[7], This paper implements a revocable group signature scheme that reduces the revocation list (RL) size to \(O(R/T)\) by accumulating entries. The authors achieve signing times under 500 ms and verification times under 900 ms for \(T = 100\), demonstrating the scheme's practicality and the effectiveness of the accumulator technique.

8. In this paper[8],This paper presents a linkable spontaneously anonymous group (LSAG) signature scheme featuring anonymity, linkability, and spontaneity without a group secret. The scheme, secure under the random oracle model, supports an efficient one-round e- voting system without registration and introduces a new reduction of the rewind simulation lemma, along with threshold extensions.

9. In this paper[9], This paper addresses membership revocation in group signature schemes, introducing a technique that enables constant-size private keys using the Naor-Naor- Lotspiech (NNL) subset cover framework. This approach reduces storage requirements and makes revocable group signatures competitive with ordinary ones, allowing unrevoked members to avoid key updates after revocations.

10. In this paper[10], This paper introduces the first quantum-resistant lattice-based verifier- local revocation (VLR) group signature scheme. It supports membership revocation, features logarithmic-size signatures, and operates under weaker security assumptions. Proven secure in the random oracle model based on the hardness of the SIVPOe(n1.5) problem, the scheme does not rely on encryption, offering a novel

4. System Architecture

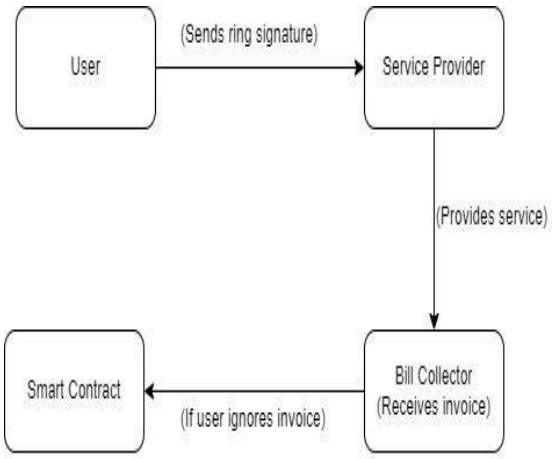

Fig: A Privacy-Preserving Enforced Bill Collection System Using Smart Contracts

System Description

The proposed system in *"A Privacy-Preserving Enforced Bill Collection System using Smart Contracts"* enhances the existing Isshiki identity management and billing framework by introducing a smart contract-based enforcement mechanism. This system ensures that users who consume services are required to pay, addressing the limitation of the Isshiki system where users could avoid payment by ignoring invoices. By integrating accountable ring signatures and Ethereum smart contracts, the system maintains user anonymity while adding a layer of accountability. Users must deposit funds into a smart contract before accessing a service, and if they fail to pay the invoice, the smart contract automatically transfers the deposit to the Bill Collector, enforcing bill collection. The use of elliptic curve digital signatures (ECDSA) reduces the computational costs of running smart contracts, making the system more efficient for real-world blockchain environments. This solution provides both privacy preservation and enforceability, ensuring fairness for service providers while protecting user identity.

Module

User Module:

Users generate **ring signatures** for authentication and send these to the service provider to prove membership without revealing their identity. They also interact with smart contracts to deposit payments.

Service Provider Module:

The service provider verifies the ring signatures provided by users to ensure they are legitimate members of the system. It does not manage personal data and only verifies that a user is valid based on their group signature.

Bill Collector Module:

The bill collector manages user identification and payment collection. It has access to a special opening key to identify users from their group signatures. The bill collector sends invoices to users and, if users fail to pay, triggers the smart contract for enforced collection.

Smart Contract Module:

This module runs on the blockchain and is responsible for handling deposits from users. If a user ignores a payment request, the smart contract automatically transfers the user's deposit to the bill collector. It is designed to reduce gas costs by only running in case of non- payment.

Accountable Ring Signature Module:

This module provides both anonymity and traceability. It allows users to generate their own signing keys and ensures that the bill collector can trace signatures to enforce payment without revealing user identities prematurely.

5. Conclusion

The proposed system successfully extends the Isshiki framework by incorporating smart contracts for enforced bill collection, ensuring users cannot bypass payment. By utilizing accountable ring signatures, the system preserves user anonymity while ensuring traceability and accountability. The integration of Ethereum smart contracts provides an automated, decentralized mechanism for payment enforcement, making the system practical for real-world blockchain environments. This approach ensures both privacy and fairness, solving the key limitation of the Isshiki system by providing guaranteed bill collection.

6. References

1. NicolaAtzei,MassimoBartoletti,Tiziana Cimoli,StefanoLande, and RobertoZunino. SoK:Unravelingbitcoinsmart contracts. InPOST, pages217–242,2018.
2. San Ling, Khoa Nguyen, Huaxiong Wang, and Yanhong Xu. Lattice based group signatures: Achieving full dynamicity (and deniability) with ease. Theor. Comput. Sci., 783:71–94, 2019.
3. Jian Liu, Wenting Li, Ghassan O. Karame, and N. Asokan. Toward fairness of cryptocurrency payments. IEEE Secur. Priv., 16(3):81–89, 2018.
4. Teppei Sato, Keita Emura, Tomoki Fujitani,

and Kazumasa Omote. An anonymous trust-marking scheme on blockchain systems. In IEEE International Conference on Blockchain and Cryptocurrency, ICBC, pages 1–3, 2021.

5. Eric Wagner, Achim V¨olker, Frederik Fuhrmann, Roman Matzutt, and Klaus Wehrle. Dispute resolution for smart contract-based two-party protocols. In IEEE ICBC, pages 422–430, 2019.
6. Yue Zhang, Jian Weng, Jia-Si Weng, Ming Li, and Weiqi Luo. Onion chain: Towards balancing privacy and traceability of blockchain-based applications. CoRR, abs/1909.03367, 2019.
7. Shahidatul Sadiah and Toru Nakanishi. Revocable group signatures with compact revocation list using vector commitments. IEICE Trans. Fundam. Electron. Commun. Comput. Sci., 100- A(8):1672–1682, 2017.
8. Joseph K. Liu, Victor K. Wei, and Duncan S. Wong. Linkable spontaneous anonymous group signature for ad hoc groups (extended abstract). In ACISP, pages 325–335, 2004.
9. Benoˆıt Libert, Thomas Peters, and Moti Yung. Group signatures with almost-for-free revocation. In CRYPTO, pages 571–589, 2012.
10. Adeline Langlois, San Ling, Khoa Nguyen, and Huaxiong Wang. Lattice- based group signature scheme with verifier-local revocation. In Public-Key Cryptography, pages 345–361, 2014.