PRIVACY-PRESERVING THROUGH INTERACTION WITH SMART CONTRACTS AND BLOCKCHAIN

Dr. M. Ramasubramanian[1], Baasaa Divyasri[2], Saba Afreen[3], Yenamala Ankitha[4]

Article History: Received: 08.02.2023 **Revised:** 23.03.2023 **Accepted:** 08.05.2023

Abstract

Striking a balance between invisibility and traceability is a difficult task for systems that protect privacy. Earlier introduced an legitimate user recognition management system based on group signatures for identifying authentic members. The system has no requirements for how the service provider manages user lists or other personally identifiable data. Too automatically transfer deposits from clients who don't pay service fees to the server account, smart contracts are employed. To reduce the requirement for pricey cryptographic techniques for managing smart contracts, we use Elliptic Curve Digital Signature Algorithm (ECDSA) signatures without altering the condition that smart contracts must affirm.

[1]Professor, Department of Computer Science & Engineering, Sridevi Women's Engineering College, Hyderabad, Telangana, India.
[2,3,4]Final Year B. Tech, Department of Computer Science & Engineering, Sridevi Women's Engineering College, Hyderabad, Telangana, India.

Email: [1]mailtoraams@gmail.com, [2]divyasribaasaa@gmail.com, [3]sabaafreen349@gmail.com
[4]ankithayenamala77@gmail.com

DOI: 10.31838/ecb/2023.12.s3.272

1. INTRODUCTION

Group signatures offer traceability via the use of a supervisor who is capable to identify valid signers as well as invisibility for signers through the verification mechanism that validates a signer membership in the group. In order to protect privacy and responsibility, this anonymity and traceability are crucial. For instance, Isshiki et al. introduced the Isshiki system, a group signature-based identity management system that protects user privacy. Reporting serving serves as the group manager in this system. The reporting server provides a signature key for a group signature algorithm to a service user and creates a group signature. Because group signatures are anonymous, the service provider only can confirm whether a client is a legitimate participant before offering a service. Subsequent to providing the service, the supplier dispatch a bill to a different organization known as the reporting server, which controls the group signatures' opening key. A invoice is sent to the user once the reporting server unlock the group signature, recognizes the client who utilized the assistance, and unbars the group signature. Since group signatures can be monitored, none exist that are authentic but cannot be connected to a person.

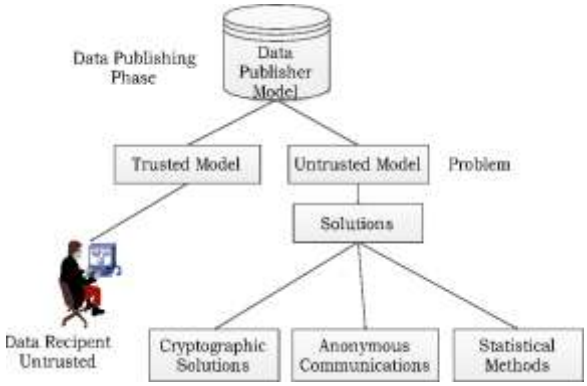

Fig.1: Example figure

To put forward earlier practice, any group signature method may be employed, in which a user-revocation system was created which removes clients from the server. The use of revocations when customers cancel services or ignore invoices was also covered earlier extended to the revocable group signature algorithm to produce the fundamental group signature system that is fickle. We draw attention to the fact that, even though the reporting server and user-revocation manager under these schemes may share the same entity, to guarantee that the tracing capacity is segregated, the service provider must be a different company. The fact that the service supplier is not obligated to control sensitive content like clients lists makes it imperative to stress that there is absolutely no risk of personal information leaking. The earlier system outruns rivals as to preserve client privacy while reducing the danger of private data leakage given the frequency of such occurrences. The earlier system can be compared to a bill-collection method that respects individual privacy.

Literature Review

Group signatures with completely dynamic membership secrecy:

By allowing the creation of fraud-proof signatures in the title of a group that disclose nothing about the genuine signer's identity other than their group associateship, group signatures strike a settlement between the traditional uses of digital signatures and the necessity for client privacy. Popular models fail to take into account an important factor: the possibility that legitimate client itself may include sensitive data. This is particularly true if a group's membership is dynamic, which means that a member's status could alter over time. We offer formal notions of membership privacy that are easy to incorporate in the most revealing structures of group signature security. Then, based on Signatures with Flexible Public Keys (SFPK) and Signatures on Equivalence Classes, we propose a general architecture for a strong group signature system with associateship privacy. This demonstrates that, despite the fact that the strictly greater security concepts we offer have never been examined in the research of strong group signatures before, they don’t cost more in actual use.

Efficiency gains for a group signature technique with contingency revocation:

One of the most critical concerns in group signature schemes is member abrogation, and several fickle methods have been presented. A Group Signature technique with Probabilistic Revocation (GSPR) has just been introduced. In GSPR, the compute amount for the abrogation inspect is dramatically decreased by applying a unique idea of contingency revocation, even while the accuracy of the examination is with a certain contingency. However, there is another issue with the GSPR scheme: m alias elements are embedded in a member's certificate.

Then, in the signing process, each element is used, and O(m) exponentiations are required to demonstrate that the used elements is embedded in the certificate.

Bulletproofs: short evidences for secret proceedings and other purposes:
We put forth Bulletproofs, a ground-breaking non-collaborative zero-knowledge evidence protocol with incredibly brief evidences, no trusted setup, and proof sizes that are just logarithmic in witness size. The times required to create and validate proofs are linear in n. For the privacy of Bitcoin and other cryptocurrencies, existing solutions perform significantly better than linear sized range proofs using bulletproofs. Additionally, bulletproofs enable the accumulation of range evidences, which enables a customer to show that m allegiances fall inside a certain range using just a few additive O(log(m)) group components dispersed across a single proof. We provide a uncomplicated Multi-Party Computation (MPC) protocol for building Bulletproofs that enables the customers to create a single evidence without disclosing their inputs to one another.

Hawk: Smart Contracts with Privacy-Preserving Cryptography and the Blockchain:
Mutually mistrusting parties can conduct secure agreements without the involvement of a third party. The decentralized blockchain makes sure that honest parties get fair recompense in the case of contract violations or terminations. Transactional privacy, however, is absent from current systems. On the blockchain, every transaction is visible, counting the movement of money linking pseudonyms and the total amount transacted. We introduce segregated smart contract solution that maintains transactional privacy from public view by not storing financial transactions on the blockchain in clear text. Hawk's compiler automatically creates an effective cryptographic protocol for contractual parties to interact with the blockchain using cryptographic primitives like zero-knowledge proofs, so a programmer can create a private smart contract in an intuitive way without having to implement cryptography.

To ensure that bitcoin payments are fair:
A variety of cryptocurrencies, including Litecoin, Dogecoin, and Ethereum, are rising in popularity as a result of the widespread success and adoption of Bitcoin. Despite the fact that current blockchain-based cryptocurrency schemes can provide an acceptable level of security for transactions, they take no account of the concept of fairness. Two players can trade digital "items," such as digital signatures, in a fair manner over unconfident networks in order for either both players to obtain the other's item or for neither player to receive it. Enabling justice in existing cryptocurrencies is a crucial but under-examined subject given that blockchain participants often do not trust one another. In this paper, we examine potential solutions for facilitating a fair cryptocurrency payment and receipt exchange. We consider an exchange's timeliness to be a crucial characteristic, specifically when one of the parties is resource-constrained. We define "strong timeliness" for a fair trade mechanism and suggest two iterations of the honest payment-for-receipt protocol that take advantage of Ethereum capability to reach secure timeliness. We put both into practice and evaluate their efficacy and security.

IMPLEMENTATION
An earlier version of this article provided a valid user recognition structure based on group signatures, in which a service supplier decides whether clients of the service are actual members, and only a reporting server may identify clients in order to send them charges. Because the service supplier is not necessary to maintain private data like clients lists, the earlier system performs better than others in safeguarding client privacy and lowering the danger of private information leaking. It's also vital to keep in mind that the earlier system only contemplate cases to which the reporting server recognizes consumers who have used the service, and that recognized customers who refuse to pay bills are really able to use the service for free.

Disadvantages:
- It enables the system to perform better than others as to protect client privacy and controlling the danger of private information leakage.
- In fact, the service is free for identifiable users who disregard bills.

We outline the suggested, legally enforced bill collecting method. Users, service providers, and reporting server are the three components that make up the system. A certificate with a ring signature is verified by the service provider, who also renders a service. Service providers do not possess any personal information, much like the Isshiki system. Users who have utilized the service are identified by the reporting server, who then sends them charges. In the event that a user declines to do payment for used services, the bill amount is either accordingly transmitted to the reporting server via the smart contract or it is transferred by force. be We point out ring signatures are transmitted over an off-chain route since anonymity is compromised by the fact that the user address is made available when the transaction is released. We also want to point out that when a charge is compelled to be paid via a smart contract, anonymity is not something we take into account.

Advantages:

- Without specifically altering the state that must be confirmed in smart contracts, we used signatures generated by the widely used Elliptic Curve Digital Signature technique (ECDS).

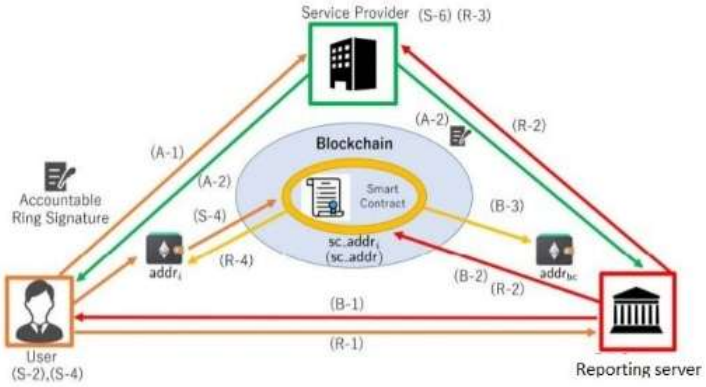

Fig.2: System architecture

2. Methodology

All service recharges today take place online, requiring consumers to register for services and service providers to deliver them in exchange for payment of fees. All service users' data will be accessible to the service provider, who may misuse it. To address this issue, "Isshiki" introduced a user privacy-preserving and identifying approach based on group signature. Wherein all users in a group will be signed by a single key, and the user in the group can be able to verify, trace, and view information; however, in this technique, reporting server and service providers can view all consumers' data, and in this system, consumers who ignore bills can use services for free because they already hold signed keys with the group, while consumers who are not using services must pay the bill. To overcome these two drawbacks, the author of this paper has in mind a number of solutions.

In the proposed paper, a smart contract for bill collection will be set up on the blockchain by requesting a security deposit from each user. If any user fails to make a payment, money will be deducted from his security deposit and given to the service provider. Only users who utilize the services will be covered by this blockchain smart contract, and the service provider will issue the bill, which the bill collector will then generate and deliver to the USER or CONSUMER for payment. Therefore, by using this smart contract, bills will only be generated for users who are using the services, and if any users ignore bills, bill payment will be made from security deposit.

Consumer and bill collector will sign documents using the Elliptic Curve Cryptography (ECC) technique to ensure the privacy of user data. Only these two users will be able to verify and access the data. The service provider won't see any data since the reporting server will only add the bill amount by utilizing the customer's login or ID. Reporting server will examine consumer data to create an invoice.

Modules:

To implement this project, we have designed the below modules

1) Service Provider Login: To access the program, use the username "provider" and password "provider," and then enter the bill amount.

2) Reporting Server: After entering the username "collector" and password "collector," the reporting server may see the user's bill amount as given by the service provider and create an invoice.

3) User: A security deposit will be placed to the user's account when they register with the service provider to get various services. To access the current bill amount for payment, a user must sign into the application.

5. Experimental Outcomes

Fig.3: Home screen

Fig.4: Signup

Fig.5: Service provider Login

Fig.6: Add bill amount

Fig.7: Bill collector login

Fig.8: generate invoice

Fig.9: User login

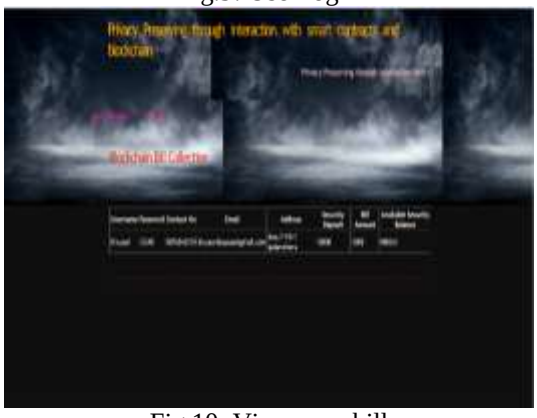

Fig.10: View your bill

3. Conclusion

In this work, we suggested an enforced bill collection system that offers the feature of forcing consumers to pay service fees while protecting their privacy. The suggested solution is based on the usage of smart contracts and responsible ring signatures.

Future Scope

It would be interesting to improve the privacy of our system in future work, for instance by introducing associateship privacy using the created strong group signature technique. It would also be fascinating to create a bill-collection method that uses anonymous crypto currencies like Monero or Zcash to take service fees from clients anonymously.

4. References

A Privacy-Preserving Enforced Bill Collection System using Smart Contracts, Tomoki Fujitani ,University of Tsukuba National Institute of Information and Communications Technology Japan; Keita Emura, National Institute of Information and Communications Technology Japan; Kazumasa Omote ,University of Tsukuba National Institute of Information and Communications Technology Japan, IEEE 2021 16th Asia Joint Conference on Information Security (AsiaJCIS).

Ivan Damgard, Chaya Ganesh, Hamidreza Khoshakhlagh, Claudio Or- ˚ landi, and Luisa Siniscalchi. Balancing privacy and accountability in blockchain identity management. In CT-RSA, pages 552–576, 2021.

Panagiotis Chatzigiannis, Foteini Baldimtsi, and Konstantinos Chalkias. SoK: Auditability and accountability in distributed payment systems. In Applied Cryptography and Network Security, pages 311–337, 2021.

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.

Benedikt Bunz, Shashank Agrawal, Mahdi Zamani, and Dan Boneh. ¨ Zether: Towards privacy in a smart contract world. In Financial Cryptography and Data Security, pages 423–443, 2020.

Cheng Shi and Kazuki Yoneyama. Formal verification of fair exchange based on bitcoin smart contracts. In INDOCRYPT, pages 89–106, 2020.

Keita Emura and Takuya Hayashi. A revocable group signature scheme with scalability from simple assumptions. IEICE Trans. Fundam. Electron. Commun. Comput. Sci., 103-A(1):125–140, 2020.

Lisa Eckey, Sebastian Faust, and Benjamin Schlosser. OptiSwap: Fast optimistic fair exchange. In ASIACCS, pages 543–557, 2020.

Yu Chen, Xuecheng Ma, Cong Tang, and Man Ho Au. PGC: decentralized confidential payment system with auditability. In ESORICS, pages 591–610, 2020.

Eric Wagner, Achim Volker, Frederik Fuhrmann, Roman Matzutt, and ¨ Klaus Wehrle. Dispute resolution for smart contract-based two-party protocols. In IEEE ICBC, pages 422–430, 2019.

Kazuma Ohara, Keita Emura, Goichiro Hanaoka, Ai Ishida, Kazuo Ohta, and Yusuke Sakai. Shortening the Libert-Peters-Yung revocable group signature scheme by using the random oracle methodology. IEICE Trans. Fundam. Electron. Commun. Comput. Sci., 102-A(9):1101–1117, 2019.

Michael Backes, Lucjan Hanzlik, and Jonas Schneider-Bensch. Membership privacy for fully dynamic group signatures. In ACM CCS, pages 2181–2198. ACM, 2019.

Nasima Begum and Toru Nakanishi. Efficiency improvement in group signature scheme with probabilistic revocation. J. Inf. Process., 27:508– 516, 2019.

Prastudy Fauzi, Sarah Meiklejohn, Rebekah Mercer, and Claudio Orlandi. Quisquis: A new design for anonymous cryptocurrencies. In ASIACRYPT, pages 649–678, 2019.

San Ling, Khoa Nguyen, Huaxiong Wang, and Yanhong Xu. Latticebased group signatures: Achieving full dynamicity (and deniability) with ease. Theor. Comput. Sci., 783:71–94, 2019.

Yasuyuki Seita and Toru Nakanishi. Speeding up revocable group signature with compact revocation list using vector commitments. IEICE Trans. Fundam. Electron. Commun. Comput. Sci., 102-A(12):1676– 1687, 2019.

Yue Zhang, Jian Weng, Jia-Si Weng, Ming Li, and Weiqi Luo. Onionchain: Towards balancing privacy and traceability of blockchain-based applications. CoRR, abs/1909.03367, 2019.

Ai Ishida, Yusuke Sakai, Keita Emura, Goichiro Hanaoka, and Keisuke Tanaka. Fully anonymous group signature with verifier-local revocation. In Security and Cryptography for Networks, pages 23–42, 2018.

Benedikt Bunz, Jonathan Bootle, Dan Boneh, Andrew Poelstra, Pieter ¨ Wuille, and Gregory Maxwell. Bulletproofs: Short proofs for confidential transactions and more. In IEEE Symposium on Security and Privacy, pages 315–334, 2018.

Jian Liu, Wenting Li, Ghassan O. Karame, and N. Asokan. Toward fairness of cryptocurrency

payments. IEEE Secur. Priv., 16(3):81–89, 2018.

Nicola Atzei, Massimo Bartoletti, Tiziana Cimoli, Stefano Lande, and Roberto Zunino. SoK: Unraveling bitcoin smart contracts. In POST, pages 217–242, 2018.

Riccardo Spagni. Monero 0.13.0 "Beryllium Bullet" release. https://web.getmonero.org/tr/2018/10/11/monero-0.13.0-released.html. Accessed : 2018-10-11.

Stefan Dziembowski, Lisa Eckey, and Sebastian Faust. FairSwap: How to fairly exchange digital goods. In ACM CCS, pages 967–984, 2018.

G. Wood. Ethereum: A secure decentralised generalised transaction ledger (eip-150 revision), 2017. https://gavwood.com/paper.pdf.

Matteo Campanelli, Rosario Gennaro, Steven Goldfeder, and Luca Nizzardo. Zero-knowledge contingent payments revisited: Attacks and payments for services. In ACM CCS, pages 229–243, 2017.

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.

Shifeng Sun, Man Ho Au, Joseph K. Liu, and Tsz Hon Yuen. RingCT 2.0: A compact accumulator-based (linkable ring signature) protocol for blockchain cryptocurrency Monero. In ESORICS, pages 456–474, 2017.

Ahmed E. Kosba, Andrew Miller, Elaine Shi, Zikai Wen, and Charalampos Papamanthou. Hawk: The blockchain model of cryptography and privacy-preserving smart contracts. In IEEE Symposium on Security and Privacy, pages 839–858, 2016.

Jonathan Bootle, Andrea Cerulli, Pyrros Chaidos, Essam Ghadafi, and Jens Groth. Foundations of fully dynamic group signatures. In Applied Cryptography and Network Security, pages 117–136, 2016.

ethereumjs-util. 7.0.7, 2020-10-15, https://github.com/ethereumjs/ ethereumjs-util.

Jonathan Bootle, Andrea Cerulli, Pyrros Chaidos, Essam Ghadafi, Jens Groth, and Christophe Petit. Short accountable ring signatures based on DDH. In ESORICS, pages 243–265, 2015.

Monero. https://getmonero.org.

Testnet Ropsten (ETH) blockchain explorer. https://ropsten.etherscan.io/.

Vireshwar Kumar, He Li, Jung-Min "Jerry" Park, Kaigui Bian, and Yaling Yang. Group signatures with probabilistic revocation: A computationally-scalable approach for providing privacy-preserving authentication. In ACM CCS, pages 1334–1345, 2015.

Zcash. https://z.cash/.

] 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.

Nuttapong Attrapadung, Keita Emura, Goichiro Hanaoka, and Yusuke Sakai. A revocable group signature scheme from identity-based revocation techniques: Achieving constant-size revocation list. In Applied Cryptography and Network Security, pages 419–437, 2014.

Benoˆıt Libert, Thomas Peters, and Moti Yung. Group signatures with almost-for-free revocation. In CRYPTO, pages 571–589, 2012.

Benoˆıt Libert, Thomas Peters, and Moti Yung. Scalable group signatures with revocation. In EUROCRYPT, pages 609–627, 2012.

Yusuke Sakai, Jacob C. N. Schuldt, Keita Emura, Goichiro Hanaoka, and Kazuo Ohta. On the security of dynamic group signatures: Preventing signature hijacking. In Public Key Cryptography, pages 715–732, 2012.

Ivan Damgard. On ˚ Σ-protocols. https://www.cs.au.dk/∼ivan/Sigma.pdf, 2010.