Protecting Blockchain-based Decentralized Timed release of Data from Malicious Adversaries

Jingzhe Wang
School of Computing and Information
University of Pittsburgh
Pittsburgh,USA
jiw148@pitt.edu

Balaji Palanisamy
School of Computing and Information
University of Pittsburgh
Pittsburgh,USA
bpalan@pitt.edu

***Abstract*—Timed-release of information refers to releasing protected sensitive data at a future point of time while securely protecting the information until the release time. Blockchain-based self-emerging data infrastructures consist of a group of blockchain accounts that jointly take charge of protecting and transferring the data at the release time. Existing solutions have focused on fully rational adversarial environments in which all peer accounts are rational. However, such protection disregards scenarios in which malicious peer accounts also exist. In our work, we focus on protecting blockchain-based timed-release service in mixed adversarial environments in which both rational peer accounts and malicious peer accounts exist. We introduce our blockchain-based timed-release framework designed for mixed adversarial environments and illustrate two concrete attacks, namely *drop attack* and *release-ahead attack*, and discuss our reputation-based solution.**

***Index Terms*—Timed Release, Blockchain, Smart Contract**

I. Introduction

Timed-release of information refers to releasing protected sensitive data at a future point of time while securely protecting the information until the release time. Examples of applications using timed data release include secure auction systems where important bidding information needs protection until arrivals of all bids. Blockchain-based self-emerging data infrastructures consist of a group of blockchain accounts that jointly take charge of protecting and transferring released data. Existing solutions [2]–[4] provide service support in a fully rational adversarial environment in which all peer accounts are rational. Recent work [3] has formulated the timed-release service protocol over Ethereum [6] network using an *imperfect information game* [1]. Under the assumption that all peers are rational, the existence of *Nash Equilibrium* [5] guarantees that every peer acts honestly. However, such a design disregards a practical scenario in which malicious peer accounts may also exist in blockchain networks. Since the malicious peer accounts do not care about any economical loss, the equilibrium will be broken even when one malicious peer account exists, which renders the protection invalid. In our work, we propose a reputation-based timed-release service to handle the mixed adversarial environment that includes both rational and malicious peers.

II. Framework Design

978-1-6654-9538-7/22/$31.00 ©2022 IEEE

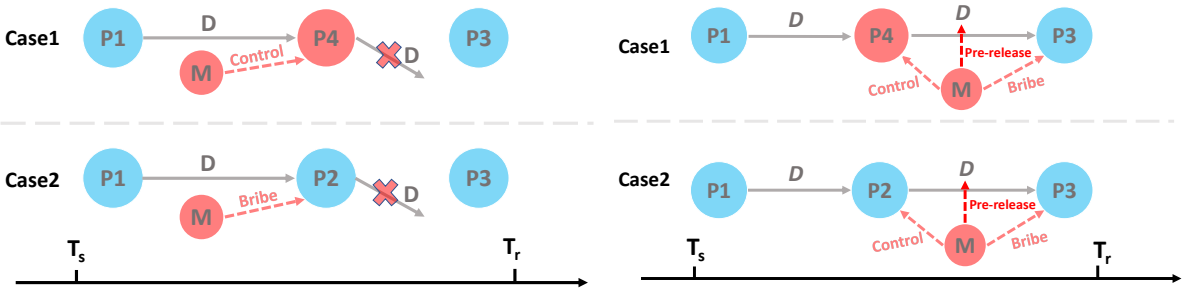
A. Key Components

There are four key components in a timed-release service as described below:
(1) Data Sender: The data sender initializes the timed-release service request. The sender encrypts the private data with a secret key and sends the encrypted private data to a trusted cloud storage platform. In parallel, the sender sends the encrypted secret key to the blockchain network and the key will be released at a prescribed release time; **(2) Data Recipient:** For each timed-release service request, the corresponding data recipient is responsible for receiving and decrypting the encrypted secret key sent by the data sender at the prescribed release time. The data recipient then decrypts the encrypted private data from the cloud storage to obtain the original private data; **(3) Cloud:** A cloud storage infrastructure acts as a third-party storage platform between the data sender and data recipient to store the encrypted private data; **(4) Blockchain Infrastructure:** In our framework, the Ethereum network serves as the blockchain infrastructure for implementing the timed release service protocol.

B. Adversarial Model

We consider three different types of peers, namely *honest peer*, *rational peer*, and *malicious peer* in the blockchain open marketplace. An *honest peer* always participates in the timed-release service protocol with absolutely honest actions. This type of peer never performs any malicious actions. On the other hand, every *rational peer* acts with economic rationality. Such a type of peer is driven by self-interest, and only chooses to violate timed-release service protocol when doing so enables to earn a higher profit. A *malicious peer* always acts maliciously and launches attacks and deviates arbitrarily from the prescribed timed-release service in an attempt to violate the security.

We consider two attacks in our framework. One is *drop attack*, which aims at destroying the data D before the prescribed release time T_r and results in a failing data release at T_r. Such an attack may be launched by a malicious adversary who controls one or more peers engaging in the timed-release service. For example, in Case 1 of Fig. 1a, the malicious adversary M could control the malicious peer P_4 to drop D, and after T_r, D is missing. In Case 2, in another service, M



(a) Drop Attack

(b) Release-ahead Attack

Fig. 1: Attack Examples

could let the rational peer P_2 drop D by bribing P_2 through off-chain interactions and make P_2 earn more profit. As a consequence, after T_r, nothing will be released. In contrast to the drop attack, a *release-ahead attack* results in the premature release of D. It can be launched by a malicious adversary by controlling a fraction of the total peers in the timed-release service to get D before the prescribed release time and disclose it. For example, in Fig. 1b Case 1, the malicious adversary M may control both P_4 and P_3 to successfully launch a release-ahead attack. Specifically, by following onion routing described in [3], the data D will be encrypted using the public keys of P_1, P_4, and P_3. If M wants to pre-release D, he/she must control P_4 to acquire the encrypted data and control P_3 to get the private key of P_3 to decrypt the encrypted data and pre-release at that time point which is earlier than T_r. Similar logic applies in Case 2, except that the malicious peer M needs more monetary cost for successfully bribing both P_2 and P_3 since they are rational peers.

III. Proposed Solution

Our objective is to design an attack-resilient timed-release protocol to handle a mixed adversarial environment. To this end, we first design a reputation measure to evaluate the behavior of each peer engaging in timed-release services. Specifically, we quantitatively measure the reputation with uncertainty, a score which indicates the likelihood of honest behavior of a peer when he/she participates in an incoming timed-release service. For example, if a peer has a score of 0.41, a sender believes that such a peer will have 0.41 likelihood to honestly follow an incoming timed-release service. Based on the reputation measure, the sender strategically performs peer selection, namely a reputation-aware peer selection, in which the sender selects a set of peers having high reputation score to achieve good attack resilience. The resilience metric captures two aspects: one is release-ahead attack resilience, which quantifies the resistance of the selected peers to the release-ahead attack and the other one is drop attack resilience, which quantifies the resistance of the selected peers to the drop attack. Through a service enforcement design, the protocol autonomously enforces the timed-release service with the help of smart contracts. Specifically, such a policy consists of a misbehavior report module which emits any attack evidence, as well as a service summary report, which performs behavior evaluations and reputation updating. After the recipient receives the data, the service will be closed.

To study the effectiveness and applicability of our proposed solution, a simulator and a smart contract implementation are being developed. The simulation study is focused on evaluating the attack resilience while the smart contract implementation will be deployed on the Ethereum public test network to test the *Gas* consumption.

IV. Conclusion & Future Work

We propose a blockchain-based timed-release service framework for protecting against malicious adversaries in mixed adversarial environments. The proposed approach adopts a reputation-aware peer recruitment policy to increase the attack resilience. Our ongoing and future work is focused on implementing and evaluating the proposed solution in terms of attack resilience and gas consumption.

Acknowledgement

The authors acknowledge the support for this work through a grant (Award #2020071) from the National Science Foundation (NSF) SaTC program. Any opinions, findings, and conclusions or recommendations expressed in this material are those of the author(s) and do not necessarily reflect the views of the National Science Foundation.

References

[1] Kevin Leyton-Brown and Yoav Shoham. Essentials of game theory: A concise multidisciplinary introduction. *Synthesis lectures on artificial intelligence and machine learning*, 2(1):1–88, 2008.

[2] Chao Li and Balaji Palanisamy. Decentralized privacy-preserving timed execution in blockchain-based smart contract platforms. In *2018 IEEE 25th International Conference on High Performance Computing (HiPC)*, pages 265–274. IEEE, 2018.

[3] Chao Li and Balaji Palanisamy. Decentralized release of self-emerging data using smart contracts. In *2018 IEEE 37th Symposium on Reliable Distributed Systems (SRDS)*, pages 213–220. IEEE, 2018.

[4] Chao Li and Balaji Palanisamy. Silentdelivery: Practical timed-delivery of private information using smart contracts. *IEEE Transactions on Services Computing*, 2021.

[5] John F Nash Jr. Equilibrium points in n-person games. *Proceedings of the national academy of sciences*, 36(1):48–49, 1950.

[6] Gavin Wood et al. Ethereum: A secure decentralised generalised transaction ledger. *Ethereum project yellow paper*, 151(2014):1–32, 2014.