Blockchain-enabled Payment Networks

CrySPR Lab: Cryptography Security and Privacy Lab. https://sites.google.com/view/crysprlabnmsu/home

Roopa Vishwanathan, Computer Science, New Mexico State University
roopav@nmsu.edu

INTRODUCTION

BlANC – Payment network to overcome the shortcomings from Speedy Murmurs and provide better routing capabilities for transition in Payment networks such as Ripple etc..

SAMPL – In this paper we discuss we present SAMPL, a novel auditing framework which leverages cryptographic mechanisms, such as zero knowledge proofs, Pedersen commitments, Merkle trees, and public ledgers to create a scalable mechanism for auditing electronic surveillance process involving multiple actors

Rebalancing –Our decentralized technique of rebalancing will help users in acyclic payment channel networks to rebalance their link weights on an as-needed basis

BLANC - CONTRIBUTIONS

BlANC, a novel, fully de-centralized blockchain-based credit network where credit transfer between a sender-receiver pair happens on demand.

BlANC provides:

- User and transaction privacy, while providing transaction integrity, and accountability. Users can choose to split their credit requests across multiple paths in the network.
- On-demand routing, that can swiftly adapt to changing network topology, with quick on-boarding/off-boarding of users, and very low maintenance overhead
- Capability for concurrent transactions.
- Distributed blockchain-based approach to publicly document transactions and identify malicious actors in transactions.
- we propose an alternative to proposed landmarks- based routing and DCN maintenance techniques, by having a subset of users facilitating transactions, termed routing helpers (RHs)

SAMPL - CONTRIBUTIONS

SAMPL, a novel auditing framework which leverages cryptographic mechanisms, such as zero knowledge proofs, Pedersen commitments, Merkle trees, and public ledgers to create a scalable mechanism for auditing electronic surveillance process involving multiple actors.

SAMPL is the first framework that can identify the actors (e.g., agencies and companies) that violate the purview of the court orders

Our novel contributions include

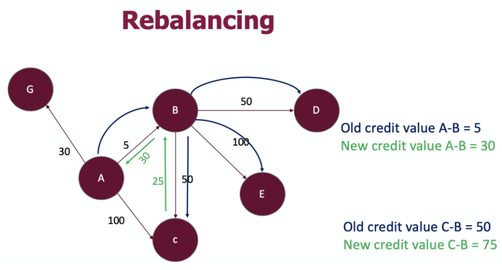
- Design of SAMPL: a generic and scalable framework for accountability of monitoring processes.
- Capability for auditing the compliance of the entities over the lifetime of the surveillance order, from the outset.
- A case study of our system in the context of the US legal system.
- Security analysis of the the proposed framework.

REBALANCING

we propose a technique for rebalancing link weights in acyclic payment networks, which are peer-to-peer networks with payment channels or links between users in an acyclic manner.

We provide

- Rebalance credit links on an as-needed basis
- Transparent rebalancing without any third-party involvement
- Minimal computational cost and only off-chain transactions



BLANC – RESULTS AND DISCUSSION

The operations of BLANC is summed up into 1. Find Route 2. Pay and 3. Hold phase

We discuss security framework with respect to the UC framework

We provide the following security and privacy properties

Sender/receiver privacy

Link privacy

Value Privacy

Accountability

Blanc is a credit network that preserves user and transaction anonymity, enables on-demand and concurrent transactions to happen seamlessly, and can identify malicious network actors that do not follow the protocols and disrupt operations.

SAMPL – DISCUSSION

In our system, there are six parties: the individual being surveilled I , company C that I has an account (e.g., e-mail) with, law enforcement/intelligence gathering agency L requesting the surveil- lance, Judge J who can potentially issue the surveillance order on I , and an Enforcer E, who enforces accountability of L and C's operations, by ensuring that L does not request more information about I than what is authorized by J , and C does not over-share information about I , more than what is authorized by J

we discuss how our system can be instantiated and adapted in a real-world legal systems with respect to the following systems mentioned below:

- Electronic Communications Privacy Act (ECPA)
- National Security Letter (NSL):
- Foreign Intelligence Surveillance Act (FISA)
- Separate simulations were run for 5, 10, 15, and 30 users in the SO posted by J . The surveillance periods simulated were 5, 10, 20, and 50 days.

SAMPL can apply to other types of surveillance criteria by modifying the way user records are stored by C

PUBLICATIONS

Blanc -Panwar, G., Misra, S., & Vishwanathan, R. (2019). BlAnC: Blockchain-based Anonymous and Decentralized Credit Networks. In Proceedings of the Ninth ACM Conference on Data and Application Security and Privacy (pp. 339–350).

SAMPL – To be published in ACM CCS 2019

Rebalancing in Acyclic Payment Networks - Muthu Subramanian, Lalitha, Guruprasad Eswaraiah, and Roopa Vishwanathan. "Rebalancing in Acyclic Payment Networks." Proceeding, 2019 17th International Conference on Privacy, Security and Trust (PST).

Research supported by NSF award #1800088