A Blockchain-Based Privacy-Preserving Medical Insurance Storage System

Son Luong (Master Student) and Rongxing Lu*

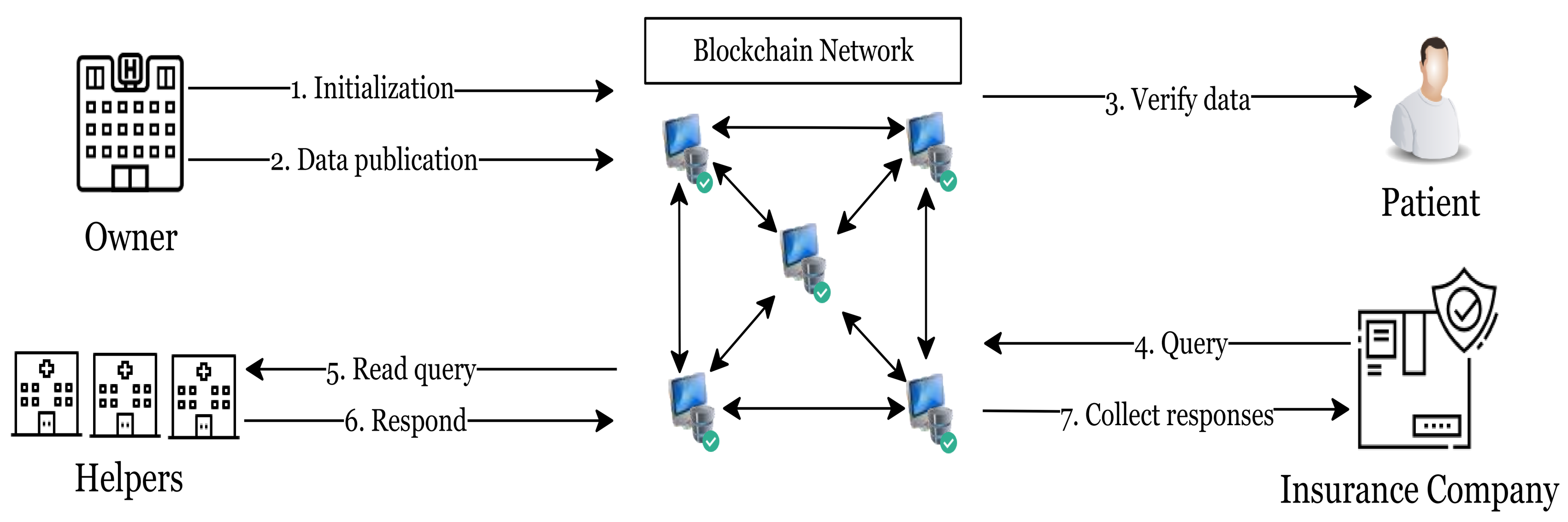
Contact Email: rlu1@unb.ca

Canadian Institute for Cybersecurity (CIC), Faculty of Computer Science, University of New Brunswick (UNB)

ABSTRACT

Blockchain technology is an innovative invention that is disrupting many industries including business and healthcare. The blockchain is essentially a secure, immutable ledger that is distributed over a decentralized network. In this work, we propose a blockchain-based privacy-preserving medical insurance storage system. This system takes advantage of the decentralization and immutability properties of blockchain technology, and makes use of a (2,3)-threshold secret sharing scheme to achieve the privacy-preservation property. In a basic instance of the system, there are a public blockchain, a patient, four hospitals - an owner hospital and three helper hospitals, and an insurance company. The owner hospital holds the spending data of the patient and publishes that data to the blockchain. The helper hospitals help the insurance company to query for the patient's spending data on the blockchain and perform homomorphic computations on the results. Meanwhile, the helpers cannot learn anything about the patient's spending data, as long as there is no collusion between helpers. We deploy our system on the Ethereum blockchain for performance evaluation.

System Model



Owner Hospital: Holds the spending data of the patient. Responsible for initializing the system and publishing the patient's data to the blockchain

Patient: Anybody who has spent money for hospital service at owner hospital. The Patient can verify the data published by owner hospital.

Helper Hospitals: Help processing the insurance company's queries for the patient's spending data .

Insurance Company: Can send queries to ask for the spending data of the patient.

Design Goals

- **Privacy Preservation:** The most important requirement of this scheme is privacy preservation. In other words, the initialization data, the stored spending data and the query result on the blockchain are kept secret from unauthorized entities.
- **Verifiable:** Every data published on the blockchain are publicly verifiable to prevent from cheating. Furthermore, a mechanism is also implemented to punish the data owner or helpers if they try to provide incorrect information. Because every transaction is digitally signed, the system is also non-repudiable.
- **High-availability**: Because every communication happens on the blockchain, the system is required to have high availability. In our case, we employ the *(2,3)-secret sharing scheme* which is robust against failures as long as 2/3 helpers function properly. Generally, the system can be scaled to support any *(t,n)* when more hospitals join the network.

Initialization

- The owner hospital HS_0 generate secret keys (x_1, x_2, x_3) for the helper hospitals HS_1, HS_2 and HS_3.
- HS_0 encrypts (x_1, x_2, x_3) with HS_1, HS_2 and HS_3's public keys and publish the ciphertexts to the blockchain along with some commitments.
- HS_1, HS_2 and HS_3 read the blockchain and retrieve x_1, x_2, x_3 respectively.

Data Publication

- The owner hospital HS_0 wants to publish the value d_z of an invoice Z.
- HS_0 splits d_z into (d_{z1}, d_{z2}, d_{z3}) such that $d_z = d_{z1} + d_{z2} + d_{z3}$
- HS_0 encrypts (d_{z1}, d_{z2}, d_{z3}) using (x_1, x_2, x_3) in such a way that:
  - HS_1 can read d_{z1}, d_{z2}
  - HS_2 can read d_{z2}, d_{z3}
  - HS_3 can read d_{z3}, d_{z1}

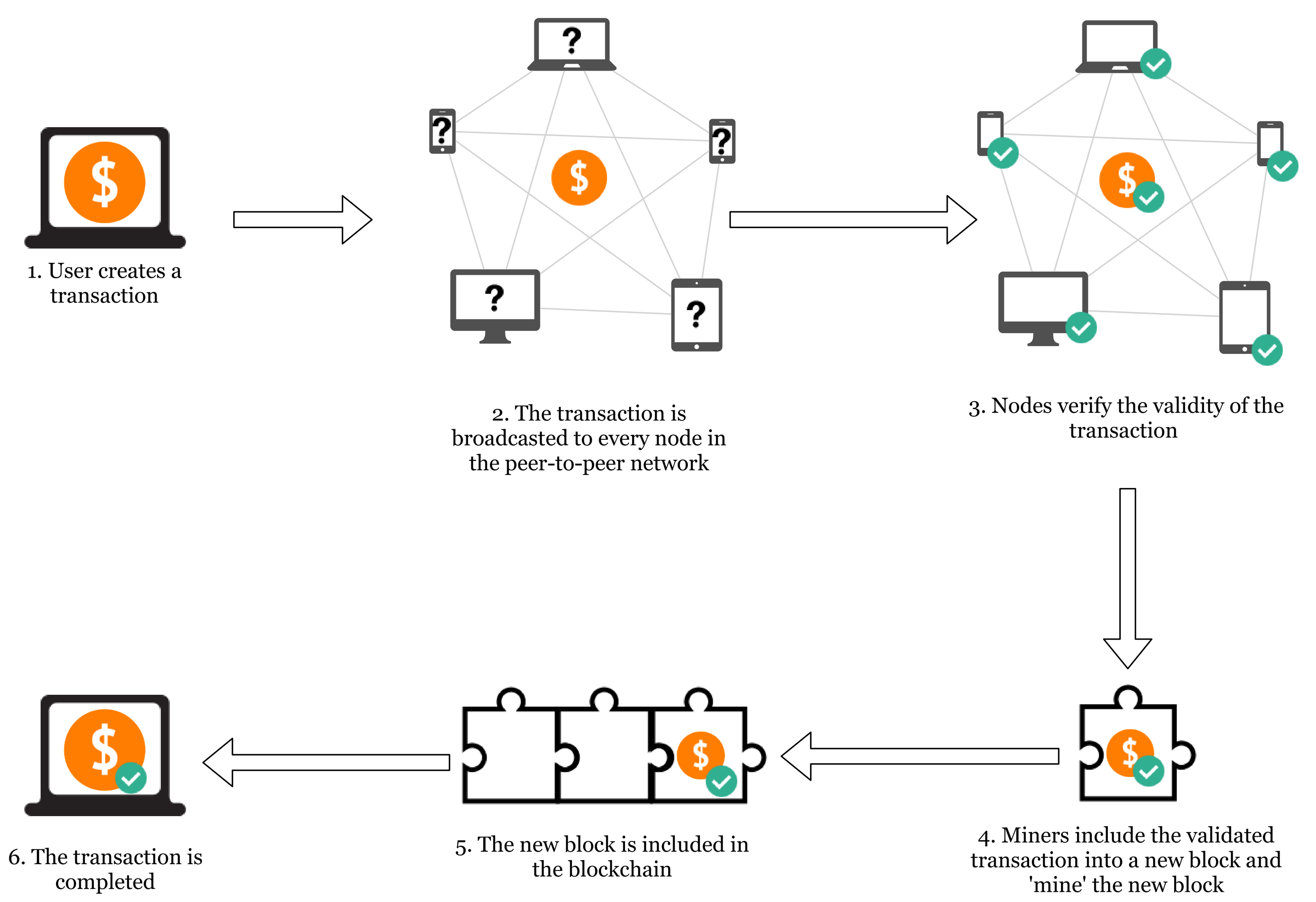
	dz_1	dz_2	dz_3
HS_1	✔	✔	
HS_2		✔	✔
HS_3	✔		✔

The secret sharing distribution scheme

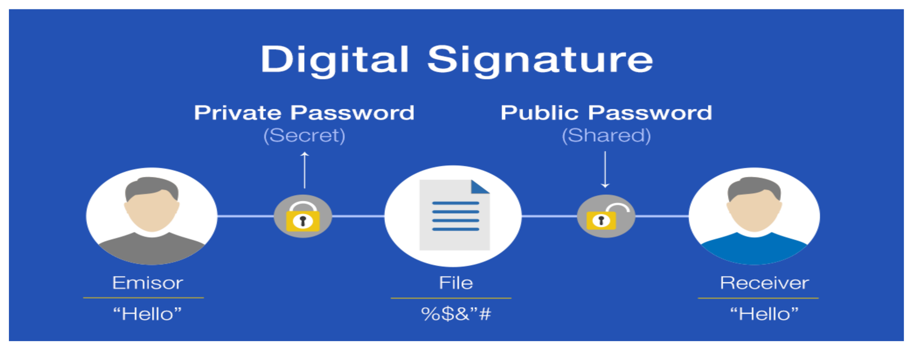
Data Request and Response

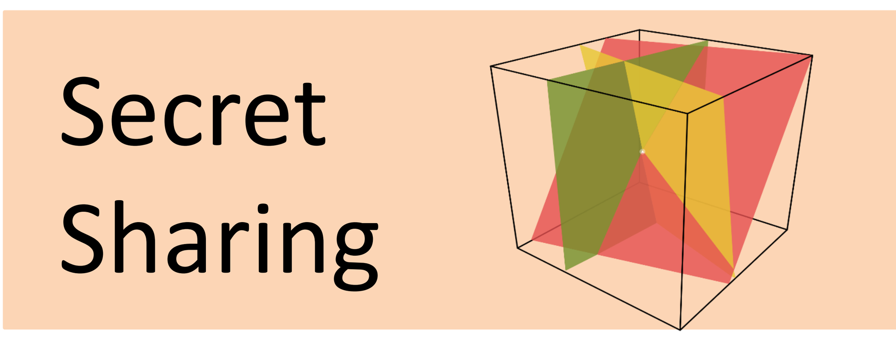
- Insurance company I issues a query request to learn about patient P's spending data. The request is published on the blockchain.
- HS_1, HS_2 and HS_3 read the request on the blockchain and start finding all of patient P's invoices. Since the value d_z of every invoice is split into (d_{z1}, d_{z2}, d_{z3}), the goal of the helper hospitals in to get the sum of all (d_{z1}, d_{z2}, d_{z3}).
- According to the distribution scheme, HS_1 only has access to (d_{z1}, d_{z2}), HS_2 only has access to (d_{z2}, d_{z3}) and HS_1 only has access to (d_{z3}, d_{z1}) of all invoices.
- Consider D_1 to be the sum of all d_{z1}'s, D_2 to be the sum of all d_{z2}'s and D_3 to be the sum of all d_{z3}'s.
- HS_1 can generate (D_1, D_2), HS_2 can generate (D_2, D_3) and HS_3 can generate (D_3, D_1). Each helper publishes their respective sums to the blockchain after encrypting them with insurance company I's public key.
- Insurance company I retrieves the sums on the blockchain and proceeds to aggregate the answers to get the total sum $D = D_1 + D_2 + D_3$.

Blockchain Transaction and Block Creation



Cryptographic Techniques





Conclusion

In this work, we proposed a blockchain-based privacy-preserving medical insurance storage system. With blockchain integration, our system takes advantage of decentralization, tamper resistance, privacy-preservation and high availability. Because of the blockchain's decentralization, parties can communicate without the need of a central entity, reducing the cost and eliminate the single point of failure. The data recorded in the system is highly credible due to the tamper-resistance property of blockchain. Furthermore, from the use of a threshold scheme to share secrets, sensitive patient data is confidential as long as the helper hospitals are honest, effectively preserving the privacy of patients.