SECURITY MODEL FOR PRIVACY-PRESERVING BLOCKCHAIN-BASED CRYPTOCURRENCY SYSTEMS

NSS 2023

Mayank Raikwar[1], Shuang Wu[2], Kristian Gjøsteen[3]

[1] University of Oslo, Norway
[2] DNV, Trondheim, Norway
[3] Norwegian University of Science and Technology (NTNU), Norway

August 14, 2023

Motivation - The Holy Grail of Cryptocurrency

*Source: https://jimmysong.medium.com/

Motivation - :

Question

Can we build a general model to assess the security of privacy-preserving cryptocurrency systems?

Motivation - :

Question

Can we build a general model to assess the security of privacy-preserving cryptocurrency systems?

Answer

Maybe?

Motivation - Contribution

- We present a general model and security definitions for the privacy-preserving blockchain-based bank.

Motivation - Contribution

- We present a general model and security definitions for the privacy-preserving blockchain-based bank.
- We prove that two privacy-related security definitions in the literature, *Transaction indistinguishability* and *Ledger Indistinguishability*, are equivalent.

Motivation - Contribution

- We present a general model and security definitions for the privacy-preserving blockchain-based bank.
- We prove that two privacy-related security definitions in the literature, *Transaction indistinguishability* and *Ledger Indistinguishability*, are equivalent.
- We also discuss the relationship among the definitions that are related to the integrity of the protocol, namely, *Balance* and *Overdraft Safety*.

Motivation - Contribution

- We present a general model and security definitions for the privacy-preserving blockchain-based bank.
- We prove that two privacy-related security definitions in the literature, *Transaction indistinguishability* and *Ledger Indistinguishability*, are equivalent.
- We also discuss the relationship among the definitions that are related to the integrity of the protocol, namely, *Balance* and *Overdraft Safety*.
- We further analyse the security properties of anonymous cryptocurrency system Monero.

Introduction - Privacy-preserving Blockchain-based Bank

[1] Gjøsteen, Kristian, Mayank Raikwar, and Shuang Wu. "PriBank: confidential blockchain scaling using short commit-and-proof NIZK argument." In Cryptographers' Track at the RSA Conference, pp. 589-619. Cham: Springer International Publishing, 2022.

Introduction - Privacy-preserving Blockchain-based Bank

- PriBank [1]

[1] Gjøsteen, Kristian, Mayank Raikwar, and Shuang Wu. "PriBank: confidential blockchain scaling using short commit-and-proof NIZK argument." In Cryptographers’ Track at the RSA Conference, pp. 589-619. Cham: Springer International Publishing, 2022.

Introduction - Privacy-preserving Blockchain-based Bank

- PriBank [1]
- Privacy-preserving Blockchain-based Bank **PBB** is a tuple of algorithms $(\mathsf{Setup}, \mathsf{KeyGen}, \mathsf{EstablishBank}, \mathsf{NewUser}, \mathsf{Deposit}, \mathsf{Withdraw}, \mathsf{Pay}, \mathsf{Commit}, \mathsf{Contract})$

[1] Gjøsteen, Kristian, Mayank Raikwar, and Shuang Wu. "PriBank: confidential blockchain scaling using short commit-and-proof NIZK argument." In Cryptographers' Track at the RSA Conference, pp. 589-619. Cham: Springer International Publishing, 2022.

Introduction - Security Properties

- *Transaction Indistinguishability* Given two different transactions $\mathrm{tx}_0, \mathrm{tx}_1$ from an adversary $\mathcal{A}$, the ledger L records only one transaction tx_i where $i \in \{0, 1\}$, the adversary $\mathcal{A}$ cannot distinguish which transaction was recorded.
- *Ledger Indistinguishability* Given two different ledgers $\mathrm{L}_0, \mathrm{L}_1$ constructed by an adversary $\mathcal{A}$ using queries to two privacy-preserving system oracles, the adversary $\mathcal{A}$ cannot distinguish between L_0 and L_1.
- *Overdraft Safety* Given an adversary $\mathcal{A}$, an honest user can always spend (or withdraw) the funds that he rightfully owns.
- *Balance* No bounded adversary $\mathcal{A}$ can control more money than he minted or received.

Security Properties - Privacy

- Privacy of balance
- Privacy of identities
- Privacy of transaction amount

Security Properties - Privacy

Ledger Indistinguishability

Given two PBB scheme oracles O_0^{PBB} and O_1^{PBB}, and two ledgers L_0 and L_1 constructed by a bounded adversary $\mathcal{A}$ using public consistent blockchain-bank queries to the two oracles, ledger indistinguishability implies that the adversary $\mathcal{A}$ cannot distinguish between L_0 and L_1.

Security Properties - Privacy

Ledger Indistinguishability

Given two PBB scheme oracles O_0^{PBB} and O_1^{PBB}, and two ledgers L_0 and L_1 constructed by a bounded adversary $\mathcal{A}$ using public consistent blockchain-bank queries to the two oracles, ledger indistinguishability implies that the adversary $\mathcal{A}$ cannot distinguish between L_0 and L_1.

- Ledger indistinguishability is defined by an experiment L-IND.

Security Properties - Privacy

Ledger Indistinguishability Experiment L-IND

A challenger $\mathcal{C}$ samples a random bit b and initialises two ledgers L_0 and L_1. Throughout, the challenger $\mathcal{C}$ allows adversary $\mathcal{A}$ to issue queries to each ledger. At the end $\mathcal{C}$ provides $\mathcal{A}$ with the view of both ledgers, but in randomized order: $\mathsf{L}_{\mathsf{Left}} := \mathsf{L}_b$ and $\mathsf{L}_{\mathsf{Right}} := \mathsf{L}_{1-b}$. The adversary's goal is to distinguish whether the view he sees corresponds to $(\mathsf{L}_{\mathsf{Left}}, \mathsf{L}_{\mathsf{Right}}) = (\mathsf{L}_0, \mathsf{L}_1)$, i.e. $b = 0$, or to $(\mathsf{L}_{\mathsf{Left}}, \mathsf{L}_{\mathsf{Right}}) = (\mathsf{L}_1, \mathsf{L}_0)$, i.e. $b = 1$.

Security Properties - Privacy

Transaction Indistinguishability

Given two different queries of an adversary, only one of the two queries is processed and the ledger is updated with the corresponding transaction. Transaction indistinguishability states that the adversary cannot distinguish which query maps to the recorded transaction.

Security Properties - Privacy

Transaction Indistinguishability

Given two different queries of an adversary, only one of the two queries is processed and the ledger is updated with the corresponding transaction. Transaction indistinguishability states that the adversary cannot distinguish which query maps to the recorded transaction.

- Transaction indistinguishability is defined by an experiment T-IND.

Security Properties - Privacy

Transaction Indistinguishability Experiment T-IND

A challenger $\mathcal{C}$ randomly chooses $b \leftarrow \{0,1\}$. Adversary $\mathcal{A}$ is allowed to make multiple challenge queries. For each challenge query $\mathsf{Q} = \mathsf{Challenge}(\mathsf{Q}_0, \mathsf{Q}_1)$ sent by the adversary $\mathcal{A}$, these two queries $\mathsf{Q}_0, \mathsf{Q}_1$ leak same information and the experiment only performs Q_b. At the end of the challenge phase, the adversary sends commit query $\mathsf{Q} = \mathsf{Commit}$ and receives the output trans_b. Finally, the adversary outputs a bit $b' \in \{0,1\}$, and wins the game if $b' = b$.

Security Properties - T-IND implies L-IND

Theorem

***1)** If there exists an adversary $\mathcal{A}_{\mathsf{T\text{-}IND}}$ that can win the* T-IND *experiment with advantage $\mathsf{Adv}^{\mathsf{PBB}}_{\mathcal{A}_{\mathsf{T\text{-}IND}}}$ within runtime t, then there must be an adversary $\mathcal{B}_{\mathsf{L\text{-}IND}}$ that can win the* L-IND *experiment with advantage $\mathsf{Adv}^{\mathsf{PBB}}_{\mathcal{B}_{\mathsf{L\text{-}IND}}}$ within runtime essentially t such that*

$$\mathsf{Adv}^{\mathsf{PBB}}_{\mathcal{A}_{\mathsf{T\text{-}IND}}} \leq 2\mathsf{Adv}^{\mathsf{PBB}}_{\mathcal{B}_{\mathsf{L\text{-}IND}}}.$$

Security Properties - L-IND implies T-IND

Theorem

2) *If there exists an adversary* $\mathcal{B}_{\text{L-IND}}$ *that can win the* L-IND *game with advantage* $\text{Adv}^{\text{PBB}}_{\mathcal{B}_{\text{L-IND}}}$ *within runtime* t*, then there exists an adversary* $\mathcal{A}_{\text{T-IND}_{l_c}}$ *that can win the* T-IND_{l_c} *game in terms of* l_c *challenge queries, with advantage* $\text{Adv}^{\text{PBB}}_{\mathcal{A}_{\text{T-IND}_{l_c}}}$ *and within runtime essentially* t *such that*

$$\text{Adv}^{\text{PBB}}_{\mathcal{B}_{\text{L-IND}}} \leq 2\text{Adv}^{\text{PBB}}_{\mathcal{A}_{\text{T-IND}_{l_c}}}.$$

Security Properties - Security

- Overdraft Safety
- Balance

Security Properties - Overdraft Safety

- It specifies that an honest user can always withdraw all the balance that he owns in the blockchain.

Security Properties - Overdraft Safety

- It specifies that an honest user can always withdraw all the balance that he owns in the blockchain.
- In UTXO based model, it means that an honest user can always spend his unspent outputs inductively.

Security Properties - Overdraft Safety

- It specifies that an honest user can always withdraw all the balance that he owns in the blockchain.
- In UTXO based model, it means that an honest user can always spend his unspent outputs inductively.
- In an account-based model, it means that an honest user can withdraw all the balance from his account (using smart contract).

Security Properties - Overdraft Safety

- It specifies that an honest user can always withdraw all the balance that he owns in the blockchain.
- In UTXO based model, it means that an honest user can always spend his unspent outputs inductively.
- In an account-based model, it means that an honest user can withdraw all the balance from his account (using smart contract).
- It prohibits an adversary to withdraw more than what it has since otherwise there must be an honest user who cannot withdraw all of his balance.

Security Properties - Balance

- It states that the total balance of honest users should not exceed the total balance of the system.

Security Properties - Balance

- It states that the total balance of honest users should not exceed the total balance of the system.
- No bounded adversary $\mathcal{A}$ can own more money than what he minted or received via payments from others.

Conclusion - :

- We presented a unified model to prove the security of privacy-preserving cryptocurrency systems.

Conclusion - :

- We presented a unified model to prove the security of privacy-preserving cryptocurrency systems.
- We presented the security-related properties of these systems.

Conclusion - :

- We presented a unified model to prove the security of privacy-preserving cryptocurrency systems.
- We presented the security-related properties of these systems.
- We analysed the security of Monero system.

Conclusion - Way Forward

- Analyse the security of other privacy-preserving cryptocurrency systems.

Conclusion - Way Forward

- Analyse the security of other privacy-preserving cryptocurrency systems.
- Check the maturity and robustness of the presented model.

Conclusion - Way Forward

- Analyse the security of other privacy-preserving cryptocurrency systems.
- Check the maturity and robustness of the presented model.
- Study and define the security properties such as transaction non-malleability, transaction unlinkability and transaction untraceablility for the presented model.

Thank you for your attention

UNIVERSITY
OF OSLO