Cost-Efficient Anonymous Authentication Scheme based on Set-Membership Zero-Knowledge Proof

Christopher Wiraatmaja and Shoji Kasahara

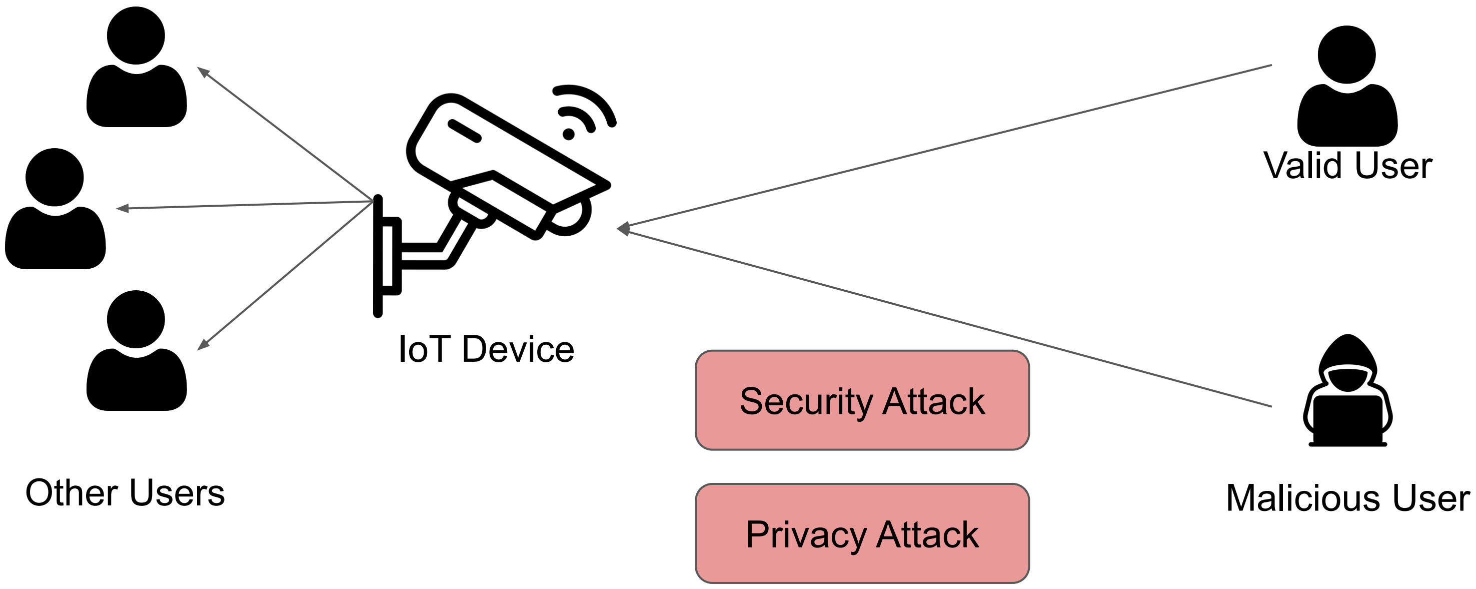
Nara Institute of Science and Technology, Japan

Table of Contents

- Introduction
- Preliminaries
- Proposed Method
- Implementation
- Experiment
- Conclusion

Introduction

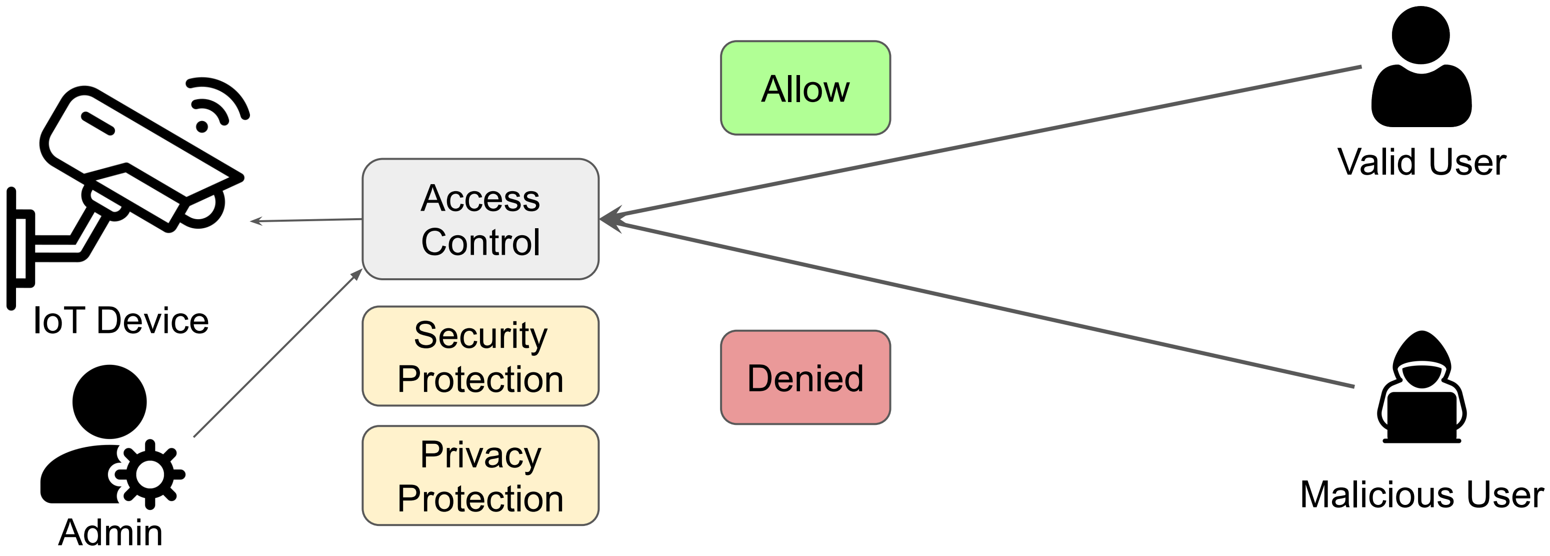
Risk of IoT Devices



IoT Devices is a target to Security and Privacy Attacks
due to their proximity to the Users

User, CCTV, Hacker icons created by Freepik - Flaticon

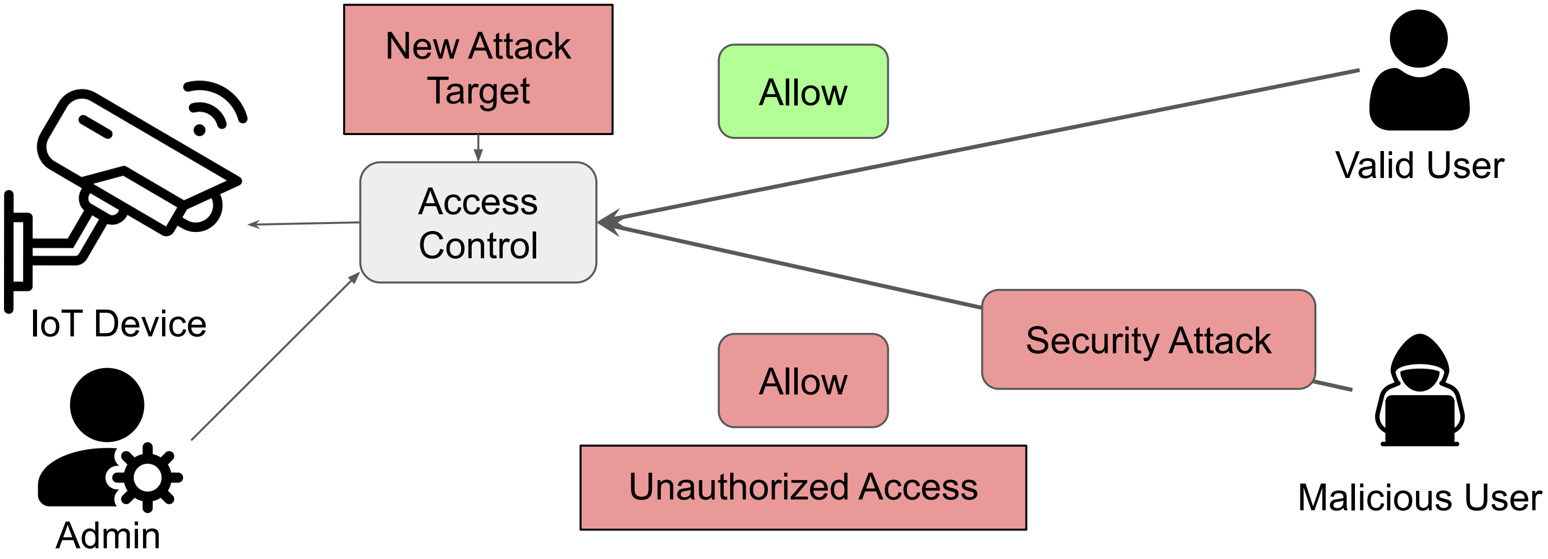
IoT Devices Protection Answer



Administrator employs an Access Control to prevents Security and Privacy Attack

Setting icons created by Tanah Basah - Flaticon

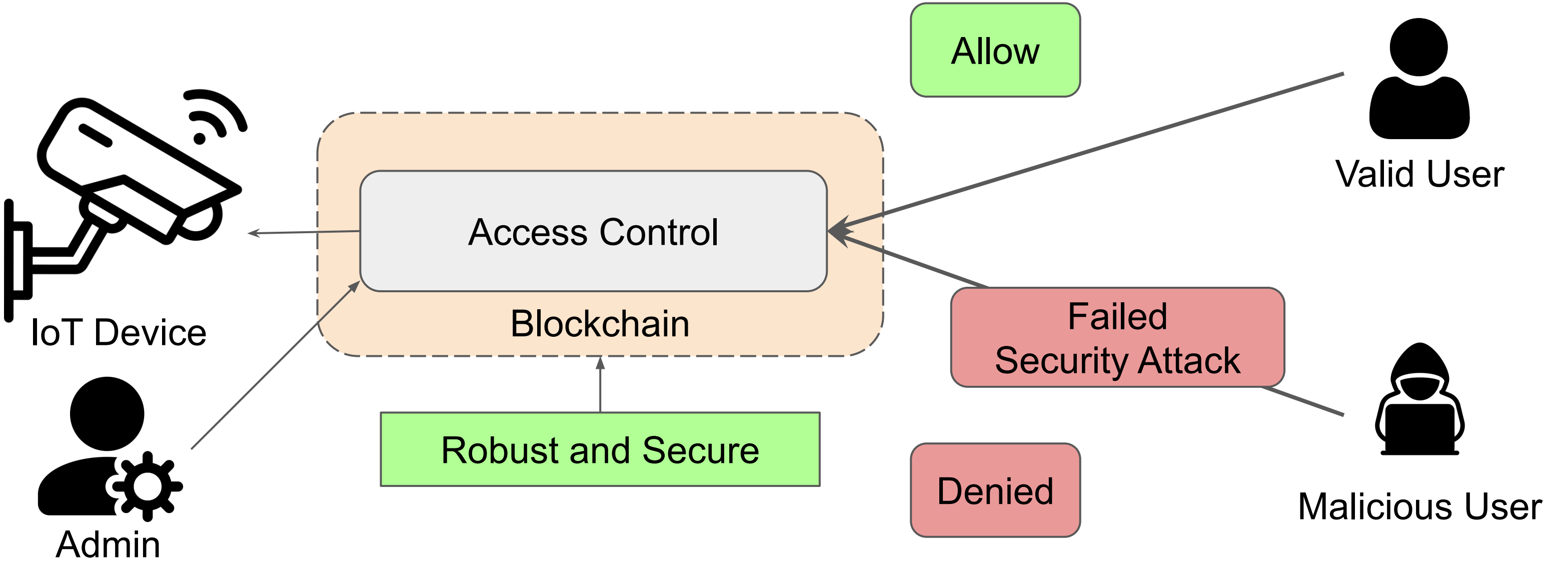
Security Issue on Access Control



Security Attacks on Access Control leads to Unauthorized Access

Setting icons created by Tanah Basah - Flaticon

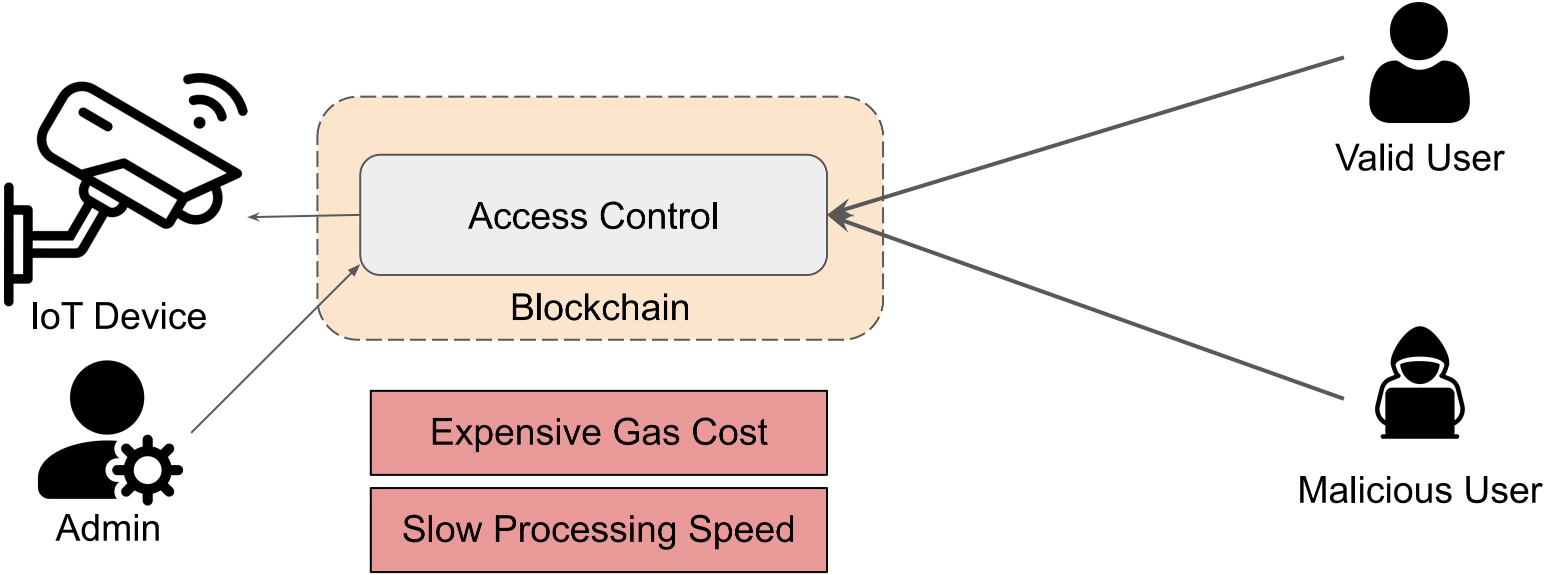
Security Issue Solution



Previous works [Yut+19,Mae+19] leverage Blockchain properties
to develop a Blockchain-Based Access Control

[Yut+19] M. Yutaka, Y. Zhang, M. Sasabe, and S. Kasahara, “Using ethereum blockchain for distributed attribute-based access control in the internet of things,” in 2019 IEEE GLOBECOM, 2019, pp. 1–6.
[Mae+19] D. Di Francesco Maesa, P. Mori, and L. Ricci, “A blockchain based approach for the definition of auditable access control systems,” Computers & Security, vol. 84, pp. 93–119, 2019.

Scalability Issue on Blockchain-Based Access Control



Access Control

Blockchain

IoT Device

Admin

Valid User

Malicious User

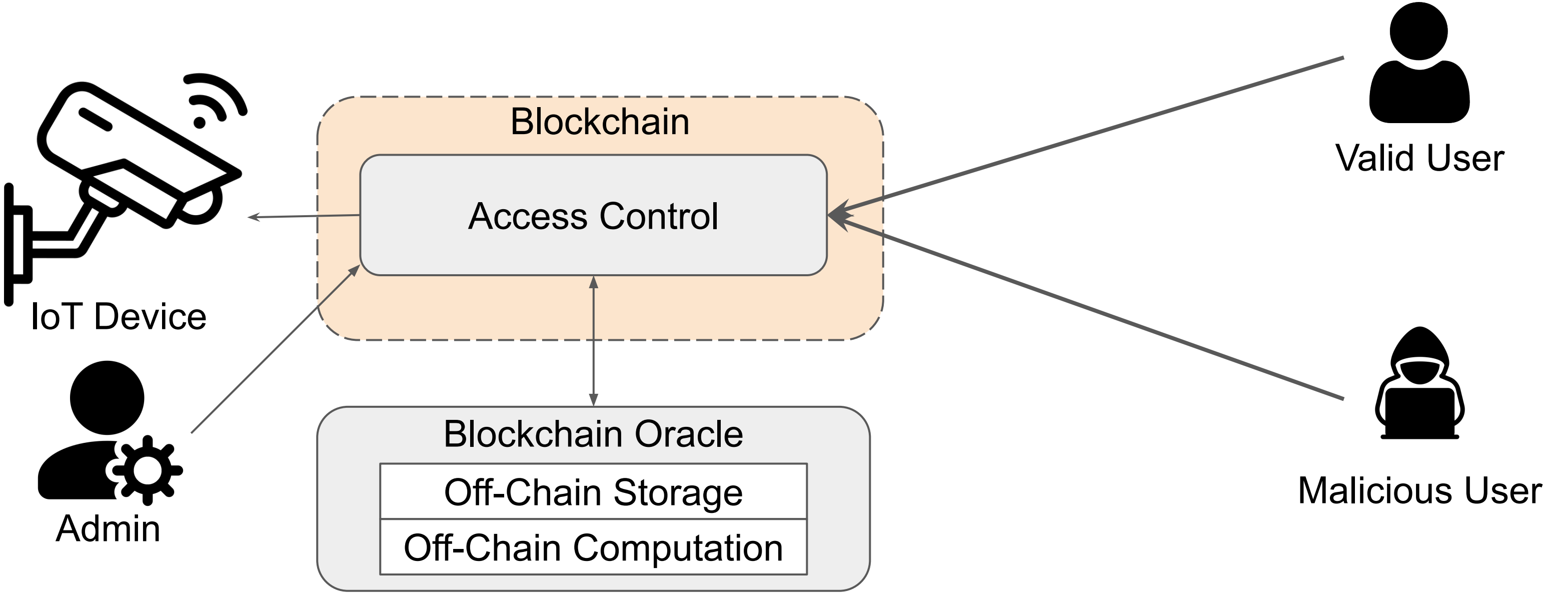
Expensive Gas Cost

Slow Processing Speed

Scalability is an important metric on BBAC due to the Blockchain limitations

[Yut+19] M. Yutaka, Y. Zhang, M. Sasabe, and S. Kasahara, “Using ethereum blockchain for distributed attribute-based access control in the internet of things,” in 2019 IEEE GLOBECOM, 2019, pp. 1–6.
[Mae+19] D. Di Francesco Maesa, P. Mori, and L. Ricci, “A blockchain based approach for the definition of auditable access control systems,” Computers & Security, vol. 84, pp. 93–119, 2019.

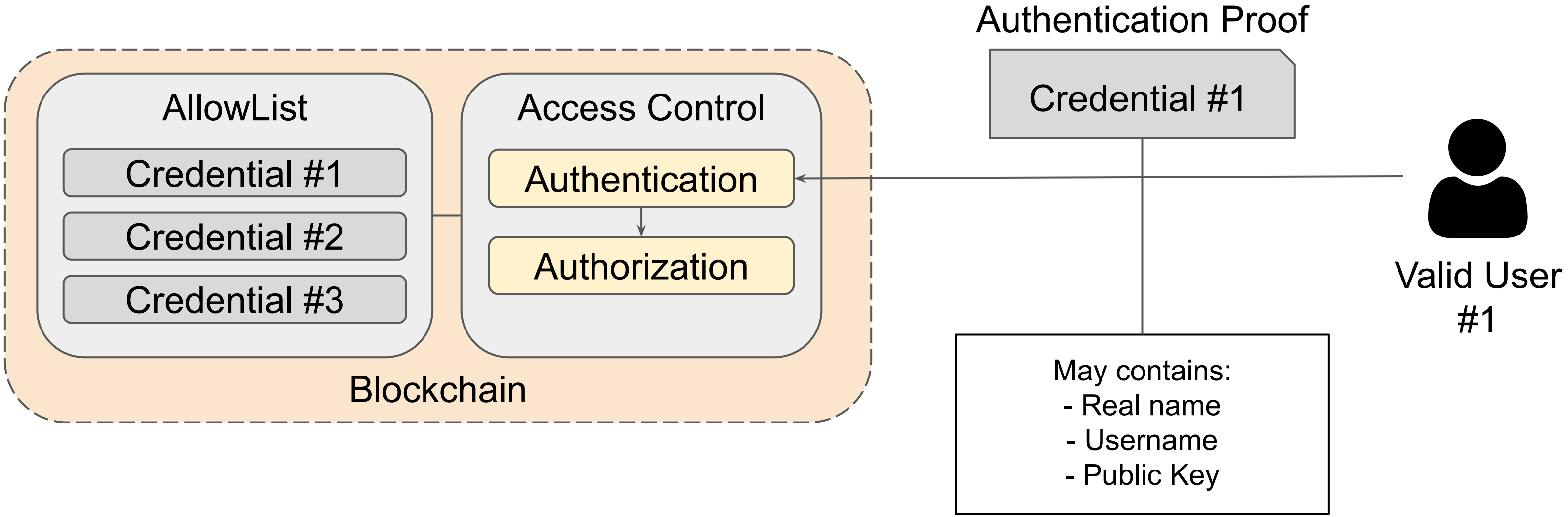
Scalability Issue Solution



Previous Work [Wir+21] addressed the Scalability Issues
by improving the Cost-Efficiency of BBAC

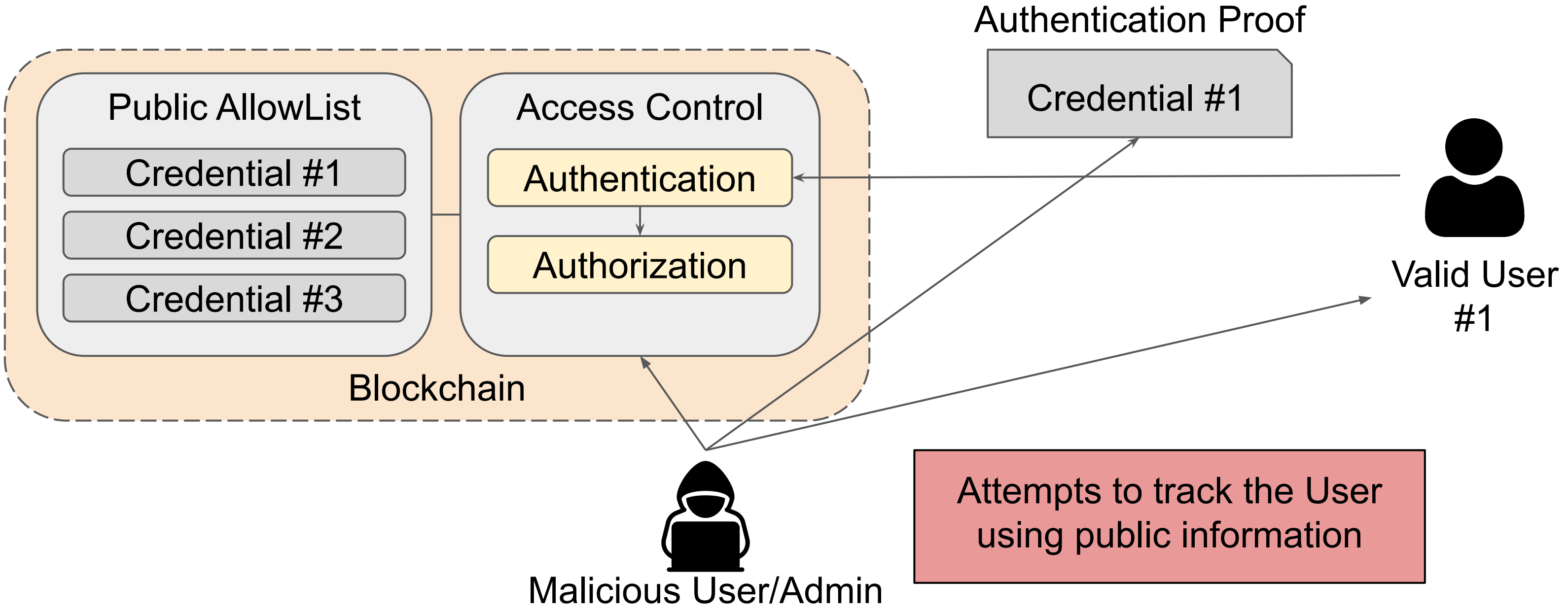
[Wir+21] C. Wiraatmaja, Y. Zhang, M. Sasabe and S. Kasahara, "Cost-Efficient Blockchain-Based Access Control for the Internet of Things," 2021 IEEE Global Communications Conference (GLOBECOM), Madrid, Spain, 2021

New Issue on Blockchain-Based Authentication



Previous BBAC Authentication Schemes require Users to show their Credential to create an Authentication Proof

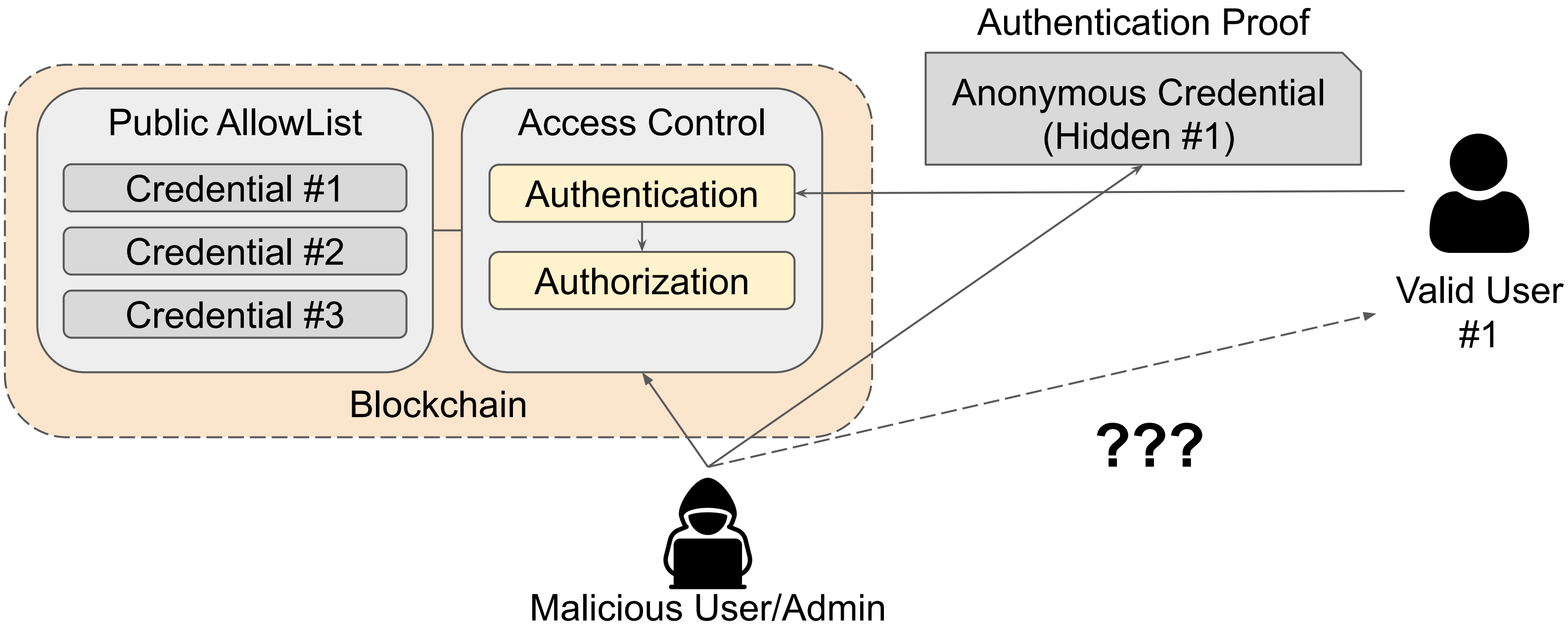
Privacy Issue on Blockchain-Based Access Control



Attempts to track the User using public information

Previous works didn't consider potential Privacy Attacks from Malicious Actor

Potential Solution for Privacy Issue



Hiding User Credential in the Authentication Proof prevents Privacy Attacks from Malicious Actor

Research Goal

We aim to:

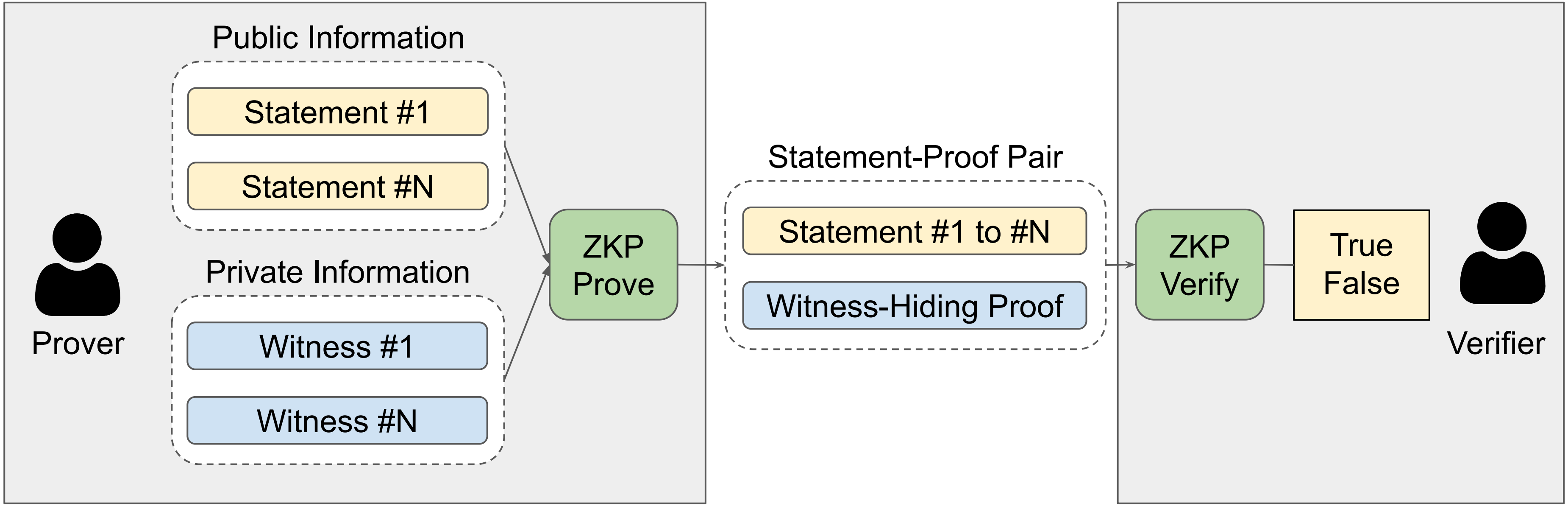
- Address the Privacy Issue on BBAC while paying attention to its Security and Performance Issue

Our steps to reach our goal:

- Develop a Scalable Blockchain-Based Anonymous Authentication Scheme
  - The Authentication Proof needs to hide the User Credential from Privacy Attacks
- Prevent potential Security Attacks in our scheme while preventing Privacy Attacks

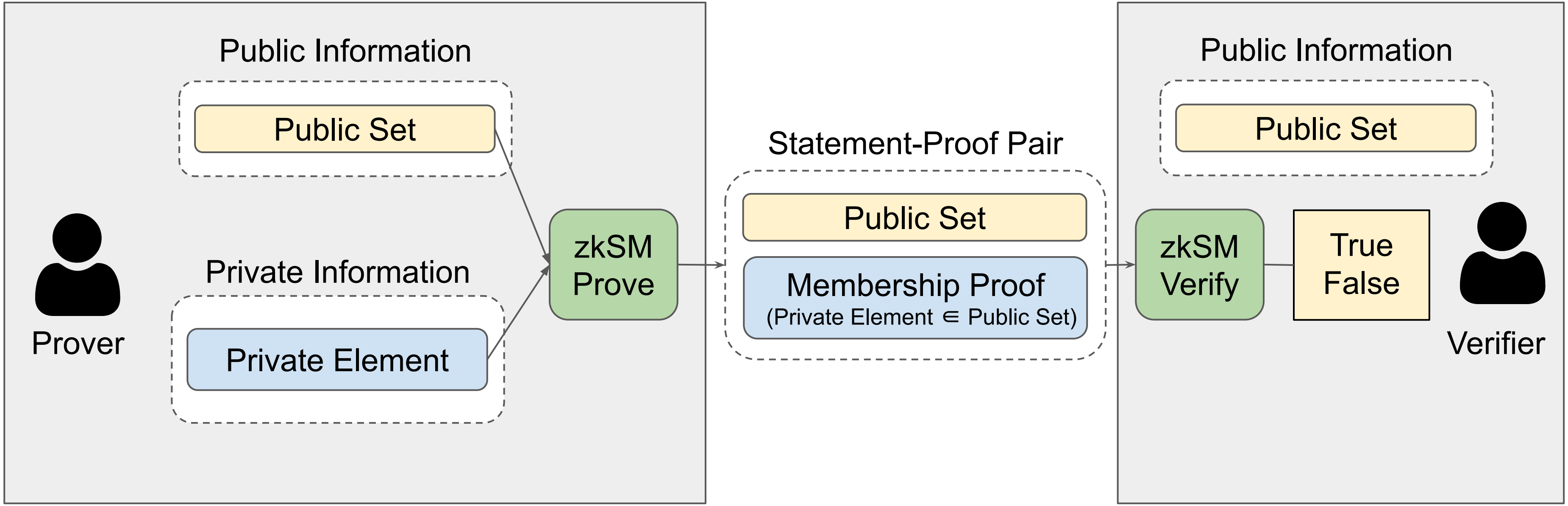
Preliminaries

Zero Knowledge Proof



Zero-Knowledge Proof allows a Prover to convince a Verifier about some Statements is True while hiding the supporting Witnesses

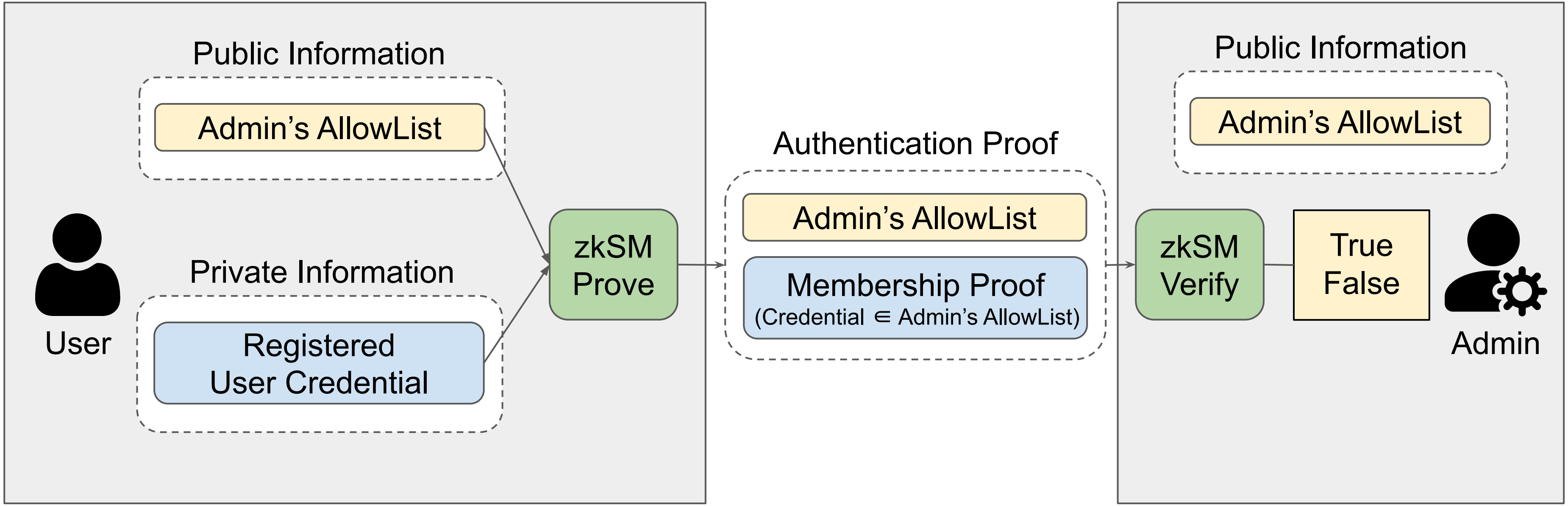
Zero Knowledge Set-Membership Proof



zk-Set-Membership Proof guarantees an Element is inside a Set while hiding that element

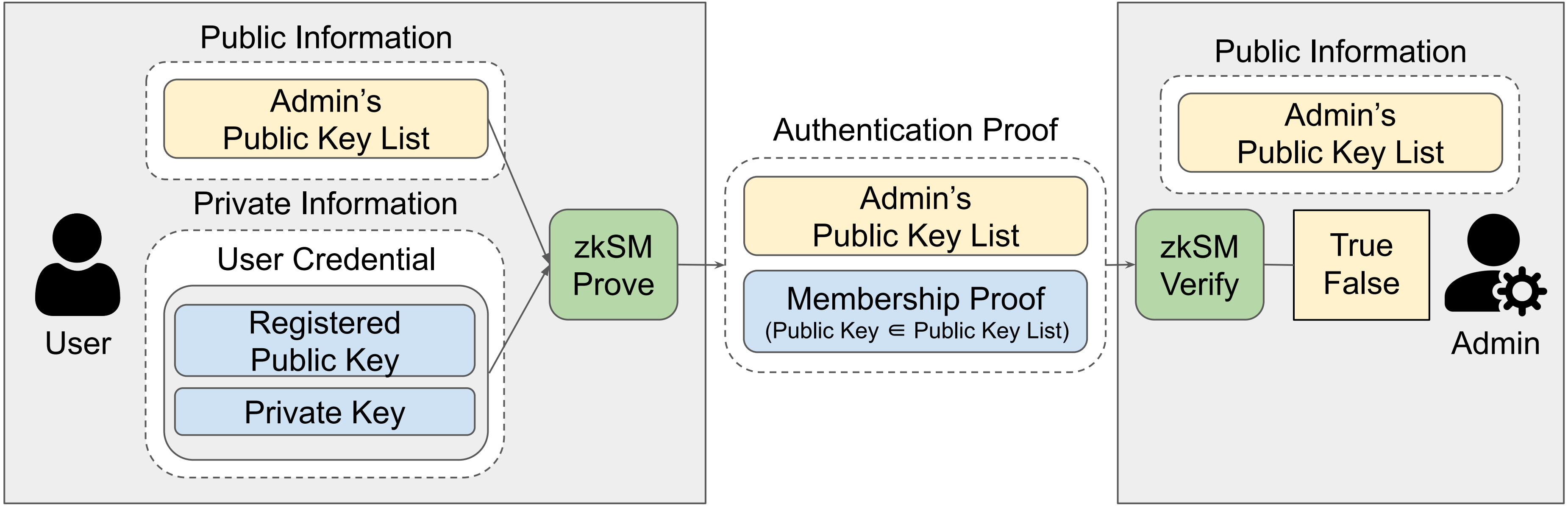
Proposed Method

Anonymous Authentication Design



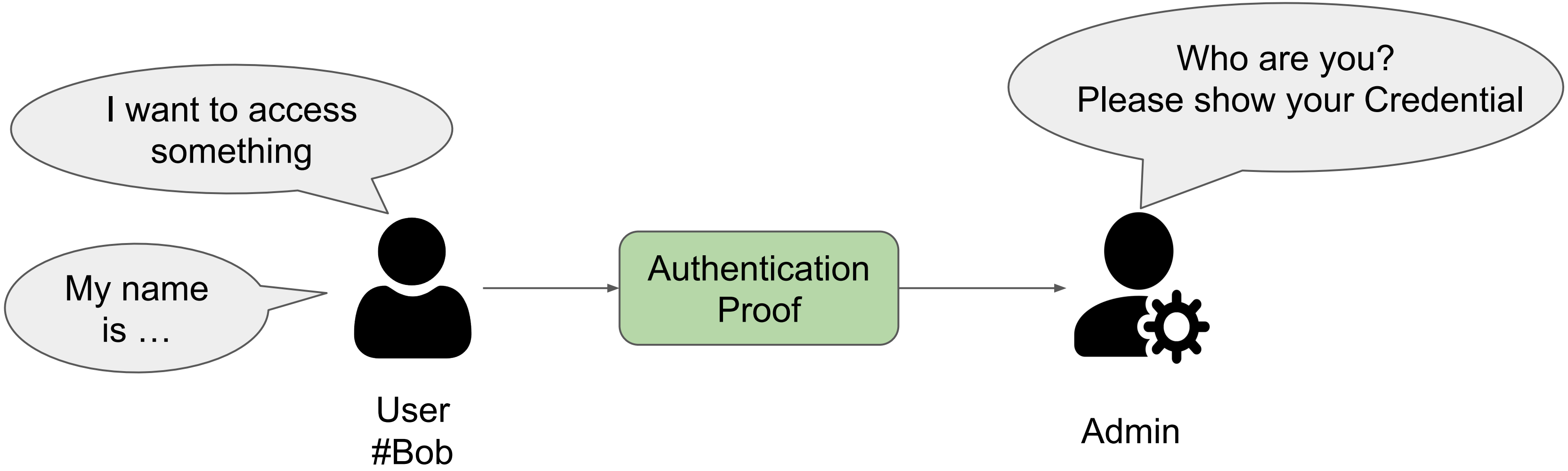
The User generates an Authentication Proof which hides their Credential using zk-Set-Membership Proof

Set-Membership-based Authentication Scheme



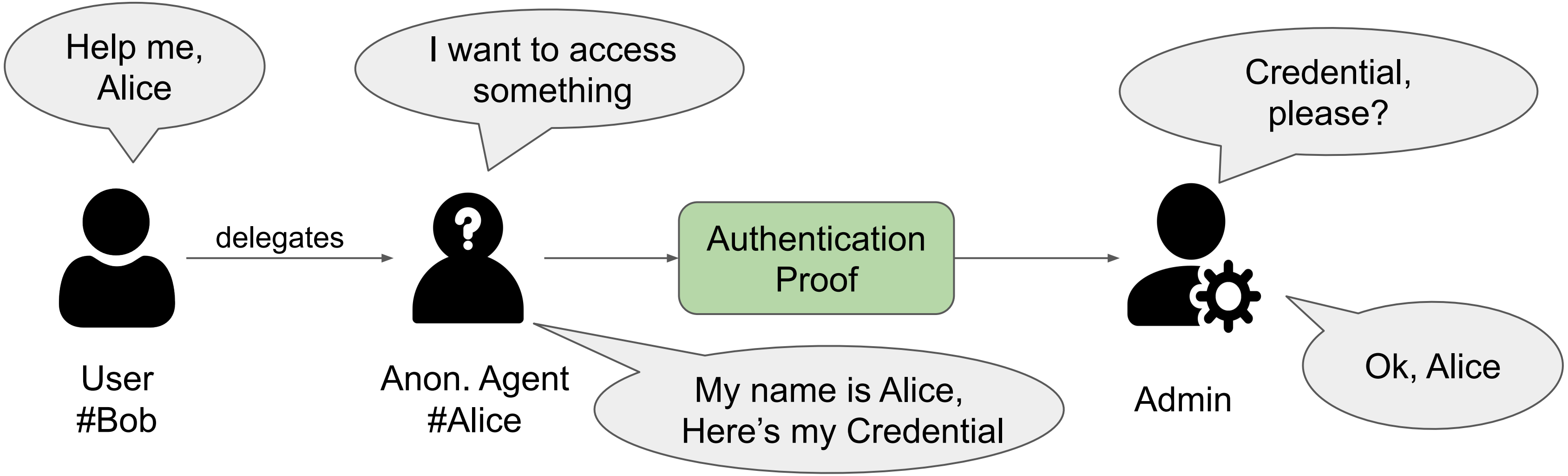
The User Credential is represented as Public-Private Key Pair to prevent unauthorized access

Difficulty in Communication


I want to access something
My name is …
User #Bob
Authentication Proof
Who are you? Please show your Credential
Admin

The User can’t directly communicate with the Administrator without revealing their Credential

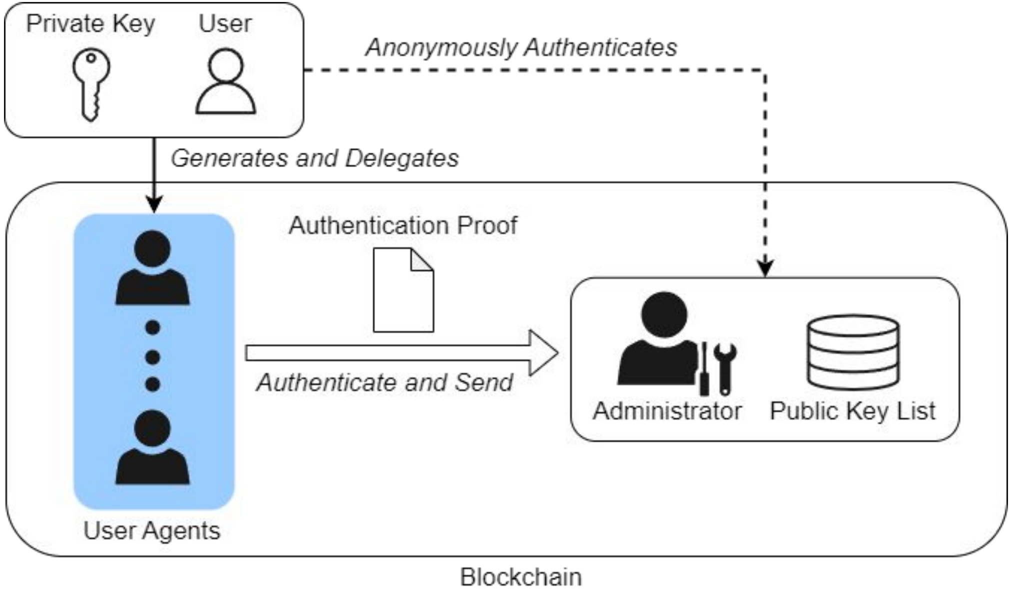
Anonymous Agent Delegation



The User delegates another entity called an Agent
to send the Authentication Proof to the Administrator

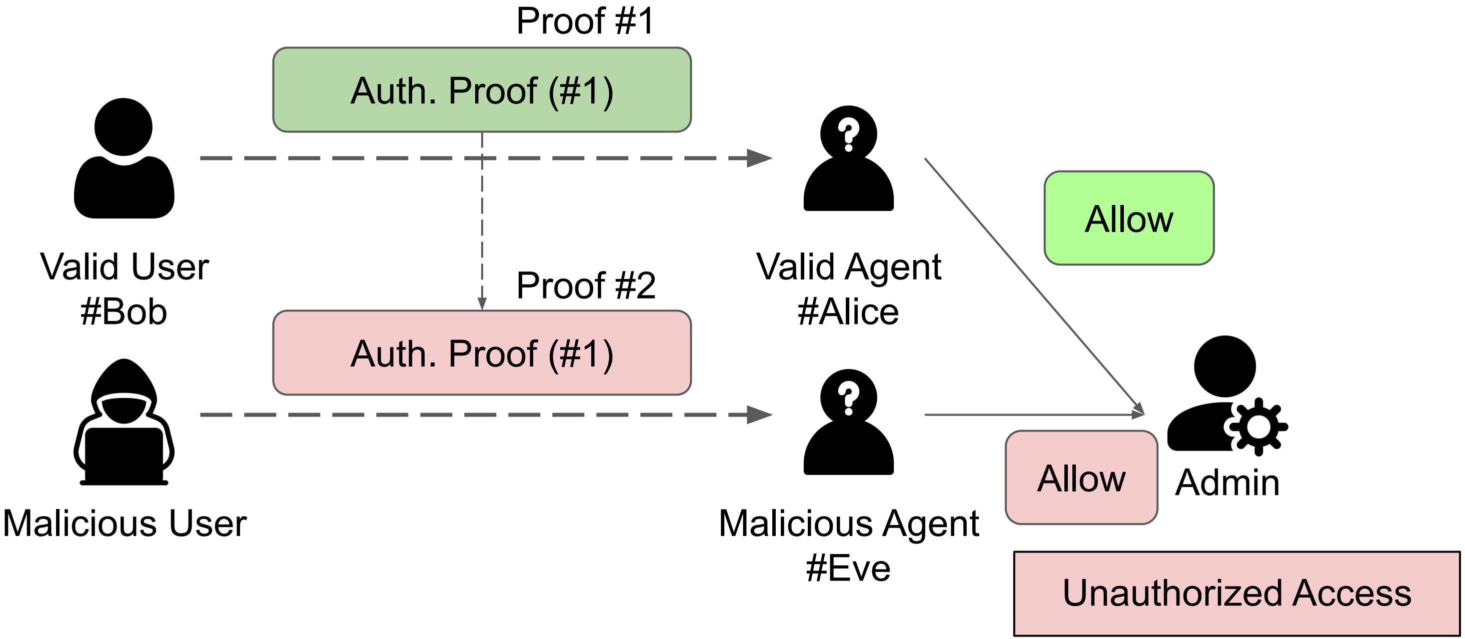
Anonymous icons created by Slidicon - Flaticon

Proposed Authentication Schematic



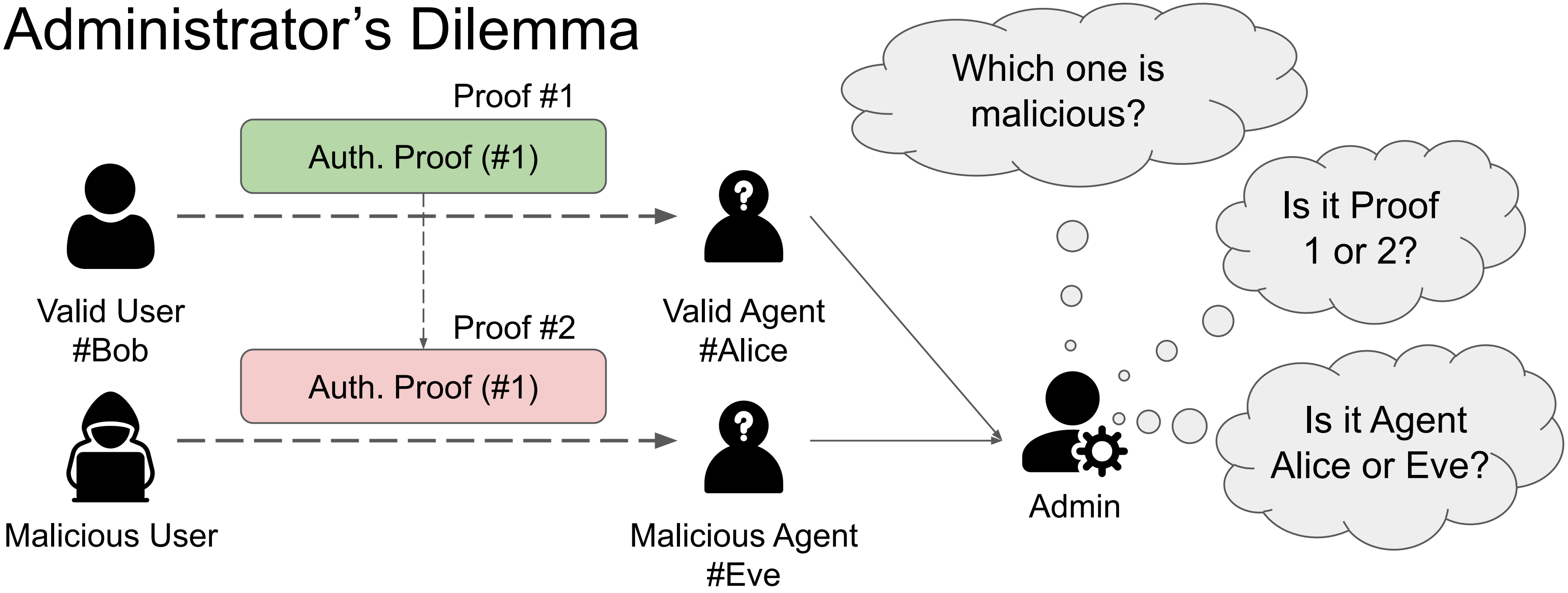
User always delegates a new Agent
to prevent Administrator tracking the Agent’s Credential

Replay Attack Problem



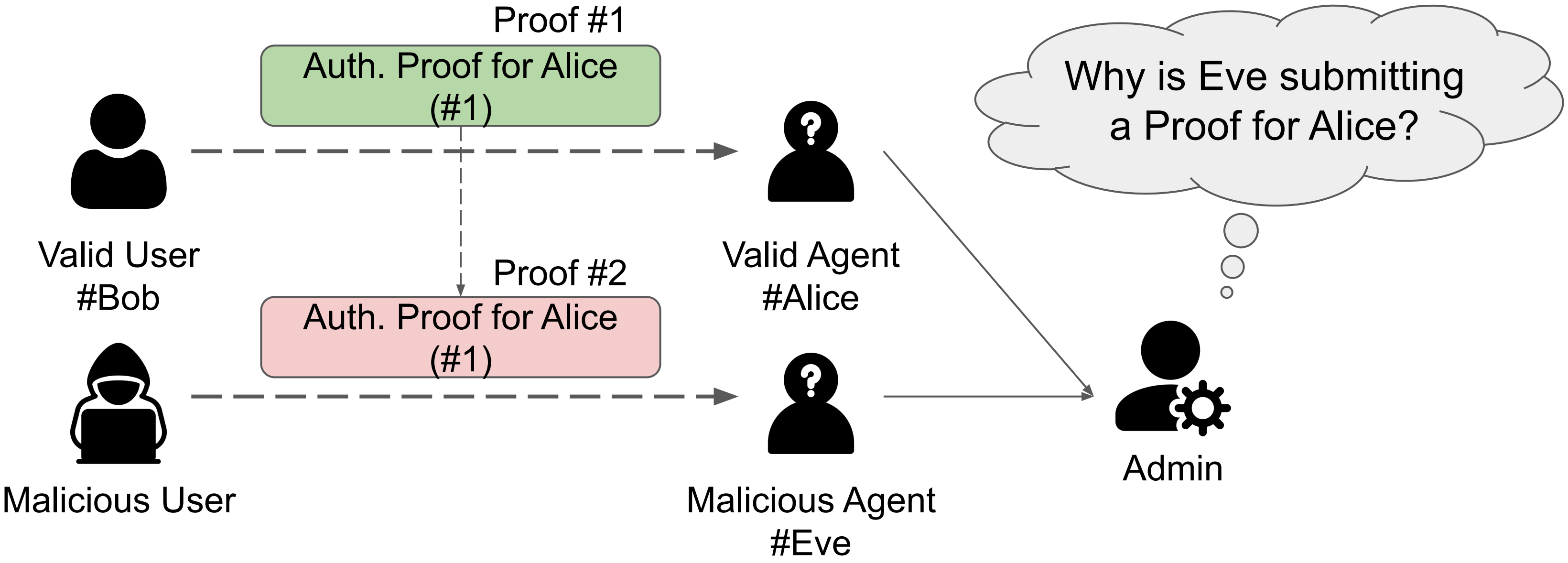
Replayed Attack occurs when another user utilized existing proof to bypass security measure

Administrator’s Dilemma



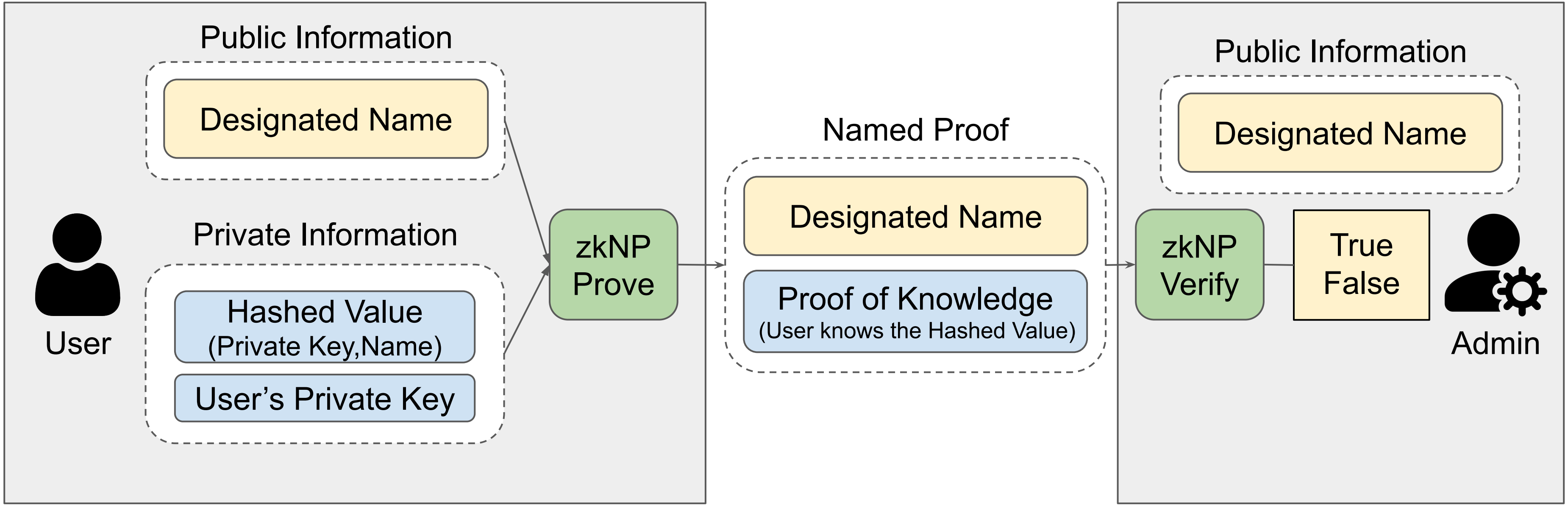
Replay Attack can be prevented by either distinguishing the Replayed Proofs or the Malicious Agents

Spotting Malicious Agent


Proof #1
Auth. Proof for Alice (#1)
Valid User #Bob
Proof #2
Auth. Proof for Alice (#1)
Malicious User
Valid Agent #Alice
Malicious Agent #Eve
Why is Eve submitting a Proof for Alice?
Admin

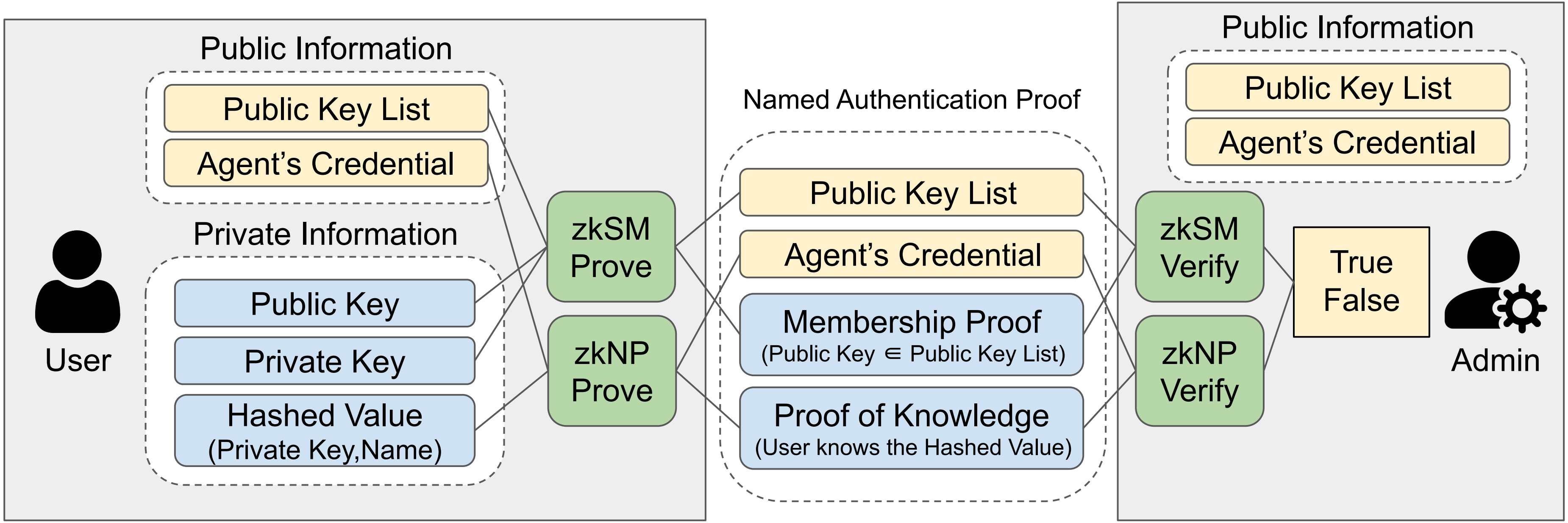
Putting a name or the Agent’s Credential in the Authentication Proof helps the Admin to distinguish Malicious Agents

Zero-Knowledge Named Proof



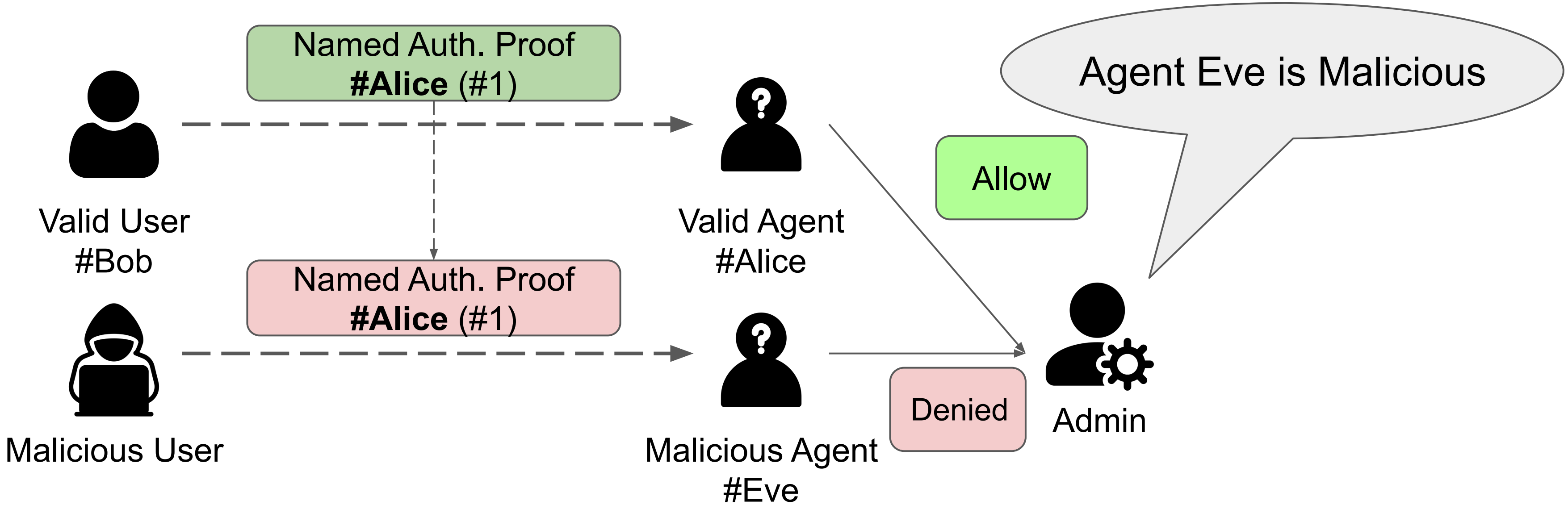
zkNamedProof works by engraving an immutable name which can be verified by the Administrator

Named Authentication Proof



The User generates a Named Authentication Proof
by composing zkSet-Membership Proof and zkNamedProof

Replay Attack Prevention Scheme



Replay Attack is prevented by comparing the Agent Credential and the Name in the Authentication Proof

Implementation

Implementation - Technology Stack

Technology	Technology
Zero-knowledge Set-Membership Proof	RSA-based set-membership Proof [Ben+21]
SNARK	LegoGroth16 [Ben+21]
SNARK Library	Arkworks-rs (Rust) [ark]
Hash Function	Blake2S
Curve	BLS12-381
Blockchain	Ethereum

[Ben+21] Benarroch, D., Campanelli, M., Fiore, D., Gurkan, K., Kolonelos, D. (2021). Zero-Knowledge Proofs for Set Membership: Efficient, Succinct, Modular. In: Borisov, N., Diaz, C. (eds) Financial Cryptography and Data Security. FC 2021.
[ark] arkworks contributors, “arkworks zksnark ecosystem,” 2022. [Online]. Available: https://arkworks.rs

Experiment

Similar Works Comparison

Authentication Scheme	Replay Attack Prevention Technique	
	Distinguishing	Technique
AnonParking [Ho+21]	Replayed Proof	Rotating Nonce
HashAuth	Replayed Proof	Collision Resistant Hash
PseudoAuth [Luong+22]	Malicious Agent	Pseudonym
NPAuth (Ours)	Malicious Agent	Named Proof

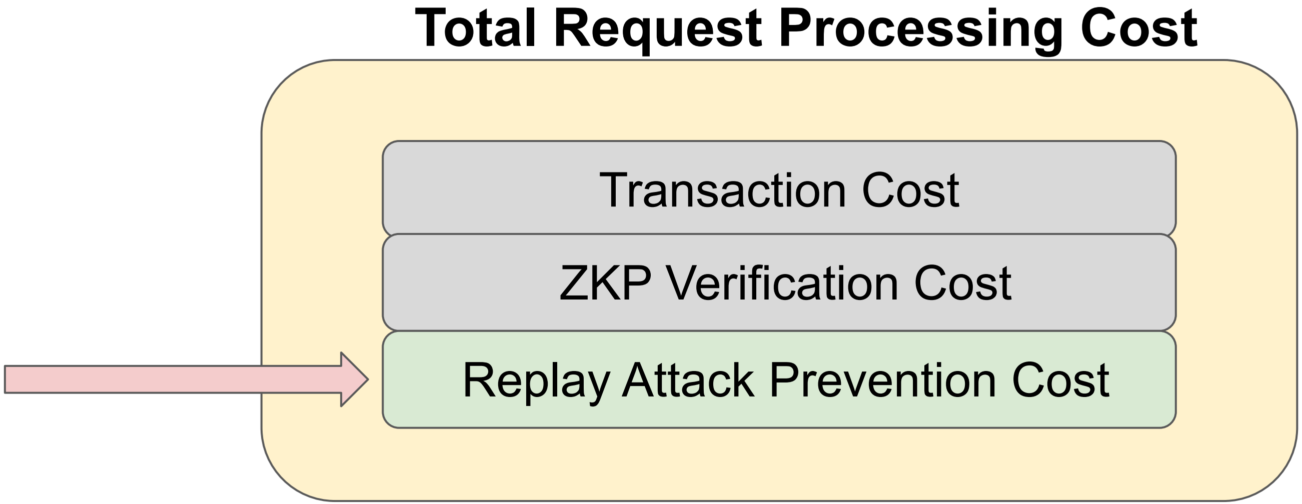
[Ho+21] J. C. L. Ho and C. Lin, “An anonymous on-street parking authentication scheme via zero-knowledge set membership proof,” CoRR, vol. abs/2108.03629, 2021.
[Luong+22] D. A. Luong and J. H. Park, “Privacy-preserving blockchain-based healthcare system for iot devices using zk-snark,” IEEE Access, vol. 10, pp. 55 739–55 752, 2022.

Blockchain Implementation Scalability

To investigate the scalability of our work, we compared the similar works in the following performance:

- Cost-Performance
    - How much gas is used on access request?
- Processing Performance
    - How many request can be processed at a time?

Cost Performance Calculation



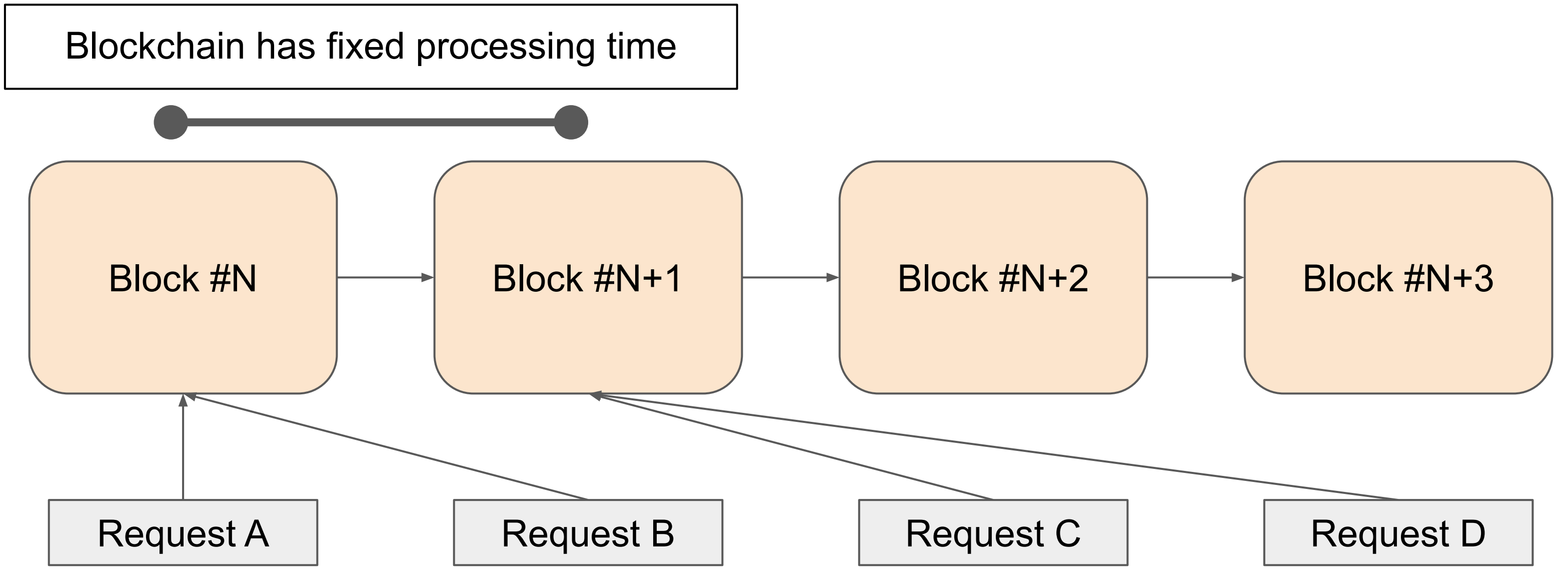
We only calculate the replay attack prevention gas cost in our experiment

Replay Attack Prevention Gas Cost Comparison

Process Detail	***AnonParking***	***HashAuth***	***PseudoAuth***	***NPAuth (Ours)***
Write Operation	22,900	20,000	-	-
Read Operation	4,200	2,100	2,100	-
Hash Calculation	472	960	-	-
Minor Operation	494	442	185	395
Total Gas Cost	28,066	23,502	2,285	**395**

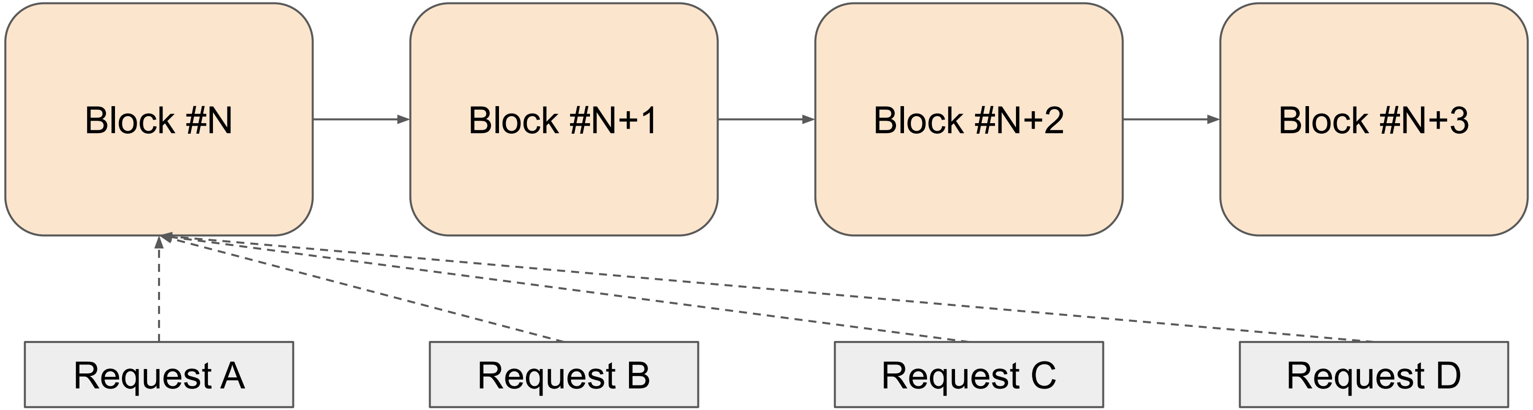
Our Authentication Scheme is significantly cheaper than the other schemes

Processing Performance on Blockchain



Capability of processing multiple access request implies high performance on Blockchain

Racing Condition Occurrence



Racing Condition prevents multiple processing access requests on the same block

Racing Condition Probability Comparison

Authentication Scheme	**Racing Condition Probability**	**Processing Limit per Block**
AnonParking	High	1 request
HashAuth	Negligible	High
PseudoAuth	-	High
NPAuth (Ours)	-	High

Our Scheme is capable of processing multiple requests simultaneously

Experiment Summary

To summarize our experiment results, we compare each authentication by each of its characteristic.

Characteristic	***AnonParking***	***HashAuth***	***PseudoAuth***	***NPAuth (Ours)***
Fully Anonymous	✔	✔	╳	✔
Cheap Gas Cost	╳	╳	╳	✔
High Throughput	╳	✔	✔	✔

Conclusion

Conclusion

To conclude our work, we proposed:

- Replay Attack Prevention Scheme called zkNamedProof that is robust against privacy attack
- Blockchain-Based Authentication Scheme, which are:
  - Fully Anonymous
  - Cost-efficient
  - High-throughput

We aim to address these problems in the future:

- Anonymous Registration Process
- ZKP Verification Cost on Blockchain

Thank You for Listening

Visit our GitHub Repository

If you have any questions, please let me know