UNIVERSITY OF BIRMINGHAM

Design and Evaluation of Blockchain-based Security Protocols

Rujia Li

PhD Dissertation Defense

June 17, 2022

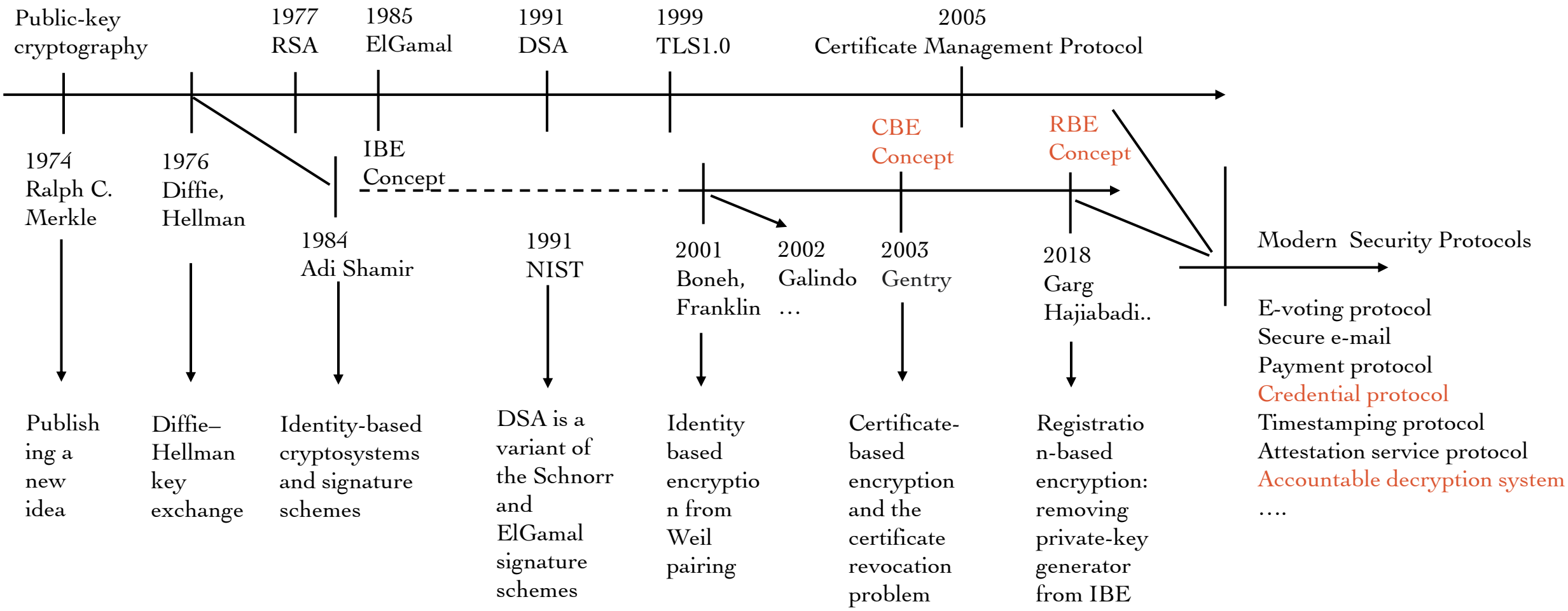
Committee

Prof. Rami Bahsoon(Birmingham)
Prof. Siamak Shahandashti (York)
Prof. Tom Chothia (Birmingham)

Supervisor

Prof. David Galindo (Birmingham)
Prof. Qi Wang (SUSTech)
Prof. Mark Ryan (Birmingham)

Security Protocols

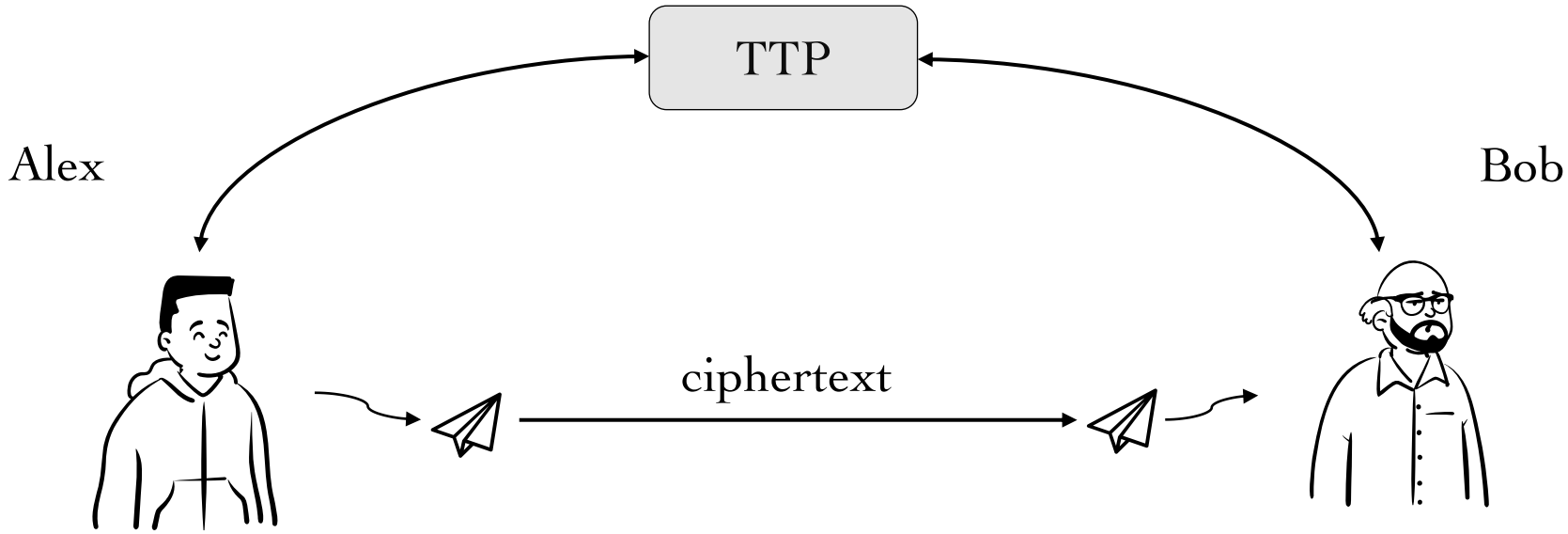


Goals of Security Protocols

- **Authentication**
  provides assurance that a communicating entity is the one that it claims to be.
- **Confidentiality**
  aims to protect data from unauthorized disclosure.
- **Integrity**
  provides assurance that data received are exactly as sent by the sender.
- **Non-repudiation**
  provides protection against denial by one entity involved in a communication of having participated in all or part of the communication.

Katz, Jonathan, and Yehuda Lindell. Introduction to modern cryptography. CRC press, 2020.

Trusted Third Party (TTP)



Without a TTP's assurance, it is difficult for Alex to confirm that Bob's identity is, in fact, the person for whom the information is intended.

Ideal World & Real World

TTP always online,
privacy preserving,
behaves “as it should”.

Ideal World

TTP may be offline,
may be compromised,
may become malicious due to
hidden interests.

Real World

“TTP assumptions cause most of the costs and risks in a security protocol.”

- Nick Szabo, 2001

Thesis Outline

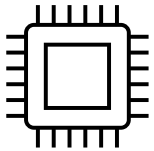
TTP issues in security protocols

Chapter 1 Aims: make cryptographic protocols practical and secure

Smart contract aided TTP

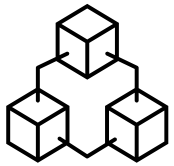
Chapter 3 Introduce a fair TTP

Smart contract & TEE-assisted TTP



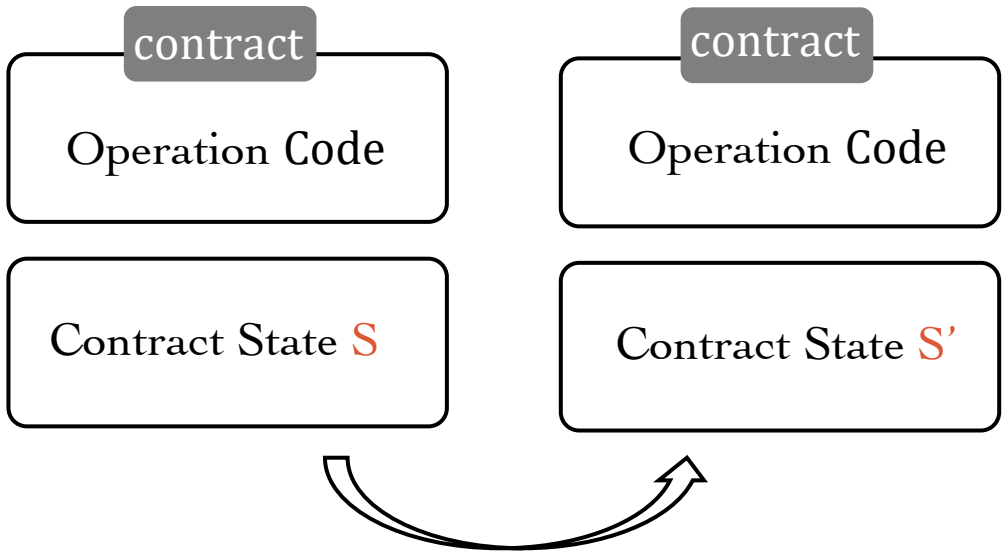
Chapters 4 and 5 Build a privacy-preserving TTP

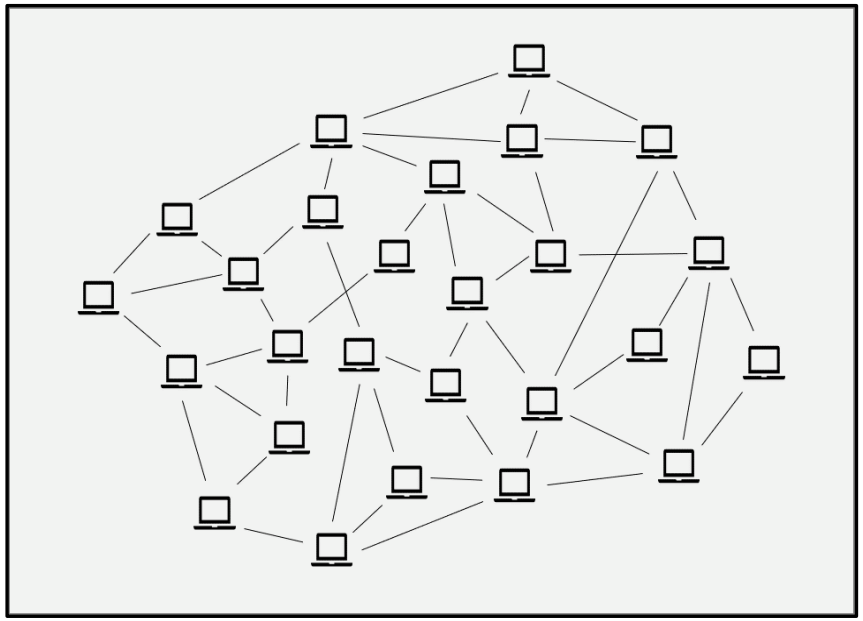
Blockchain system enhancement



Chapter 6 Create better blockchain systems

Smart Contract

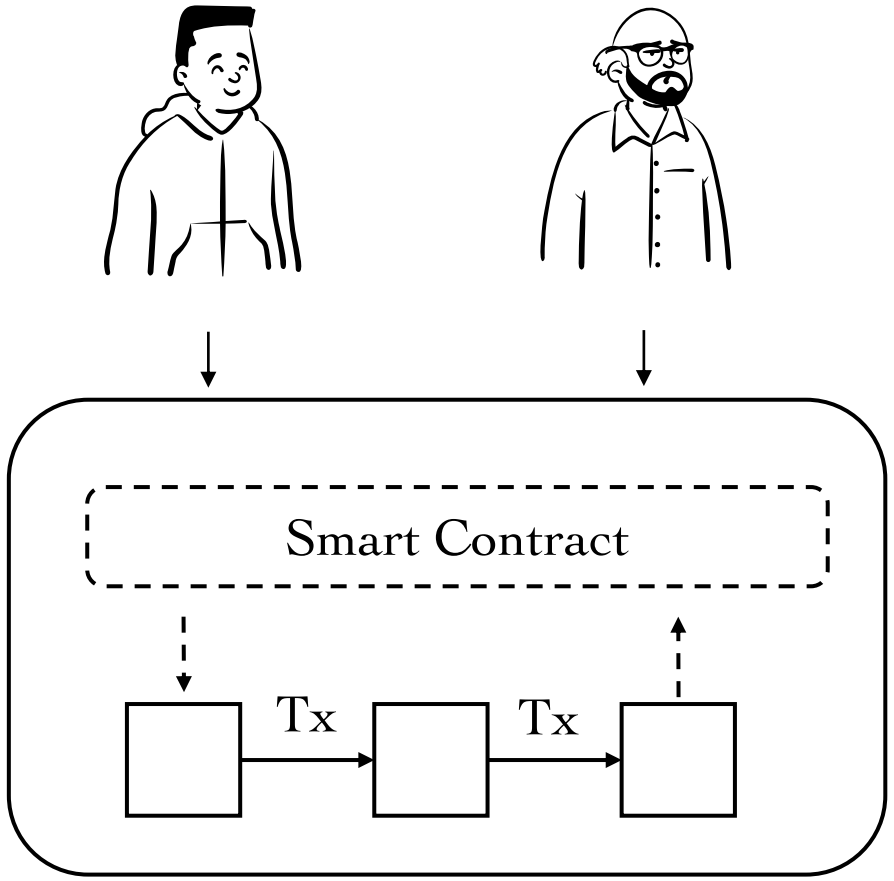




Distributed computing platform

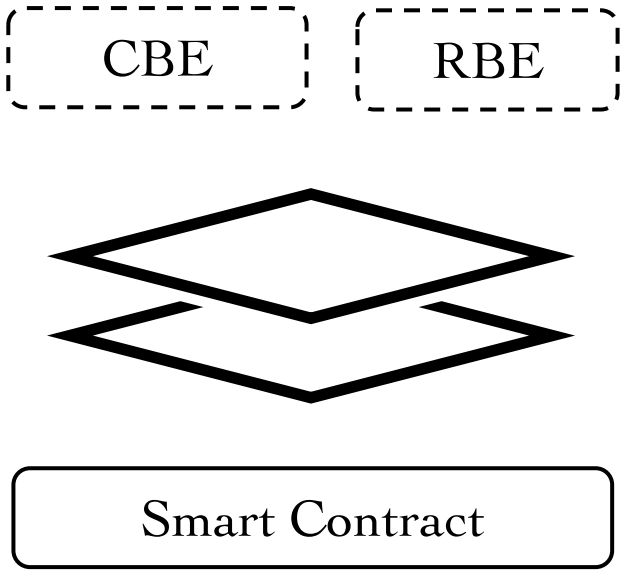
G. Wood. Ethereum: A secure decentralised generalised transaction ledger. Ethereum project yellow paper, 151(2014):1–32, 2014.

TTP-I: Smart Contract-aided TTP



1. Force one entity to do operations based on the transparent logic.
2. Provide protection against denial of one entity's behaviour.
3. Create a single shared view of the world, which supports more efficient settlement.

Research Outcomes

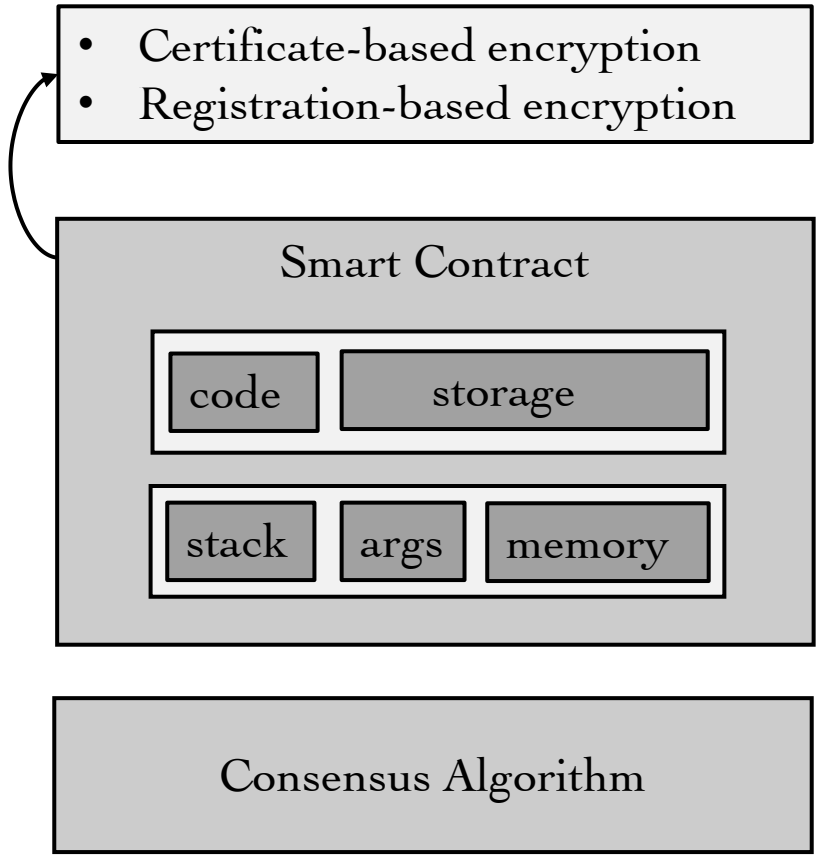


- Qin Wang*, **Rujia Li***, Qi Wang, and David Galindo. "*Poster: Transparent Certificate Revocation for CBE Based on Blockchain*." In Poster Session of 41st IEEE Symposium on Security and Privacy (**S&P20 Poster**). 2020 (*equal contribution).

- **Rujia Li**, Qin Wang, Qi Wang, and David Galindo. "*How Do Smart Contracts Benefit Security Protocols ?*" arXiv preprint arXiv:2202.08699. https://arxiv.org/pdf/2202.08699.pdf.

- **Rujia Li**, Qin Wang, David Galindo, Qi Wang, Shipping Chen and Yang Xiang. "*Transparent Registration-Based Encryption through Blockchain*" ACM Transactions on Distributed Ledger Technologies: Research and Practice (**DLT 22**) (under review).

TTP-I Protocol Challenges



Benefits

TTP-I shifts the requirement for trustworthiness from any particular party to the majority of ledger maintainers.

- ✓ Non-equivocation
- ✓ Non-repudiation
- ✓ Non-frameability

Challenges

Smart contract lacks confidentiality. The operation code and contract state in TTP-I are completely transparent, and any state and its changes are publicly accessible and observable.

Thesis Outline

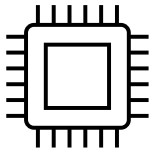
TTP issues in security protocols

Chapter 1 Aims: make cryptographic protocols practical and secure

Smart contract aided TTP

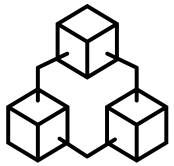
Chapter 3 Introduce a fair TTP

Smart contract & TEE-assisted TTP



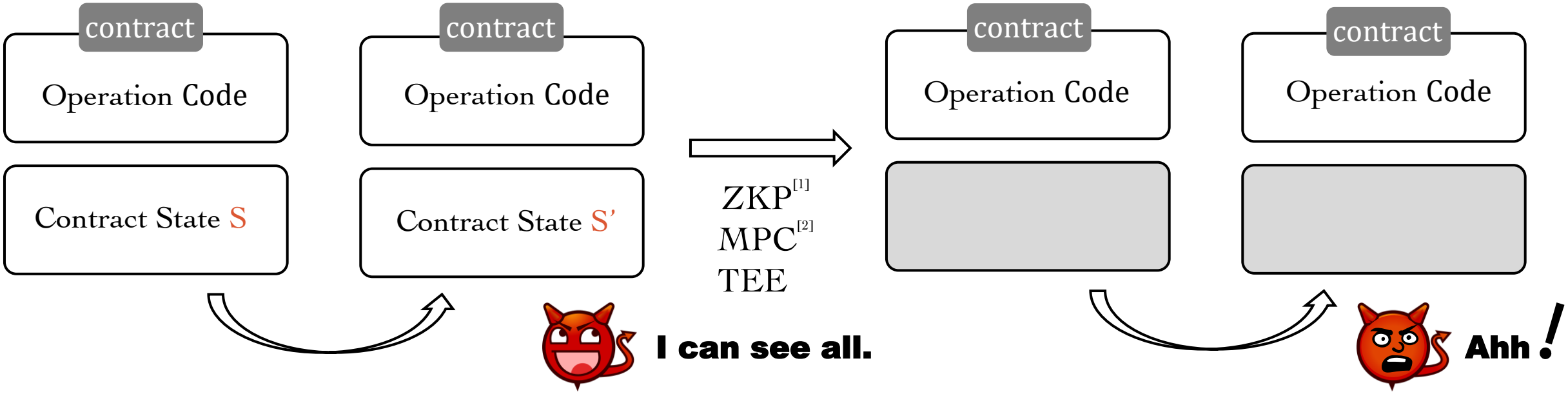
Chapters 4 and 5 Build a privacy-preserving TTP

Blockchain system enhancement



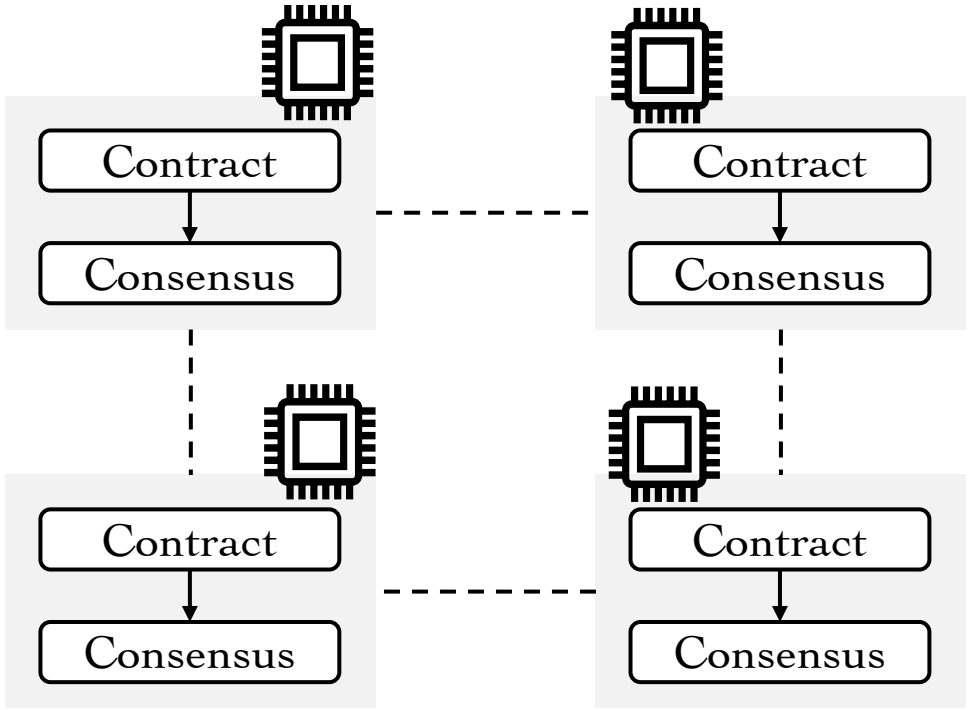
Chapter 6 Create better blockchain systems

Confidential Smart Contract



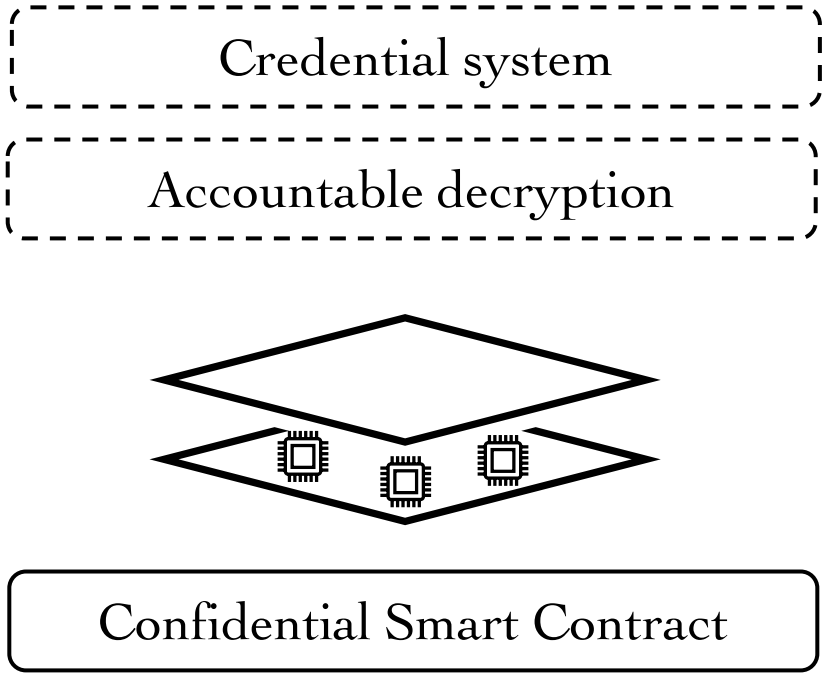
[1] K. Baghery. On the efficiency of privacy-preserving smart contract systems. In Proceedings of the 2019 International Conference on Cryptology in Africa (AFRICACRYPT), pages 118–136. Springer, 2019.
[2] G. Zyskind, O. Nathan, and A. Pentland. Enigma: decentralized computation platform with guaranteed privacy, 2015. arXiv preprint.

TEE-assisted Confidential Smart Contract (TCSC)



- **Rujia Li**, Qin Wang, Qi Wang, David Galindo, Mark Ryan. "*SoK: TEE-assisted Confidential Smart Contract*." The 22nd Privacy Enhancing Technologies Symposium (**PETS 22**).
- **Rujia Li**, Qin Wang, Yuanzhao Li, Qi Wang, David Galindo. "*A Formal Treatment of TEE-assisted Confidential Smart Contract*." The 27th European Symposium on Research in Computer Security (**ESORICS 22**) (under review).

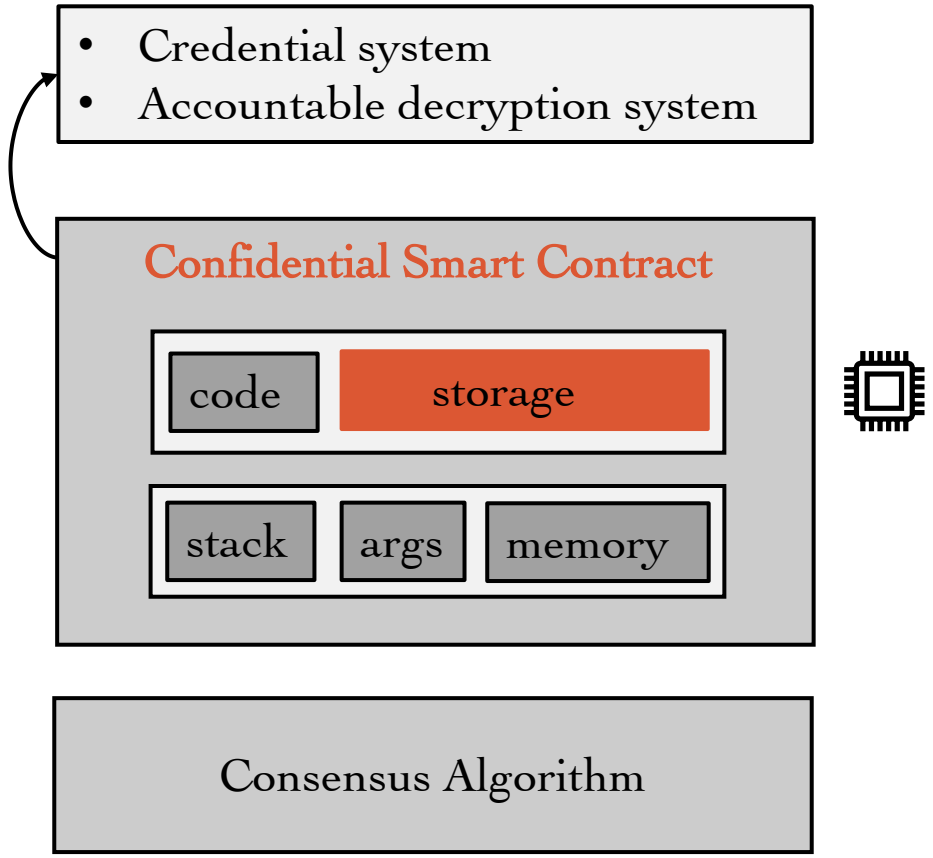
TTP-II: Smart Contract & TEE-assisted TTP



- **Rujia Li**, David Galindo, Qi Wang. "*Auditable Credential Anonymity Revocation Based on Privacy Preserving Smart Contracts*." The 3rd International Workshop on Cryptocurrencies and Blockchain Technology (**CBT 19**) on the 24th edition of the European Symposium on Research in Computer Security (**ESORICS 19**).

- **Rujia Li**, Qin Wang, Feng Liu, Qi Wang, David Galindo. "*An Accountable Decryption System Based on Privacy-Preserving Smart Contracts*." The 23rd Information Security Conference (**ISC 20**).

TTP-II Protocol Challenges



Benefits

TTP-II inherits the TTP-I's benefits, while it brings the confidentiality.

- ✓ Non-equivocation
- ✓ Non-repudiation
- ✓ Non-frameability
- ✓ State-confidentiality

Challenges

- Low performance
- Poor scalability
- Bad user experience

Thesis Outline

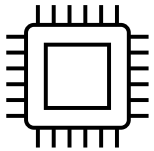
TTP issues in security protocols

Chapter 1 Aims: make cryptographic protocols practical and secure

Smart contract aided TTP

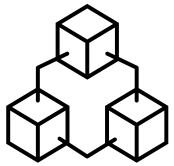
Chapter 3 Introduce a fair TTP

Smart contract & TEE-assisted TTP



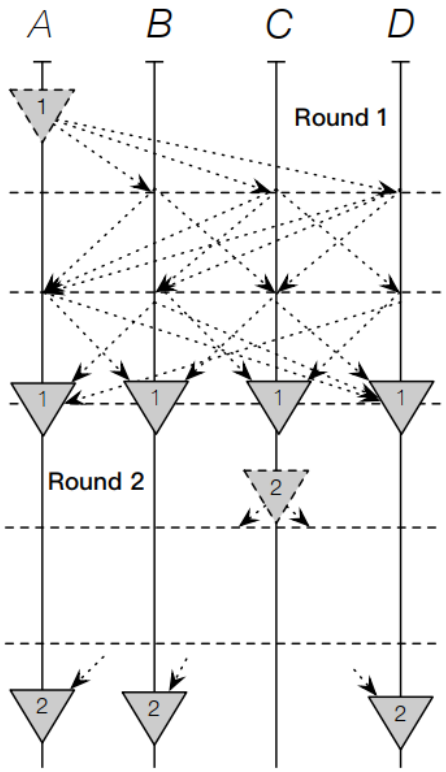
Chapters 4 and 5 Build a privacy-preserving TTP

Blockchain system enhancement

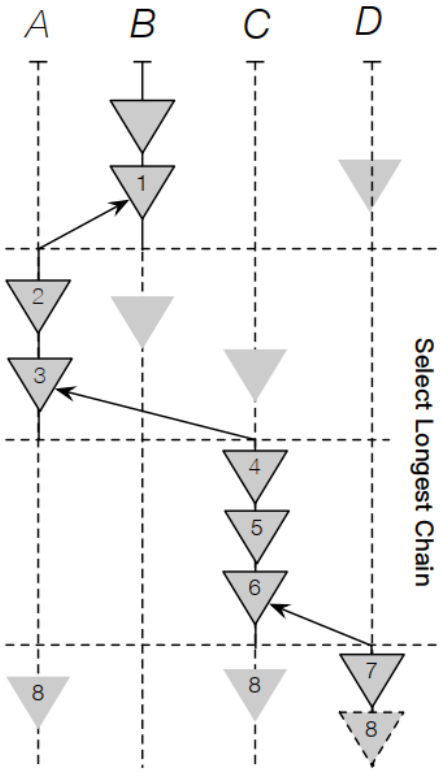


Chapter 6 Create better blockchain systems

Root Reason of Blockchain Bottleneck



a. (Traditional) BFT Consensus



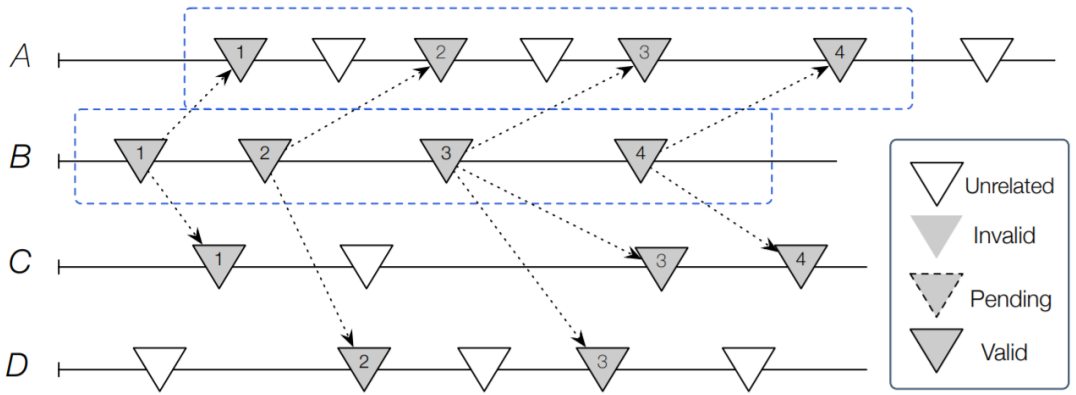
b. Nakamoto Consensus

A fundamental problem in distributed systems

The consensus mechanism requires agreement among a number of nodes for a single data value. Some nodes may fail or be unreliable in other ways.

Our Solution - Weak Consensus Algorithm

The sequence of (B1 → B2 → B3 → B4) can be correctly maintained across chains, no matter how many blocks (generated by other nodes) are inserted between them.

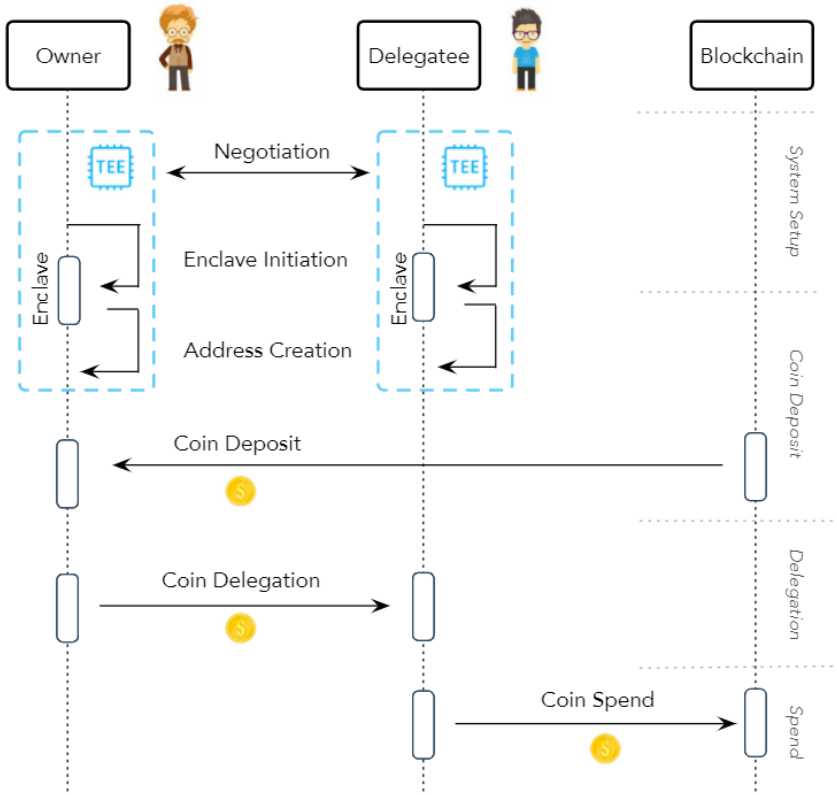


- Qin Wang*, **Rujia Li***. "*A Weak Consensus Algorithm and Its Application to High-Performance Blockchain*". The 40th IEEE International Conference on Computer Communications (**INFOCOM 21**) (*equal contribution).

- Qin Wang*, **Rujia Li***, Shiping Chen, Qi Wang, Yang Xiang. "Exploring Unfairness on Proof of Authority: Order Manipulation Attacks and Remedies." 17th ACM ASIA Conference on Computer and Communications Security (**ASIACCS 22**) (*equal contribution).

Solving this fundamental problem by proposing new consensus algorithm

Our Solution - Delegatable Payment



- **Rujia Li**, Qin Wang, Xinrui Zhang, Qi Wang, David Galindo, Yang Xiang. "*Poster: An Offline Delegatable Cryptocurrency System.*" In Poster Session of 28th Annual Network and Distributed System Security Symposium (**NDSS 21 Poster**).

- **Rujia Li**, Qin Wang, Xinrui Zhang, Qi Wang, David Galindo, Yang Xiang. "*An Offline Delegatable Cryptocurrency System.*" The 3rd IEEE International Conference on Blockchain and Cryptocurrency (**ICBC 21**).

Solving this fundamental problem by proposing a TEE-based payment solution

Summary of Thesis