An Accountable Decryption System Based on Privacy-Preserving Smart Contracts

Rujia Li[1,2], Qin Wang[3] , Feng Liu[1] , Qi Wang[1] , David Galindo[2,4]

1 Southern University of Science and Technology, Shenzhen, China
2 University of Birmingham, Birmingham, United Kingdom
3 Swinburne University of Technology, Melbourne, Australia
4 Fetch.AI, Cambridge, United Kingdom

December 17, 2020.

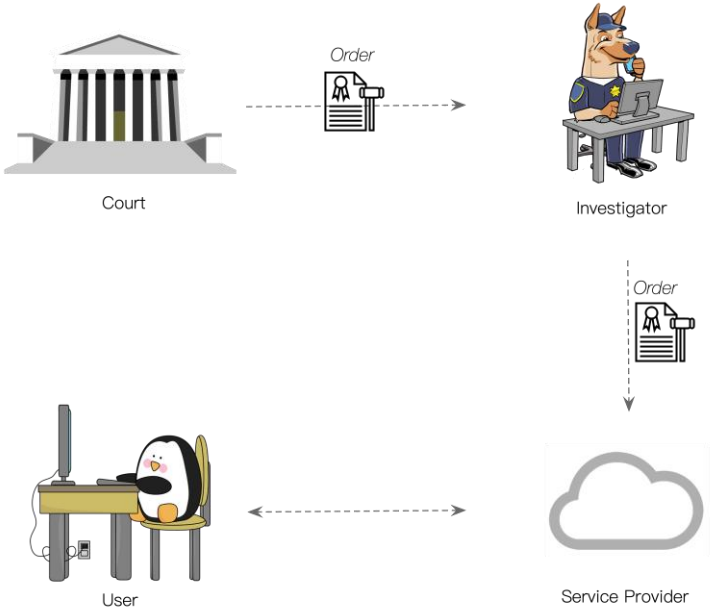
FBI vs Apple

FBI filed a court order in 2016 commanding Apple to unlock the iPhone of one of the shooters in a terrorist attack.

Surveillance lacks accountability

Surveillance powers may be misused or abused.

How to hold law-enforcements (investigators) accountable for their electronic surveillance ?

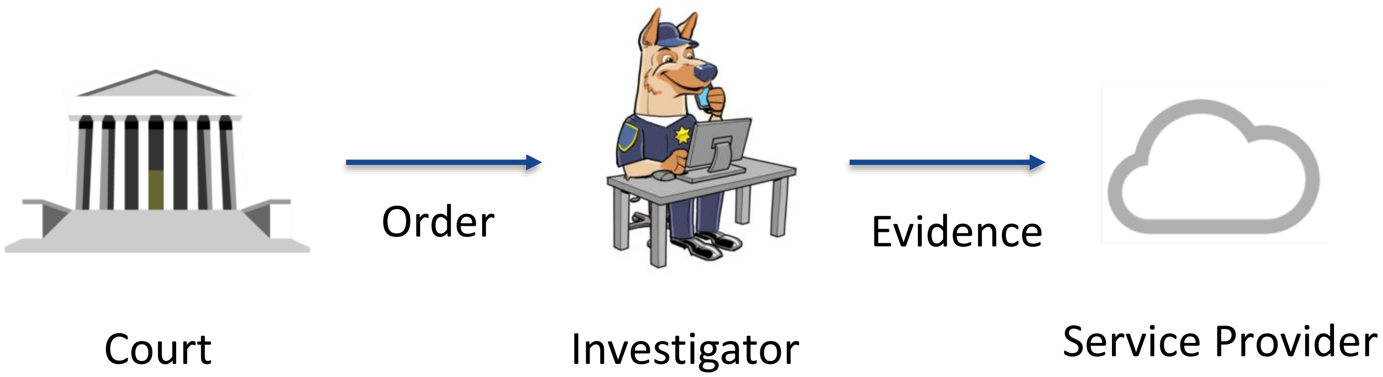


Surveillance lacks accountability

Secrecy: The orders usually never see the light of day. The data owners have no way to know when and how law enforcements collect and accesses their sensitive data.

Abused: The abuses of granted warrant of decryption may easily happen since the overseers cannot verify whether the practical investigation activities match the scope permitted in the document.

How does accountability work ?



Order

Evidence

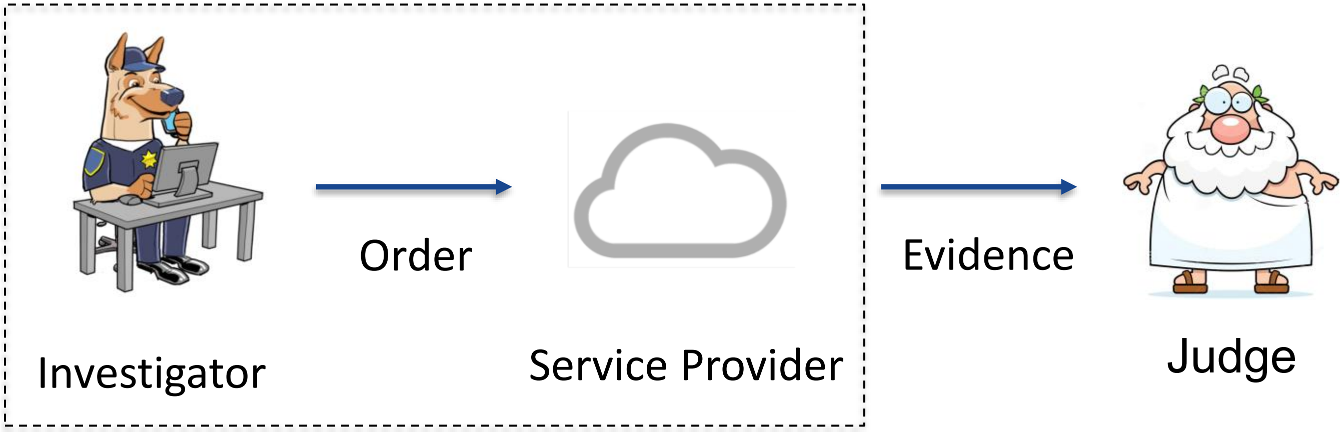
Court

Investigator

Service Provider

Firstly, the investigator obtains an order from the court. Then, this investigator demands access to personal encrypted data held by service providers.

How does accountability work ?



Investigator

Order

Service Provider

Evidence

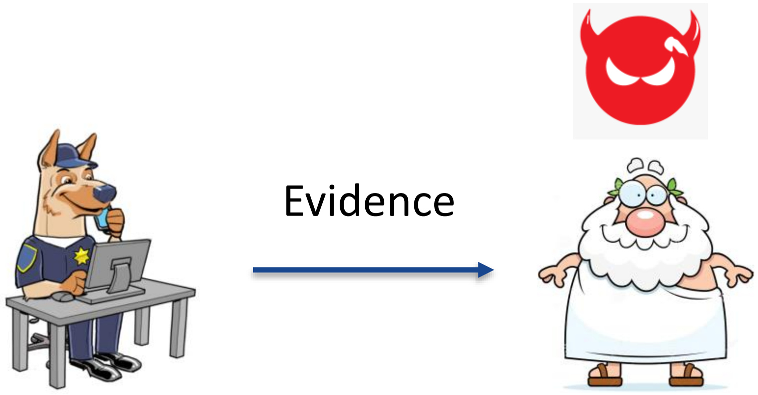
Judge

Since the investigators cannot autonomously convince others of the accountability of their actions, they need to resort to one or more judge(s), to audit their actions.

Challenges: malicious judge

An judge may

- apply the wrong examination procedure.
- give a fake examination result to void the accountability

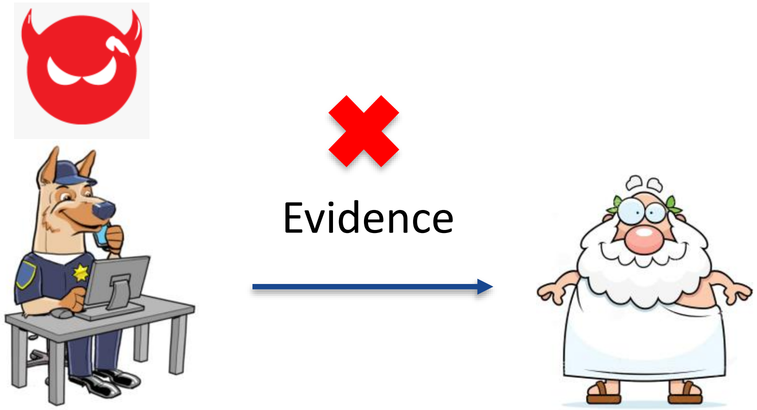


Evidence

Investigator

Judge

Challenges: malicious investigator



Evidence

Investigator

Judge

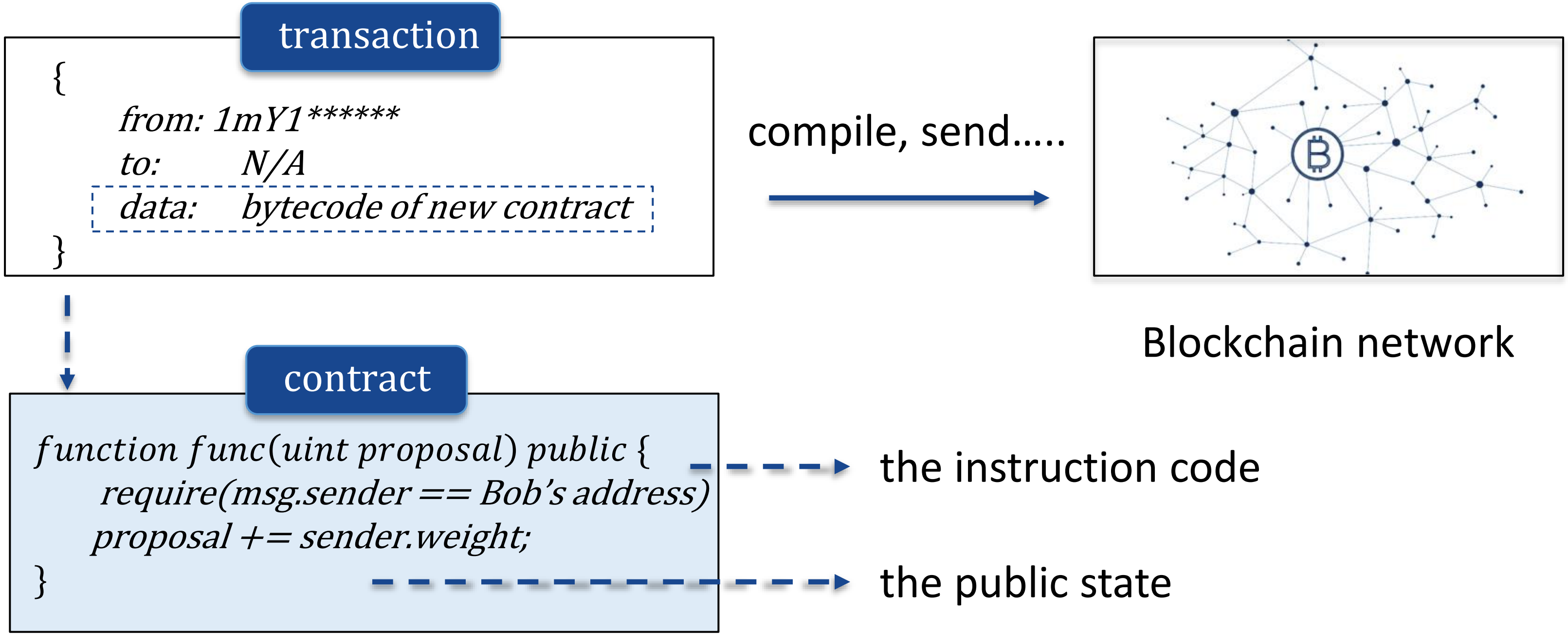
An investigator may

- fabricate fake evidence
- reject to cooperate with the judge.

Research problem

Is it possible to design an accountability mechanism guaranteeing that (1) the judge honestly checks the evidence; (2) the investigator does not refuse to provide the evidence trail of their actions?

Smart contract



transaction

```
{
    from: 1mY1******
    to:       N/A
    data:    bytecode of new contract
}
```

compile, send.....

Blockchain network

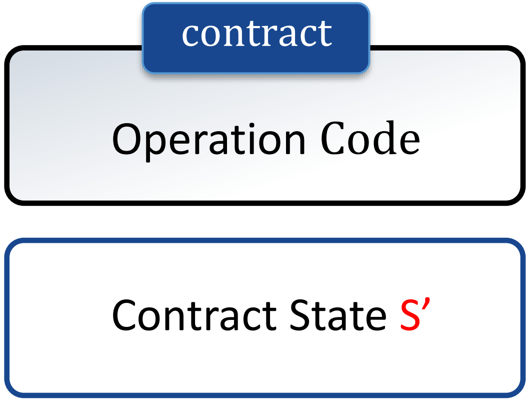
contract

```
function func(uint proposal) public {
    require(msg.sender == Bob's address)
    proposal += sender.weight;
}
```

the instruction code

the public state

Smart contract properties



contract

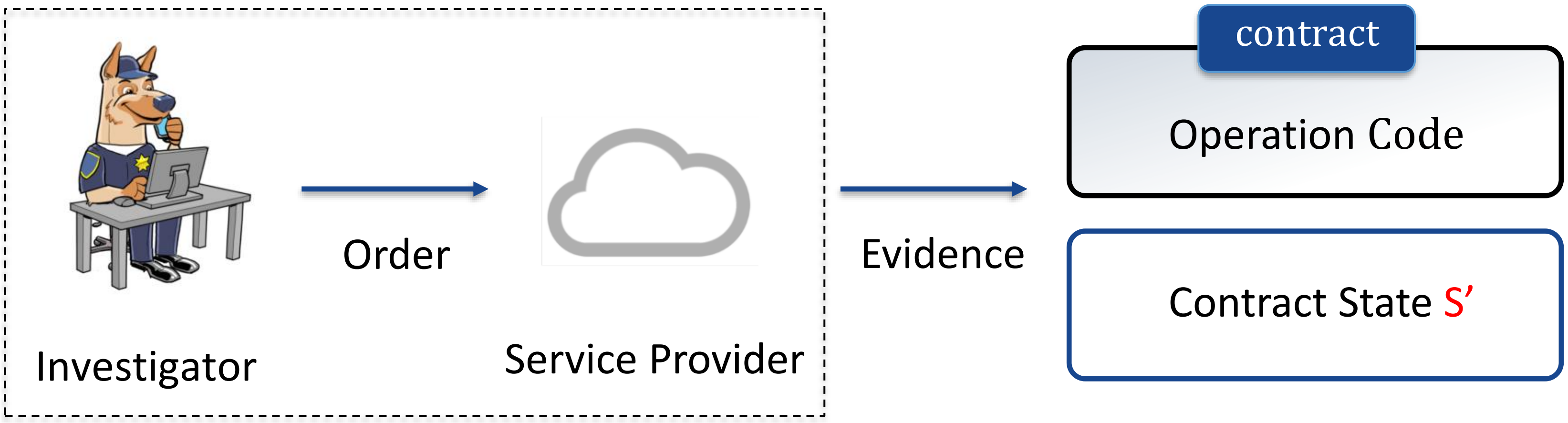
Operation Code

Contract State S’

State and its changes are transparent.

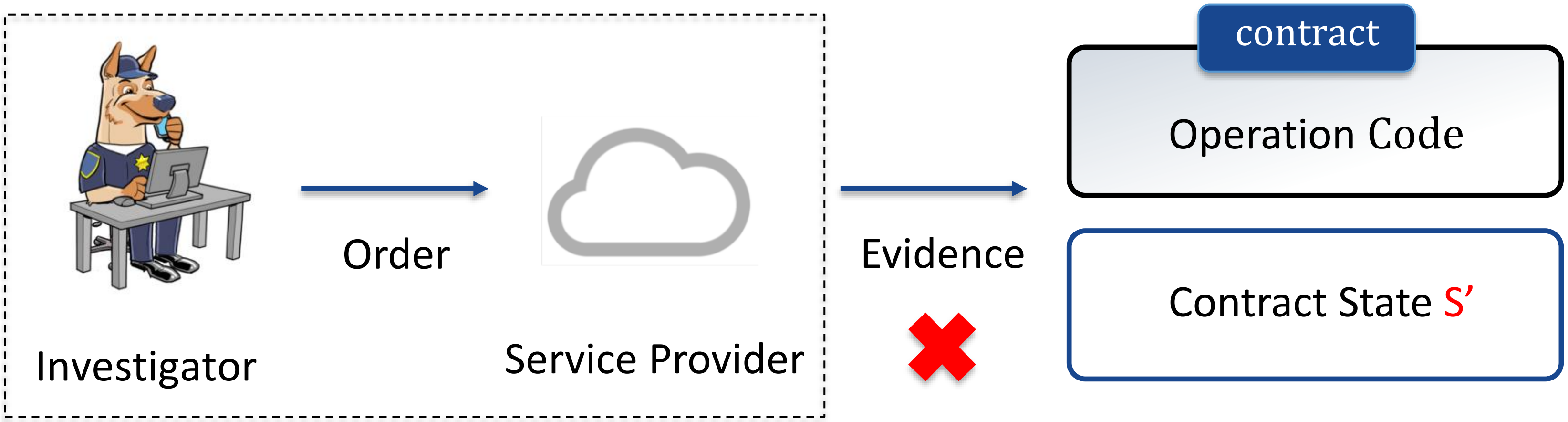
Transactions cannot be cancelled or reversed.

Smart contract as judge?



Smart contract is naturally acting as a judge. Selected examples: [AAT16] [KLM17] [NSG17]

Smart contract as judge?



Investigator

Order

Service Provider

Evidence

✖

contract

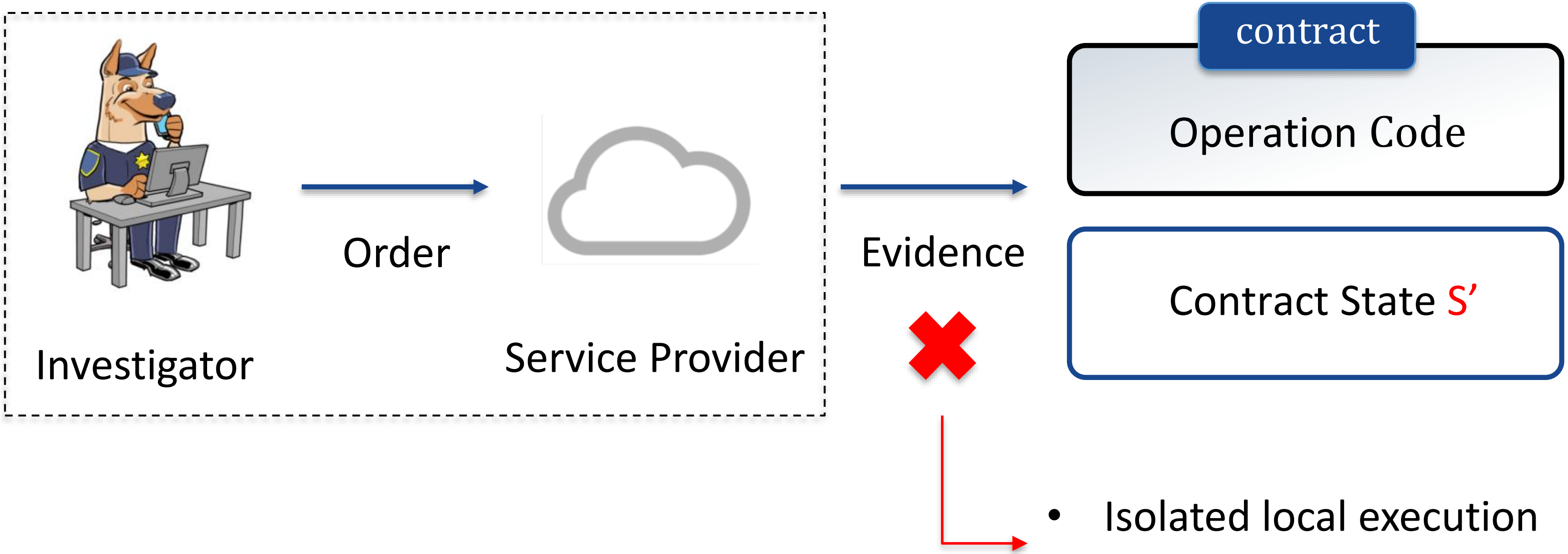
Operation Code

Contract State S’

- Execution automatically
- State and its changes are transparent.

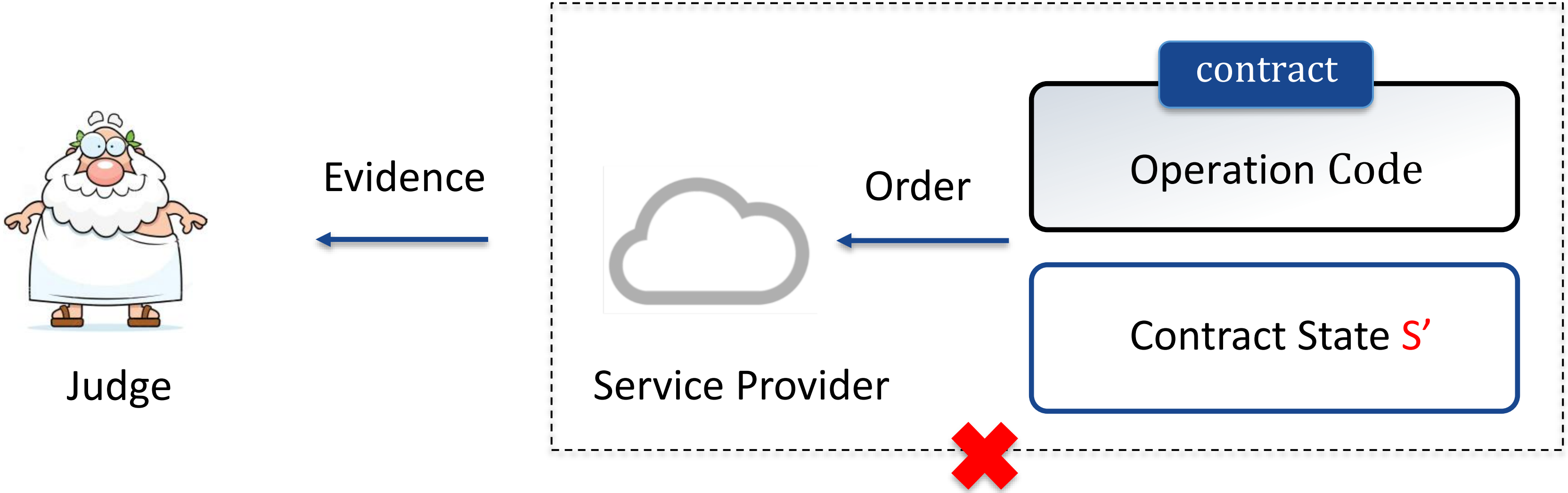
- Refuse to provide authentic evidence.
- The input evidence is fake.

Smart contract as judge?



- Isolated local execution
- A low risk of being detected

Smart contract as investigator?



Judge

Evidence

Service Provider

Order

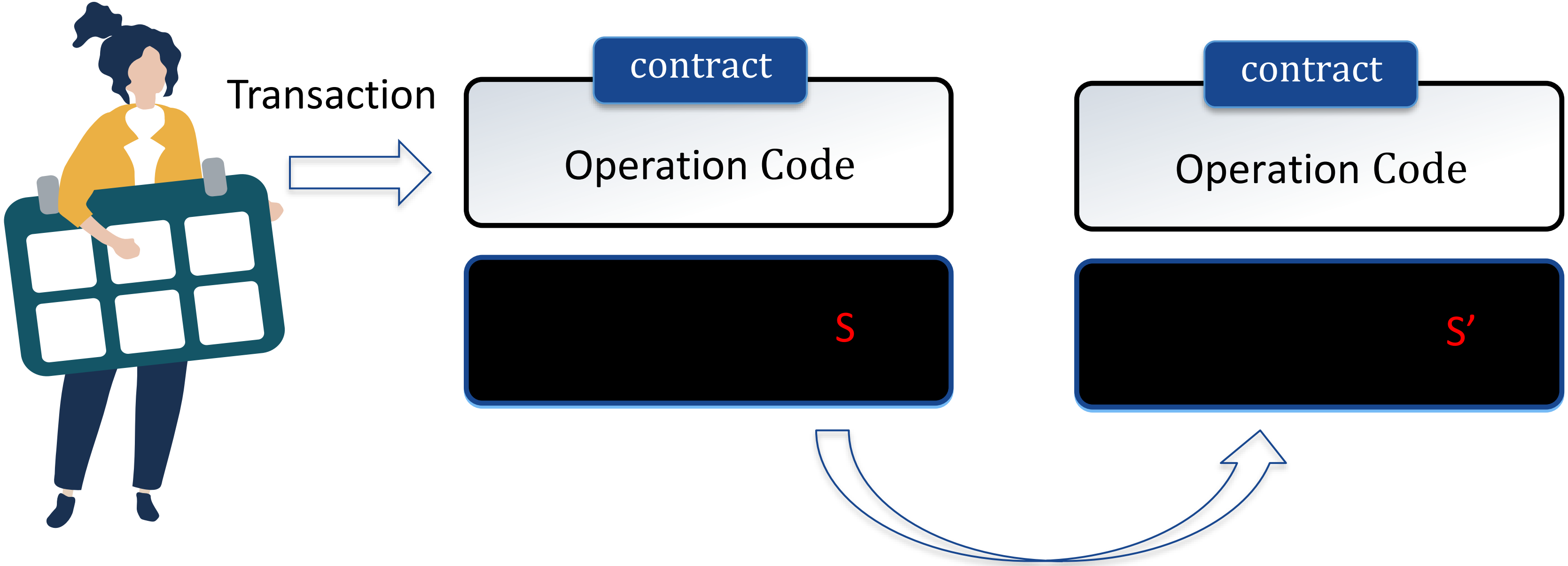
contract

Operation Code

Contract State S’

Total transparency to the public limits its adoption under confidential-related protocols.

Privacy-preserving smart contract



Related project

ZKP

Zkay project, [Sbg+19] (CCS 2019), Zether project, [Bunz +19] (FC 2020),

TEEs

Ekiden project , [Che+19] (EuroS&P 2019)

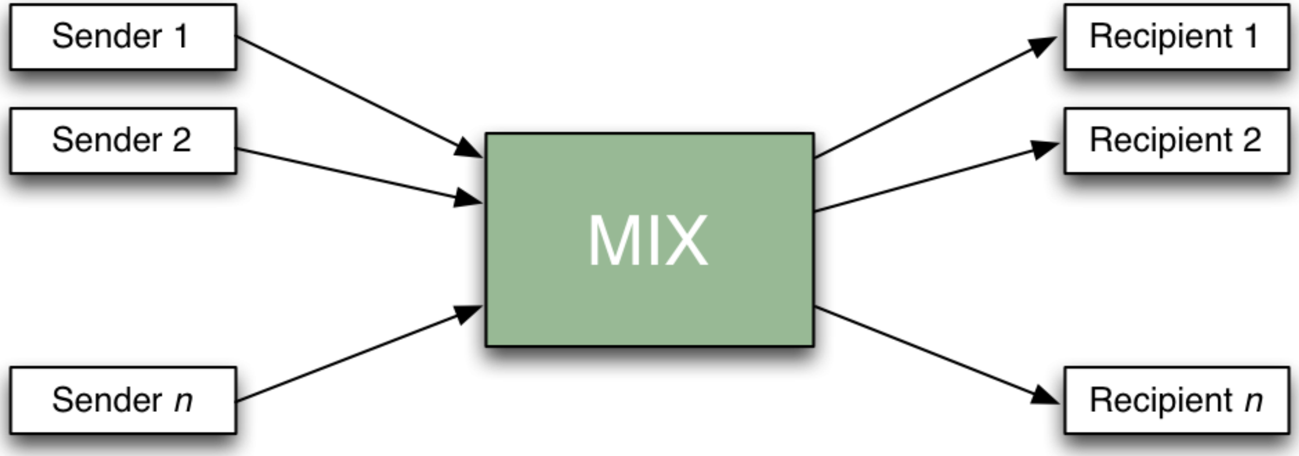
MPC

Enigma project, [ZNP15] (arXiv, 2015)

Others

On/Off-chain SC project, [LPX19] (arXiv, 2019)

PPSC ≈ Distributed verifiable shuffles



TEEs, e.g., Intel SGX

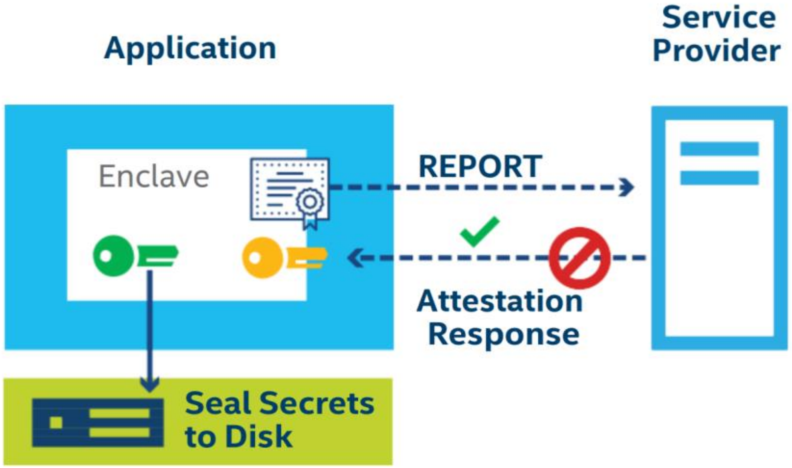


Image source [Intel20]

- Full Isolation
- Local Attestation
- Remote Attestation

PPSC example: Ekiden (EuroS&P, 2019)

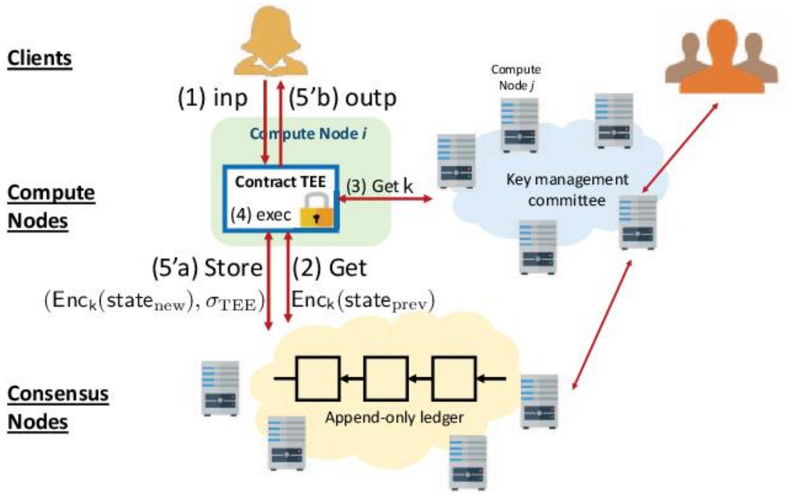


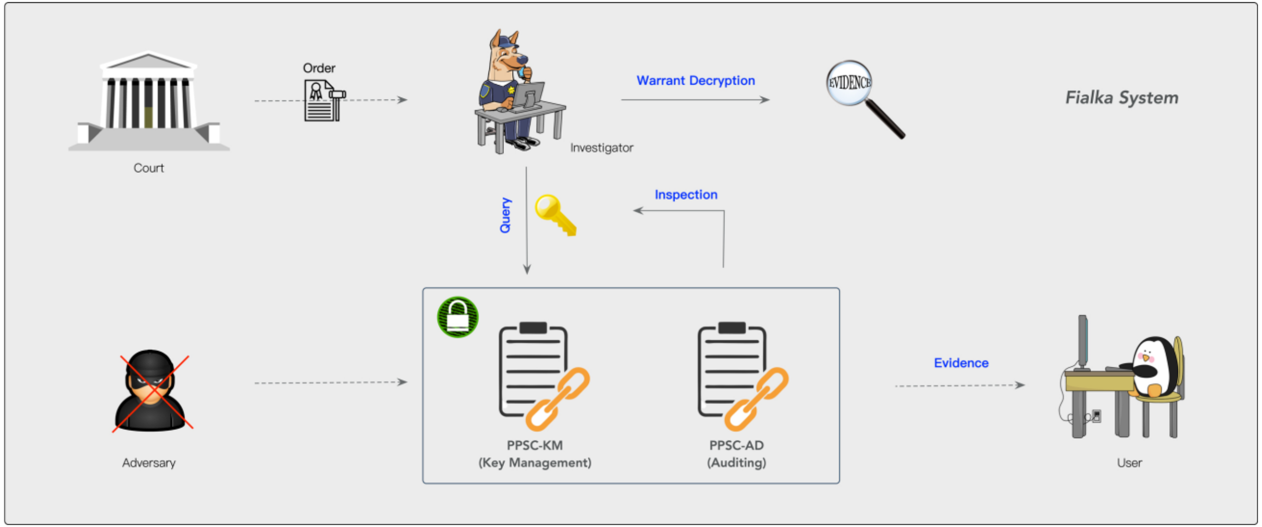
Image source [Che+19]

Clients can create contracts or execute existing ones with secret input.

Compute nodes process requests from clients by running the contract in a contract TEE and generating attestations proving the correctness of state updates.

Consensus nodes maintain a distributed append-only ledger, i.e. a blockchain, by running a consensus protocol.

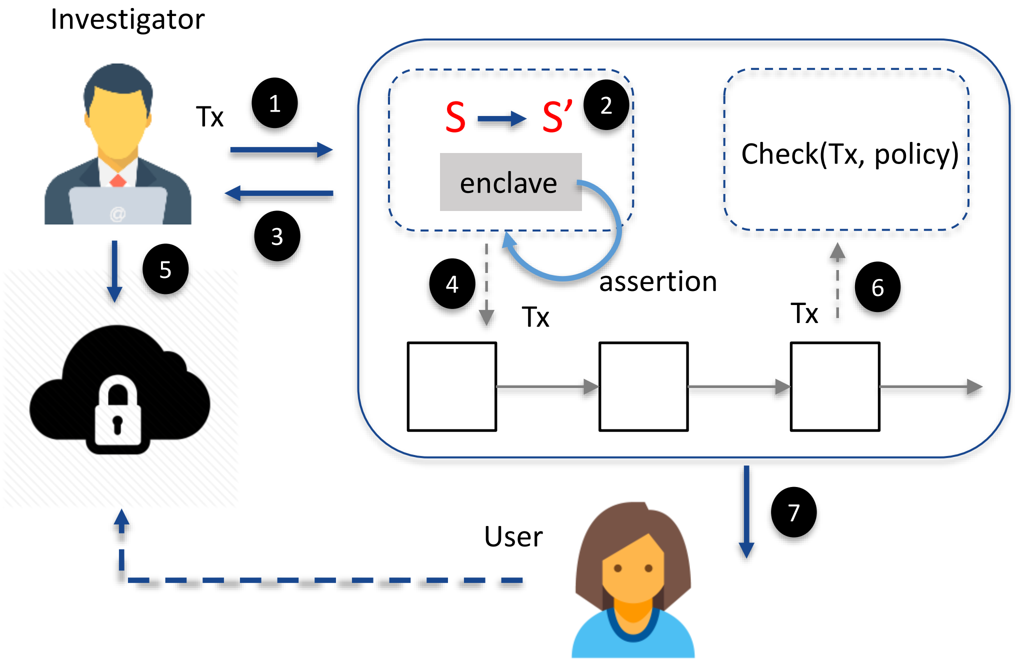
Fialka system overview



PPSC is used as key manager

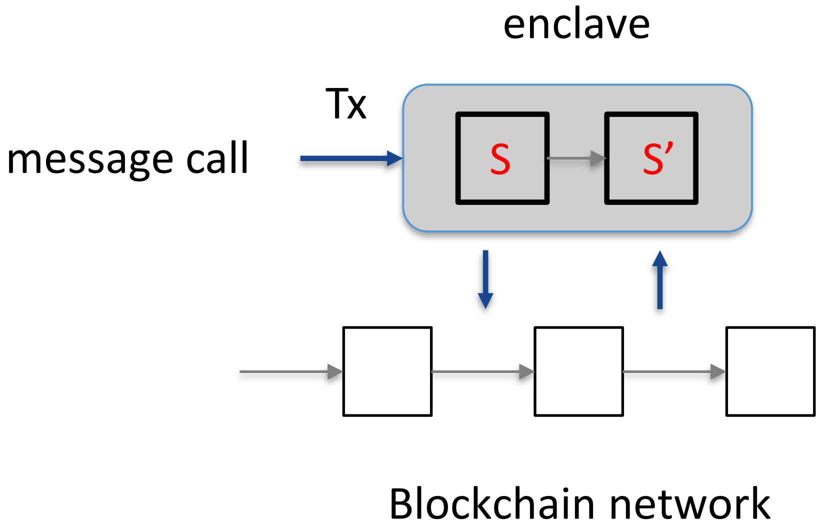
PPSC is used as auditor

How does Fialka work ?



1. **Send a transaction**
2. **State change**
3. **Obtain the private key**
4. **Transaction confirmation**
5. **Decryption**
6. **Check the evidence**
7. **User notification**

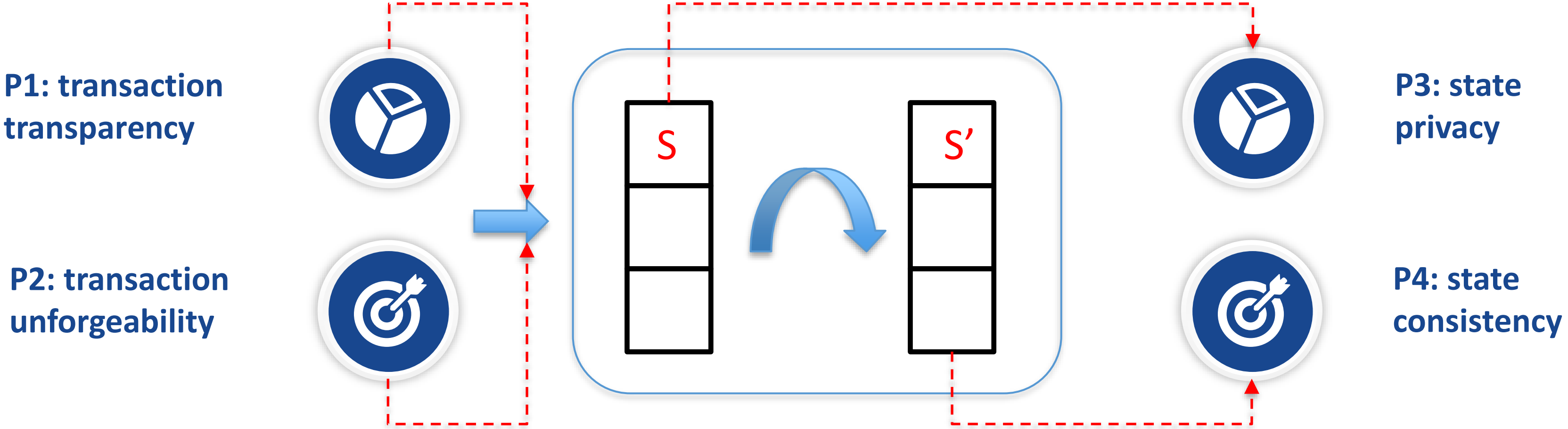
PPSC-based accountability



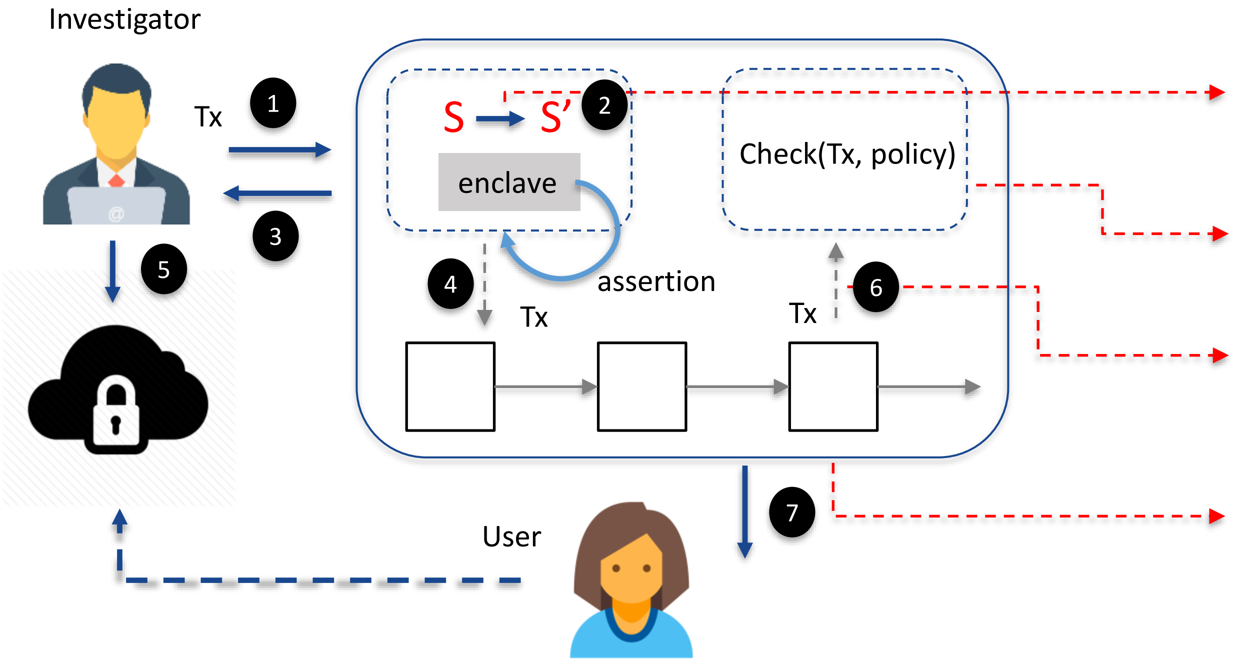
PPSC inherits the state triggering mechanism from smart contracts, namely, the state-changing is based on external message call.

By tracing the account who sends the transaction, the auditor implicates the wrongdoing of the contract caller.

PPSC's security properties



Fialka security discussion



TEEs protects the privacy of private key. **(P3)**

Distributed execution ensures the neutrality of the judge. **(P1)**

Transaction makes evidence transparent. **(P1, P2)**

Blockchain guarantees the consistency of the private key. **(P4)**

Fialka security discussion

Fairness

It prevents the judge from framing investigators who behave honestly.

The adversary cannot maliciously executes the warrant/order, or frame an honest investigator.

- Transaction-unforgeability
- State-consistency

Fialka security discussion

Completeness

It guarantees that the judge always punishes investigators who are misbehaving.

An adversary cannot evade the responsibility of illegally executing the authorized decryption.

- Transaction-unforgeability
- State-consistency
- State-privacy

Summary

- Surveillance lacks accountability.
- Challenges of current accountability schemes.
- The mechanisms and properties of privacy-preserving smart contract.
- Apply PPSC to an accountable decryption scheme.
- Security discussion.

References

- [Che+19] Raymond Cheng et al. “Ekiden: A Platform for Confidentiality-Preserving, Trustworthy, andPerformant Smart Contracts”. In:2019 IEEE European Symposium on Security and Privacy(EuroS&P). IEEE. 2019, pp. 185–200.
- [Kos+16] Ahmed Kosba et al. “Hawk: The blockchain model of cryptography and privacy-preserving smart contracts”. In:2016 IEEE symposium on security and privacy (SP). IEEE. 2016, pp. 839–858
- [B¨unz+19] Benedikt B¨unz et al. “Zether: Towards Privacy in a Smart Contract World.” In:IACR CryptologyePrint Archive2019 (2019), p. 191
- [ZNP15] Guy Zyskind, Oz Nathan, and Alex Pentland. “Enigma: Decentralized computation platformwith guaranteed privacy”. In:arXiv preprint arXiv:1506.03471(2015)
- [LPX19] Chao Li, Balaji Palanisamy, and Runhua Xu. “Scalable and Privacy-preserving Design of On/Off-chain Smart Contracts”. In:arXiv preprint arXiv:1902.06359(2019)
- [Intel] Software.intel.com. 2020. [online] Available at: <https://software.intel.com/sites/default/files/managed/c3/8b/intel-sgx-product-brief-2019.pdf> [Accessed 1 November 2020].
- [AAT16] Azaria, A., Ekblaw, A., Vieira, T.: Medrec: Using blockchain for medical data access and permission management. In: OBD’16. pp. 25–30. IEEE (2016)
- [NSG17] Neisse, R., Steri, G., Nai-Fovino, I.: A blockchain-based approach for data accountability and provenance tracking. In: ARES’17. p. 14. ACM (2017)
- [KLM17] Kaaniche, N., Laurent, M.: A blockchain-based data usage auditing architecture with enhanced privacy and availability. In: NCA’ 17. pp. 1–5. IEEE (2017)

Thanks

An Accountable Decryption System Based on Privacy-Preserving Smart Contracts

Rujia Li[1,2], Qin Wang[3], Feng Liu[1], Qi Wang[1], David Galindo[2,4]

1 Southern University of Science and Technology, Shenzhen, China

2 University of Birmingham, Birmingham, United Kingdom

3 Swinburne University of Technology, Melbourne, Australia

4 Fetch.AI, Cambridge, United Kingdom

December 17, 2020.