

# Using ABE to Secure Blockchain Transaction Data

Andrei Cristian

June 6, 2021

# Table of Contents

- 1 Introduction
- 2 System and Models
- 3 PoP System Models
- 4 PoP Operation and Performance Analysis
- 5 Summary
- 6 References

# Introduction

- Blockchain technology is increasingly being adopted as a trusted platform to support business functions including trusted and verifiable transactions, tracking, and validation.
- Most business use-cases require privacy and confidentiality for data and transactions  $\Rightarrow$  **Private blockchain solutions**  $\Rightarrow$  Unable to take full advantage of the capabilities, benefits and infrastructure of public blockchain systems.
- **Attribute-Based Encryption** security solution built on private-over-public (PoP) blockchain  $\Rightarrow$  Businesses will be able to **restrict access, maintain privacy, improve performance**, while still being able to benefit from the distributed trust of public blockchains.

# Public and Private Blockchains I

- Similarities[1]:
  - ① both are decentralized peer-to-peer networks, where each participant maintains a replica of a shared append-only ledger of digitally signed transactions;
  - ② both maintain the replicas in sync through a protocol referred to as consensus;
  - ③ both provide certain guarantees on the immutability of the ledger, even when some participants are faulty or malicious.
- The main distinction between public and private blockchain is related to who is allowed to participate in the network.

## Public and Private Blockchains II

- One of the drawbacks of the public blockchain is the substantial amount of computational power to maintain a distributed ledger at a large scale to achieve consensus, in which each node in a network must solve a complex, resource-intensive cryptographic problem - called Proof of Work (PoW)[2] to ensure all are in sync.
- Another disadvantage is the openness of public blockchain, which implies little to no privacy protection for transactions and only supports a weak notion of security.

## Public and Private Blockchains III

- Many people believe private blockchains could provide solutions to many financial enterprise problems, that public blockchains do not, such as abiding by regulations such as Health Insurance Portability and Accountability Act (HIPPA), anti-money laundering (AML) and know-your-customer (KYC) laws, etc.
- Private blockchain is usually much faster, cheaper and respects the company's privacy.
- Private blockchains also provide more control power over the participants in the blockchain.

# Public and Private Blockchains IV

- **Cross-chain** functionality aims to combine the best features of different blockchain systems[3], both private and public, for the purposes of exchanging value across disconnected ecosystems.
- None of existing solutions clearly addressed the problem of applying access control policies to enforce data privacy protection on transaction secrets.

## Public and Private Blockchains V

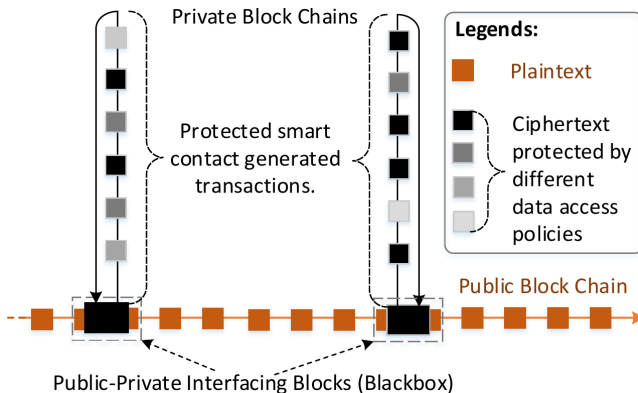
- For example, when using smart contract solutions, e.g. Ethereum[4], for procurement in supply-chain, transaction parameters such as product name, quantity, price, purchasing terms, shipping options, address, etc. could all be **sensitive business secrets**. They should be only viewable for relevant stakeholders.
- Hyperledger[5] addresses this problem by relying on a TA approach to build permission groups for data access control. However, data access must be **predefined** which is not suitable for complex and dynamic businesses logic that require dynamic access control.



# Public and Private Blockchains VI

- **RBAC** is **incompatible** with the distributed nature of blockchain operations where transaction data are mobile and shared by multiple blockchain participants.

# POP architecture



**Figure:** Illustration of PoP blockchain architecture.

# ABE over PoP Blockchain I

- PoP architecture is presented in Figure 1.
- Applying ABE on an off-chain basis means it can inter-operate with the public blockchain without interference.
- Private blockchains transactions can be much **less computationally intensive** and provide **superior performance** since they do not have to be verified by all participants.
- Businesses are able to choose the private blockchain solution that **best suits their needs** independently from the public blockchain.

## ABE over PoP Blockchain II

- Each private blockchain can be viewed as a **protected state channel**.
- The integrity of a private blockchain can be validated and checked in ciphertext and in aggregate by all public blockchain participants.
- The public blockchain infrastructure is leveraged to provide **validation** and **immutability** for the entirety of the private blockchain state channel.
- This can take the form of the final private blockchain transaction result, or a hash of the entire private blockchain  
⇒ distributed trust on the public chain is **not necessary** for the private blockchain.

## ABE over PoP Blockchain III

- **ABE** provides **data privacy** for the private blockchain state channel.
- Only participants with the appropriate permissions and corresponding ABE attribute private keys can view and validate their relevant blocks in the private block chain.
- It provides the benefits of private blockchains in terms of privacy without requiring the deployment of trusted nodes or multiple verification nodes.
- It essentially minimizes the entry cost businesses in adopting blockchain solutions.

# The PoP Solution I

In summary, the presented PoP solution has the following main features:

- It is a decentralized trust model for key management of ABE-based data access control. Using this approach, it can incorporate access control policies into ciphertext to protect content of smart contracts.
- It is a privacy-preserving messaging protocol to allow private blockchain participants to interact with the smart contract that can generate a private blockchain. This chapter illustrates how to use this protocol based on a supply-chain procurement application.

## The PoP Solution II

- The solution provides two smart contracts: PPP (Public Parameters and Policies) to establish attribute based security trust model and ppSCM to provide secure data access control based on ABE scheme.
- A comprehensive security and performance analysis is presented based on the presented PPP scheme. The presented solution is practical that can significantly reduce the effort and cost to establish dedicated and isolated private blockchains.

# System and Models

- System and Models



# PoP System Models

- PoP System Models

# PoP Operation and Performance Analysis

- PoP Operation and Performance Analysis

# Summary

- Summary

# References I






P. Jayachandran, “The difference between public and private blockchain,” , 2017. [Online]. Available: <https://www.ibm.com/blogs/blockchain/2017/05/the-difference-between-public-and-private-blockchain/>.



S. Nakamoto, “Bitcoin: A peer-to-peer electronic cash system,” , 2008. [Online]. Available: <https://bitcoin.org/en/bitcoin-paper>.

## References II

-  J. Liebkind, “Public vs private blockchains: Challenges and gaps,” , 2018. [Online]. Available: <https://www.investopedia.com/news/public-vs-private-blockchains-challenges-and-gaps/>.
-  *Ethereum project*, [Online]. Available: <https://www.ethereum.org>.
-  C. Cachin, “Architecture of the hyperledger blockchain fabric,” , vol. 310, 2016. [Online]. Available: <https://www.zurich.ibm.com/dccl/papers/cachindccl.pdf>.