Using ABE to Secure Blockchain Transaction Data

Andrei Cristian

June 7, 2021

Table of Contents

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 consesnsus;
  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 **incompatbile** with the distributed nature of blockchain operations where transaction data are mobile and shared by multiple blockchain participants.

POP architecture

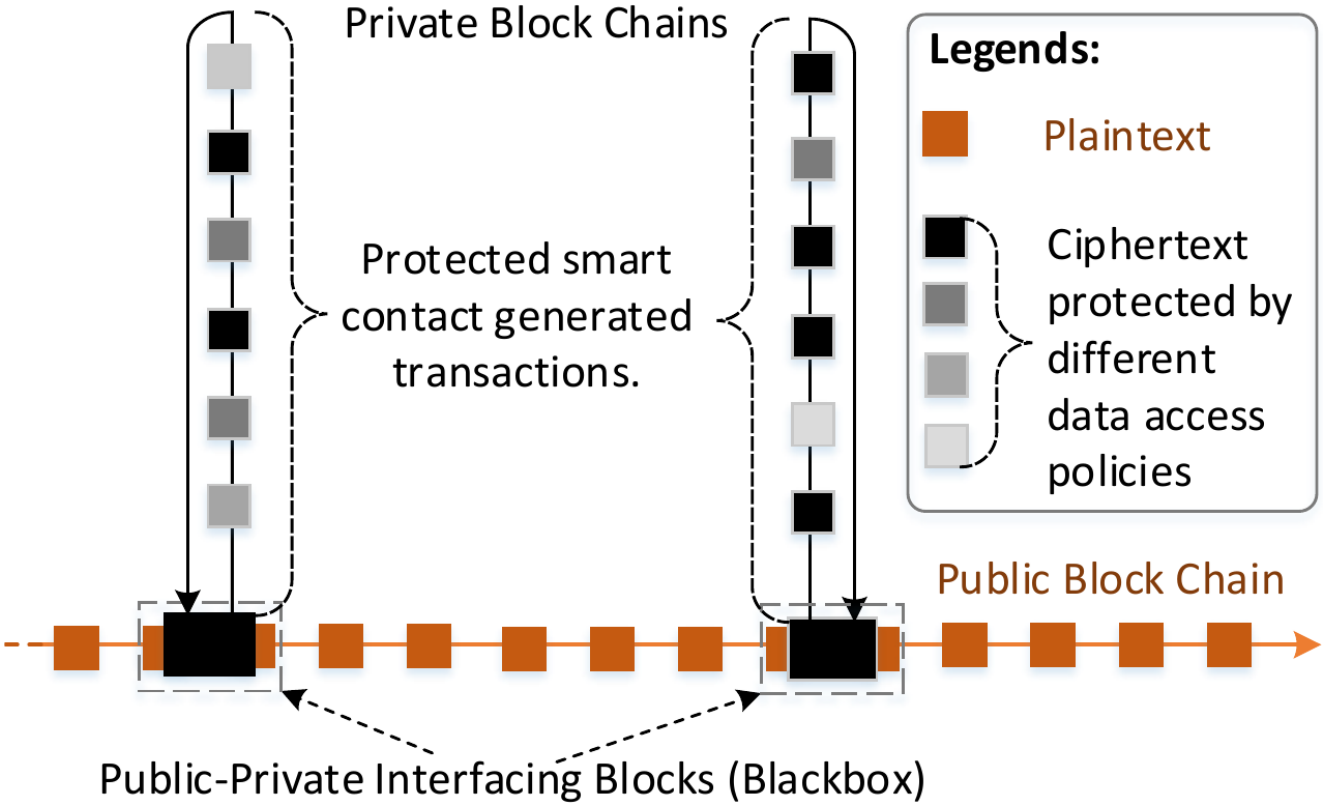

Figure: Illustration of PoP blockchain architecture.

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 $\Rightarrow$ 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

- To illustrate the presented solution, in Figure 2 it is used a supply chain example based on **Block-Chain Technology**(BCT), which involves multiple parties.
- The potential of having all the information written in a blockchain allows the creation of an **authoritative record** that can be used to **automatically** establish smart contracts.
- Because the information is registered on a distributed database, it makes it **tamper-resistant** and **fosters greater trust** in the trade network.

Supply chain example

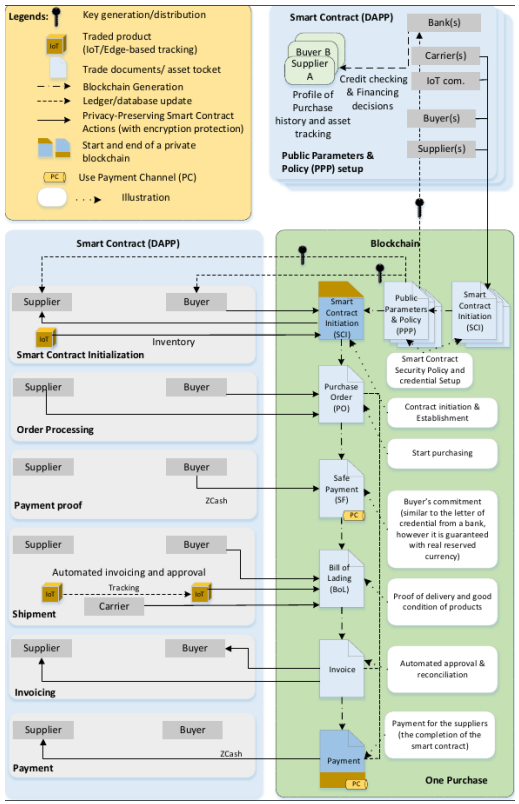

Figure: A supply chain scenario using IoT devices, blockchain, and data encryption protections.

Legends and Smart Contract interaction with Blockchain

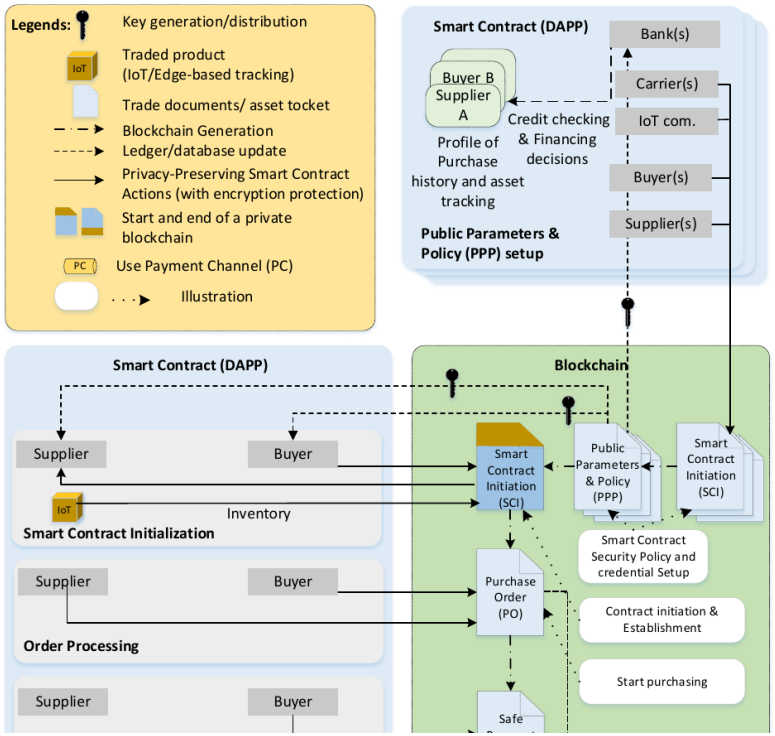

Figure: Zoom-in on Legends and interaction of the first smart contract with the blockchain

Smart Contract interaction with Blockchain

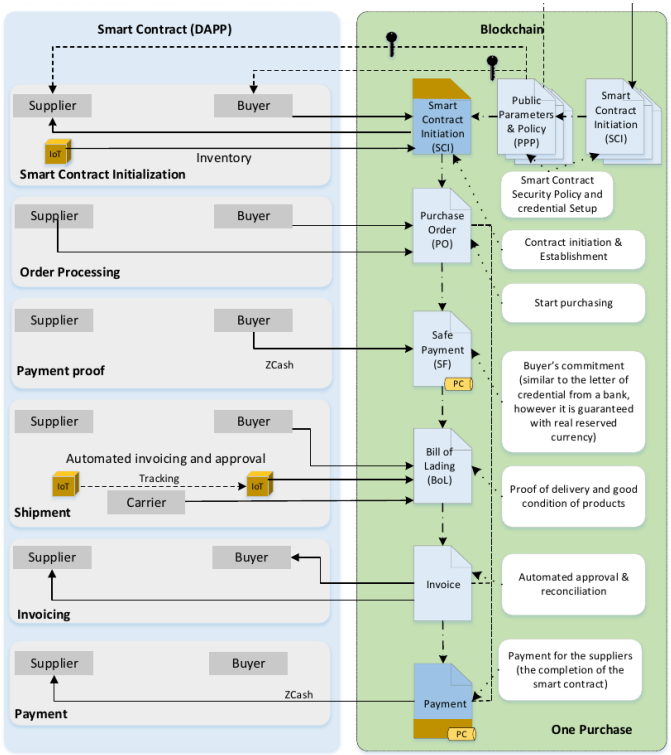

Figure: Zoom-in on the interaction of the second smart contract with the blockchain

BCT-supported purchase related transaction using DApp I

The left side of the figure present a BCT-supported purchase related transaction by using Ethereum's Decentralized App (DApp) solution involves 4 main procedures based on supply-chain operation procedures:

- **Order Processing**:
  - The order-processing workflow starts with a PO from the buyer. Within the blockchain, once created, the PO is time-stamped and can become a valid document whose clauses can be executed **only if valid**, due to the programming features of smart contracts.

BCT-supported purchase related transaction using DApp II

- Assuming delivery documents can also be registered on it, the metadata of the invoice, PO and bill of lading could be matched automatically due to the smart contracts feature, which **ensures consistency between price and quantity** in all three documents (i.e. three-way-match), permitting an **automated** and **fast invoice approval**.
- The entire history of the transactions offers **perfect audibility**, and **trust between parties** is provided by the **immutability of the data** entered in a blockchain.

- **Shipment**:
  - **IoT-based tracking capability** is a critical component for this procedure.

BCT-supported purchase related transaction using DApp III

- Keeping track of the **material flow** at each step, along with the corresponding **paper flow**, is a major undertaking that **requires manual processes** that are subject to **human error**, **loss**, **damage** or even **theft** and **fraud**.
- Another potential application is provided by smart contracts and cryptographic multi-signatures and product content protection for all the various documentation and processing stages involved in a trade transaction.
- In such a blockchain-based IoT, there is the possibility of maintaining **product information**, its **history**, **product revisions**, **warranty details** and **end of life**, transforming the blockchain into a distributed and trusted blockchain.

- **Invoicing**:

BCT-supported purchase related transaction using DApp IV

- Blockchain-based services can register the invoice-related information on a blockchain in order to **avoid duplicates** and **fraud** across the network.
- As explained by [6], each invoice would be distributed across the network, hashed and time-stamped in order to create a **unique identifier**.
- If a supplier tried to sell same invoice again through the network, that invoice would indicate a previous instance of financing to all parties, and the **double financing would be avoided**.

BCT-supported purchase related transaction using DApp V

- The **integration with the payment system** is given by the ability of smart contracts to **take control over an asset** registered on a blockchain (e.g. crypto-cash) and **automatically trigger the payment**.

- **Payment**:
  - Developed to create a purely peer-to-peer version of electronic cash to allow online payments, **payments are the first application of BCT**.
  - With the use of Bitcoin or similar cryptocurrencies in a B2B scenario, buyer and supplier could **transact without any intermediaries** (e.g. banks) and with **very small transaction fees**.

BCT-supported purchase related transaction using DApp VI

- Blockchain solutions could create **more efficient payment processes** between banks, eliminating the need for each institution to **maintain** and **reconcile their own ledger**.

Privacy problem I

- The described smart contract **does not provide privacy protection** for transaction contents processed by smart contracts.
- Two additional modules (incorporated into original supply-chain procedures):
  1. **Smart contract initialization**:
     - sets up the initial smart contract credentials such as agreed data access control policies for each step of smart contract;
     - initiates the off-chain operation, in which we start a private blockchain at this point.
  2. **Payment proof**:
     - the private chain can also incorporate public blockchain evidence into the private blockchain;

Privacy problem II

- the addition of the payment proof procedure is to utilize the payment channel feature of public blockchains to **prove the buyer has sufficient money** to pay for the purchased product;
- the buyer first pays for the product to a Escrow account, and once the product is landed, the cashed money will be delivered to the supplier to close the blockchain based purchase.

Smart Contracts I

- In Bitcoin, the concept of *"scripting"* has already existed, which is actually **a weak version** of smart contract.
  - it lacks Turing-completeness, thus does not nearly support everything;
  - it is value-blinded;
  - it lacks state, UTXO can either be spent or not, there is no way to keep other states except for these two;
  - it is blockchain blinded.
- Ethereum smart contract is to build a decentralized application to create a blockchain with a build-in Turing complete programming language.

Smart Contracts II

- Smart contract means is defined to be a cryptographic "boxes" that contain value and only unlock it if certain conditions are met.
- A smart contract will also be stored in the blockchain and can be retrieved by its address and integrity can be guaranteed as well.
- With smart contract, one can express logics such as "only after April 17th, 2018, can the document be sent to A".
- In the presented supply-chain example in Figure 2, two smart contracts are involved:

Smart Contracts III

1. **public blockchain smart contract**: the smart contract on the right side box includes multiple stake holders providing supply-chain services to settle down a **PPP** (Public Parameters and Policies).
   A PPP describes what encryption **public parameters** will be used for **data privacy protection**, who may serve as a **trusted party** for **data access control management** for running private blockchains, and what **security policies to be enforced** in the private blockchain. **We can treat PPP as a template**;

Smart Contracts IV

2. **private blockchain smart contract**: the smart contract on the left side of Figure 2 represents a one purchase between a supplier and a buyer. In addition, an **IoT company** can be involved to provide **product tracking and inventory**.

ABE-Enabled ABAC

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.

References III

 H. Erik, S. Urs Magnus, and N. Bosia, "Supply chain finance and blockchain technology: The case of reverse securitisation," , 2017.