CS6290 55323707 Reading Summary 3

Yu SU
Dept. of Computer Science
ID:55323707

I. Summary of Paper [1]

A. Problem statement

Smart contracts are protocols that digitally enforce agreement between or among distrusting parties on the blockchain, which are popular these years, but because the nature of blockchain and the consensus need, existing smart contracts lack the confidentiality and privacy. What's more, smart contracts are hampered by the consensus of blockchain.

As a result, the paper proposed a system called Ekiden, which is highly performant and confidentiality-preserving with the trusted execution environment. Besides the theory, the paper also presented a good evaluation result for the Ekiden-BT, a implementation for Ekiden.

B. Problem Significance

This paper is very meaningful. The existing smart contracts systems are not flexible enough for the smart contracts, even like ethereum, which is the most popular decentralized smart contracts platform, could only hold up the simple application because of the poor performance. What's more, the lack of confidentiality and privacy will also restrict the function of the smart contracts and cause some security and auditing problems. To make the smart contracts could develop better, we need a better system, which is not only efficient but also confidential.

C. State of the Art

At that time, to solve the problems that I have mentioned above, the researcher proposed many cryptographic solution, like zero-knowledge proof and secure multiparty computation. However, these approaches will cause significant overheads. That's the reason why these method could not be applied at that time.

So another approach called trusted execution environment came out, which combined the blockchain and trusted hardware. Although this design is very talented, there were still some challenges at that moment. First is there is a limitation for the hardware, as the scheduling and IO would be manipulated. Second, without utilization limitation, the confidentiality would be jeopardized by integrity attacks. What's more, supporting robust, fault tolerance, key management for enclaves and so on problems waited for solving.

D. Contributions

There are many key sights in the paper.

First, instead of talking about the Ekiden, the paper focused on the general challenge for TEE-blockchain hybrid system. In detail, the paper talked about how to solve the tolerating TEE failures, proof of publication for PoW blockchains, key management in TEEs and atomic delivery of execution results.

After that, the paper demonstrated the talented designs on Ekiden. First the paper talked about the whole architecture of it, the computation and consensus is independent. To realize this design, there are two types of nodes in Ekiden. One is compute nodes, the other is consensus nodes. Compute nodes are the off-chain nodes to perform smart contracts computation over the private data. And the consensus nodes are the real on-chain nodes, which do not need the trusted hardware. When the compute nodes are attested by the system, which could join the consensus nodes.

To actually achieve the architecture, the paper specified the protocol details, which specifically told how the each part of the systems works. And also the paper give out the security proof with math to prove the the quality of the system in theory.

What's more, they do not just implement the system, in the implementation, they used a lot of mechanism to improve the performance of system by reducing the number of round tips, storage capacity from blockchain and the work for the compute node, such as write-ahead log, caching intermediate state at the enclave, batching transactions off-chain and coordinating the choice of compute nodes.

Furthermore, to give more convinsed experimental result, the paper presented revaluation results for end-to-end latency and throughput in 5 example applications.

E. Remaining Questions

The main problem for Ekiden is the trusted execution environments part. On the one hand, TEE is kind of violate the aim of blockchain, as the decentralized system, the one of the best advantage is there is no need for a trusted party. However, in this design, all the premise is under the trusted hardware. What if the hardware becomes bad, this could always be a concern for Ekiden. On the other hand, even assuming we could definitely trust the hardware, the system need to be update frequently to fit the hardware. What's worse, if the hardware is facing elimination, the system need to find a new carrier or die out with the hardware, which restricts the scalability of the system a lot.

II. Summary of Paper [2]

A. Problem Statement

Bitcoin is a successful decentralized digital currency because its security and efficiency, while there are always some privacy or confidentiality concern for bitcoin. Although the payments of bitcoin are conducted between pseudonyms, it is possible that anyone could de-anonymize it by the joint control of different address [3]. However, the privacy is very important for a cryptocurrency and other distributed storage system such as the financial, legal and healthcare area, so it is essential to propose an approach to give not only bitcoin but all the project based on the blockchain a better future. And this paper proposed zk-SNARKs which could solve this problem and implemented it in a efficient way.

B. Problem Significance

This paper is very meaningful. Because this paper applied a new approach to solve the privacy problem on the blockchain and give it new optimization and make it available in practice. In the paper the approach is different from the traditional approach which focus on the anonymous bitcoin itself, instead, zk-SNARKs try obfuscating the transaction history by mixes.

However, there are three limitation for mixes. First is to realize mix, there will be a long delay for accumulating the transactions. What's more, the mix operator could trace and even steal the coins. As a result, to protect their privacy, there is need for an instant, risk-free and automatic-guarantee anonymous system. And the zk-SNARKs just meet all the requirement.

C. State of the Art

Before this paper, to solve the traditional problems of the mixes the researchers proposed decentralized mix, where no central bank for avoiding the double spending. For implementation, they proposed the zerocoin, which applied zero-knowledge proofs to prevent transaction. In detail, Zerocoin authenticates coins by proving. However, as a decentralized mix, there are many problem still not solved.

First is the performance problem. The cost for Zerocoin is higher than bitcoin by orders of magnitude because of proving process. Second problem is the functionality. The functions for anonymous payments of Zerocoin are not complete, such as the flexible denonmication, independent transaction and privacy for matadata of transactions on the network. Just because of these challenge, the privacy problem can not be solve in practice.

D. Contributions

There are three main contributions in this paper. One is the new protocol, zk-SNARKs and the second is the paper proposed a construction of decentralized anoymous payment scheme. The last one is there is one efficient implementation called Zerocash.

zk-SNARKs is Succinct Non-interactive ARguments of Knowledge, which is based on the public key and private key pair with proving and verifying. The detail process is when there is a new input C, the one-time setup phase will generate one proving public key pk, which enable any provers produce a proof F for x in L and one verification public key vk, which enable anyone verifies the proof F without knowing x. And the best part is the whole process is succinct, which means the proof can be verified in linear time.

And with the zk-SNARKs the paper constructed a decentralized anonymous payment scheme. There are six steps including user anonymity with fixed-value coins, compressing the list of commitments, extending coins for direct anonymous payments, sending coins, public outputs and non-malleability. Finally the this DAP scheme could provide both completeness and security.

At last, the paper outlined a concrete implementation of the DAP scheme called Zerochash. The point for the Z-chsh is to optimize the efficiency of zk-SNARKs. The approach is all the necessary cryptographic ingredients are based on SHA256, like commitment schemes, pseudorandom functions and collision-resistant hashing. In detail, they designed a hand-optimized circuit for verifying SHA256 computations first and they use it to construct the relatively small arithmetic circuit C , which verifies all the necessary checks for satisfying the NP statement. After all these optimizations, teh prover runnning time is reduced to a few minutes and the verifier running time is a few milliseconds, which is very acceptable.

E. Remaining Questions

One of the problem is the zk-SNARKs is dependent on the setup phase, which means the zk-SNARKs is not a completely decentralized currencies, because there still is a trusted party to generate the public key pair. This means it is possible that there is a trapdoor for someone. And this will always be a great concern for the Z-cach.

The other remaining question is about the flexibility of its privacy. Although the privacy is very important, there still is the need for the accountability. For example, what if there are criminals using the zerocash or there are some illegal actions on the zerocash and even further, if the zerocash is popular enough, there will also be the need for the system to be auditable. Therefore, it is essential to make the zerocash realize a balance between the accountability and privacy.

The last problem is although the performance of zerocash is acceptable but the prover and verifier running time is still not perfect. Maybe in the future, there are more talented optimization on it to make it efficient and scalable enough in the practice.

References

[1] Ekiden: A platform for confidentiality-preserving, trustworthy, and performant smart contracts. [Online]. Available: https://arxiv.org/pdf/1804.05141.pdf

[2] B.-S. Eli, C. Alessandro, G. Christina, G. Matthew, M. Ian, T. Eran, and V. Madars, "Zerocash:decentralized anonymous payments from bitcoin."

[3] R. Fergal and M. Harrigan, "An analysis of anonymity in the bitcoin system."