Decision Framework and Detailed Analysis on Privacy Preserving Smart Contract Frameworks for Enterprise Blockchain Applications

Misha Abraham
Robert Bosch Engineering and Business Solutions Private Limited
Bangalore, India
Abraham.Misha@in.bosch.com

Krishnan Mohan
Robert Bosch Engineering and Business Solutions Private Limited
Bangalore, India
Krishnan.Mohan@bosch.com

***Abstract*—Blockchains are globally gaining traction and gradually disrupting the traditional transactional eco-systems by eliminating the non-value adding parties in the value chain. Although blockchains enables digital currency transactions, distributed consensus models and provenance, the problem of scalability, security and privacy has to be solved for the blockchains to be utilized in its full potential. Typically all the transactions recorded in blockchain are visible to all the participants. Even though some blockchain frameworks offers private transactions they still lack transactional privacy and confidentiality. Privacy preserving smart contracts is an emerging field which guarantees the privacy of transactions during runtime and ensures confidentiality as well. In this paper we analyze various frameworks and methodologies and propose a systematic way of choosing the right privacy preserving smart contract framework for enterprise needs and requirements.**

***Index Terms*—Blockchain, Smart Contracts, Zero Knowledge Proofs, Multi Party Computation, Trusted Execution Environment.**

I. Introduction

Blockchain technology have changed the way we foresee business [1]. Transactions in today's business is now bound within multiple organizations/systems making it difficult to maintain such complex systems and also to bring in trust using conventional security practices. Blockchain technology acts as a distributed immutable ledger between the parties in a network, offering a single source of truth for the exchanged data.

Introduction of smart contracts by Ethereum foundation [2] have uplifted the blockchain technology to the next level by enabling decentralized applications (dApps). Replication of data and computation across all the nodes brings in availability and fault tolerance to the network. However critical limitations in the existing technology have been a major cause of declining adoption of Blockchain technology by the enterprise world. First, expensive computation of fully replicated smart contracts. It was reported that to add two numbers together one million times, it costs $26.55 [3]. Second, lack of privacy preserving in smart contract execution. Many industries and investors are trying to shift to private blockchain because of this reason sacrificing the resource utilization of public blockchains.

Confidentiality is one of the core characteristics of information security triad (Confidentiality, Integrity, and Availability) and decentralized applications that run on top of Blockchain technology lacks in preserving the confidentiality of blockchain transactions. Researchers have explored both software based approach, such as various zero-knowledge proof systems [4], [5], [6] secure multiparty computation [7], [8], [9] and hardware based approach (Trusted Execution Environment (TEE)) [10], [18], to bring in privacy in the public blockchain technology. Some of the proposals for confidentiality preserving smart contracts interestingly brings in ideas on how to maintain user privacy without affecting the validation process and helps in preserving trust, integrity, availability and confidentiality. Some of these proposals serves as a good breakthrough for the blockchain technology by extending the applicability of blockchain in the field of healthcare, financial etc., where confidentiality of user data is mandatory.

Even though the proposals serves solution for single confidentiality problem, the methods and performance differ in various ways thus behaving differently in various scenarios. It is necessary to understand the advantages and disadvantages of each of the privacy preserving models for selecting the best for enterprise use case. Our paper aims at bringing in a detailed survey of these methods and act as a single source of reference for selecting suitable privacy preserving model for the smart contracts based on enterprise use case.

This paper consists of the following sections. Section II briefly describes the background study done. Section III describes the problem statement formally. Section IV explains in detail on the Literature Survey done on different existing privacy preserving techniques. This section also brings in technical advantages and disadvantages of each of these techniques. Section V introduces the methodology proposed to choose the right privacy preserving framework based on the business need. Section VI include the comparison of software and hardware based privacy preserving frameworks like Ekiden, Enigma, Hawk and Bulletproof. We have identified key

978-1-7281-6371-0/20/$31.00 ©2020 IEEE

parameters like performance, Integrity, confidentiality etc for the comparison. This section also classifies these frameworks based on their applicability in a typical data flow model as shown in figure 6. Section VII concludes the paper by giving a brief summary on the work done.

II. Background Study

A. Blockchain and Smart Contracts

A blockchain is a decentralized, distributed ledger [11] that stores updated record of transactions in all the nodes. The valid transaction's are grouped together and they form a block in a blockchain. Each block is linked to the previous block in the blockchain using cryptographic algorithms [12]. Second generation blockchain applications introduced the concept of smart contracts which have predefined conditions, so they can automatically trigger actions if these conditions are fulfilled. They form the basic structure for the performance of contracts from participant to participant [13]. Smart contract can be written in languages like go, java, solidity etc., out of which solidity [14] is the most commonly used language.

B. Trusted Execution Environments (TEE)

Trusted Execution Environment provides a fully isolated runtime environment. It maintains the integrity of a code or an application running in the TEE by restricting the access of other software applications and operating systems. Intel Software Guard eXtensions (SGX) [15], [16] is an example of trusted execution environment. TEE's neither guarantees the availability of data nor it can provide persistent storage. But with TEE, one can build confidentiality of applications and algorithms during runtime. The convergence of blockchain technology and TEE can bring in availability, persistence, privacy and confidentiality as shown in Table I.

TABLE I
Blockchain V/S Trusted Execution Environment

Features\Technology	Blockchain	TEE
Integrity	Strong	Strong
Availability	Strong	Weak
Persistence	Strong	Weak
Confidentiality	×	Strong
Transactional Privacy	×	Strong
Runtime Security	Weak	Strong

C. Secure Multi Party Computation

Multi Party computation also known as privacy preserving computation aims at jointly computing a function with an input while maintaining the privacy of the user input [17]. Cryptographic algorithms like Zero knowledge proof, homomorphic encryption is the base for multi party computations and aims in bringing in privacy in computation within multiple parties. Table II shows the features that blockchain technology and multi party computation algorithms (cryptographic algorithms) brings and thus proving the effectiveness of converging both the technologies.

TABLE II
Blockchain V/S Cryptographic Algorithms

Features\Technology	Blockchain	Cryptographic Algorithms
Integrity	Strong	Strong
Availability	Strong	Not Applicable
Persistence	Strong	Not Applicable
Confidentiality	×	Strong

D. Privacy Preservation in Smart Contracts

Hardware based solutions and software based solutions are the broader classification of privacy preserving methodologies as shown in figure 1. Software based solutions mainly include cryptographic techniques like Zero knowledge proof, homomorphic encryption, multi part computation etc. Hardware based solutions is achieved by using trusted execution environments. Our analysis brings in a comparison of methodologies under these categories and a proposed framework to select right framework for the enterprise blockchain use case.

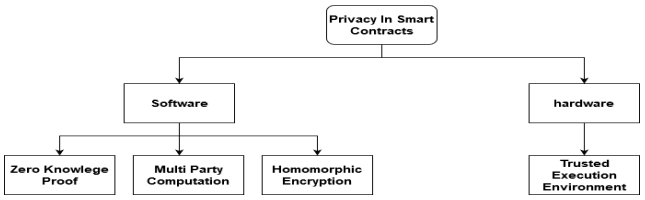

Fig. 1. Privacy in Smart Contracts.

III. Problem Statement

Smart Contract transactions are not confidential by default. Everyone can access and see all information that is sent to and stored in blockchain. Majority of the enterprise grade solutions need data privacy, confidentiality and security of the transactions. This increased the need of bringing privacy preserving smart contracts without compromising the blockchain features. Many researchers and developers are now exploring on TEE's and cryptographic algorithms that could bring in confidentiality and privacy in smart contracts. Even though we could achieve privacy and confidentiality of transactions many of these frameworks have adoption and implementation overheads. Businesses adopting these techniques needs to be well informed on the advantages, disadvantages and the overheads. Our paper aims at bringing in such a detailed report on the comparison of privacy preserving frameworks like Ekiden [18], Enigma [19], BulletProof [20], Hawk [4] and also propose a methodology to select the right privacy preserving framework based on the business requirement.

IV. Literature Survey

In this section we explain in detail about the different projects and architectures available for privacy preservation of smart contracts.

A. Ekiden

Ekiden is a hardware based protocol that aims at bringing two main characteristics to smart contracts in blockchain which are :

- Scalability
- Confidentiality

The main focus of the protocol is to develop a trusted platform for blockchain using Trusted Execution Environments (TEE). Ekiden architecture separates out the computation from consensus. The computation is performed in Intel Software-Guard eXtensions (SGX) which provides a CPU based TEE implementation known as enclaves. Apart from integrity and confidentiality SGX can also provide proofs for correctness of computation.

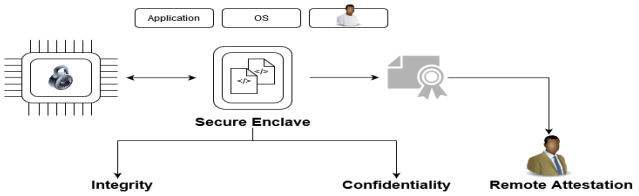

Fig. 2. Workflow of Ekiden [18]

Figure 2 shows the workflow of Ekiden protocol. When data from a secure enclave moves to memory, encryption of data is performed with keys that are known only to the processor. Thus applications, operating systems and other users are separated out from enclaves memory and cannot access the same. The encryption engine of SGX thus guarantees integrity and confidentiality. SGX also issues an attested document over the execution output of the code along with the code which acts as a digital signature and helps remote users to establish a trusted channel (authenticated and encrypted) to the hardware.

TABLE III
ADVANTAGES AND DISADVANTAGES OF EKIDEN PROTOCOL

Advantages	**Remarks**
Computation Correctness	Remote Attestation
Existentially Unforgeable Attestation	Digital Signature with private keys known only to hardware
Scalability	Anyone with a TEE-enabled platform can participate as a compute node
Confidentiality	Secure Enclave

Disadvantages	**Remarks**
Side Channel Attack [21]	This attack can compromise the entire functionality and guarantees provided by Ekiden.
Contract level leakage	Leakage of data is possible through covert channels, bugs or side channels.
Weak Key Management	Current key management is viable to many attacks and the paper acknowledges this fact.

Table III lists some of the technical advantages and disadvantages of the Ekiden protocol. The protocol was tested in a network consisting of 4 consensus nodes and one compute node. As of our understanding the evaluation does not guarantee the results for large scale blockchain networks.

B. Enigma

Enigma is a decentralized computation platform capable of preserving privacy. Computations of the system are performed both in the blockchain and also in Enigma. Blockchain handles computation of public data and ensures correctness of the execution. Whereas enigma handles computation of transactions which requires privacy and and ensures both privacy and correctness of the execution. The proof of execution is stored in the blockchain and can be validated by participant in the network. Figure 3 shows the code execution of the model. Some of the technical advantages and disadvantages of the protocol is listed in table IV respectively.

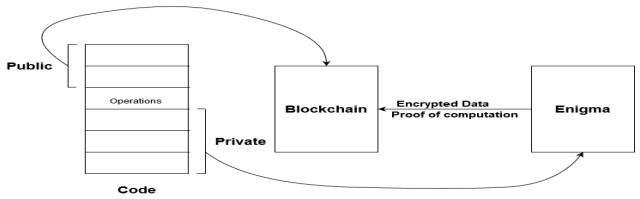

Fig. 3. Enigma code execution model [19]

TABLE IV
ADVANTAGES AND DISADVANTAGES OF ENIGMA PROTOCOL

Advantages	**Remarks**
Autonomous control of personal data.	Secure Multi Party Computation
Privacy	Secret Sharing & Off-chain storage
Scalability	Computation on different parts of the data is performed by a small subset of nodes in the network.
Open Source	The project is openly available and have good tutorials for the developers to start with.
Correctness in Computation	Using SPDZ [22] (pronounced speedz) algorithm the protocol brings in a method to compute correctness in execution.

Disadvantages	**Remarks**
Performance	The protocol is slower because of cryptographic computation and on-chain, off-chain operations
Reversible Transactions	Off-chain transactions does not guarantee irreversible transactions
Third Party requirement	Off-chain transactions are manage by a third party
Evaluation	Proper Evaluation results is missing in the white paper

C. BulletProof

Bulletproofs are zero knowledge proofs to build confidentiality in a non trusted setup. This protocol leverages the non-interactive zero knowledge using the FiatShamir heuristic concept to build very short proofs. Bulletproofs is known to work efficiently in the field of range proofs : to prove that a committed value is within a range, which makes it well suited for trustless characteristics of blockchain and distributed systems. A framework for multi asset transactions was build, known as Cloak Protocol, based on Bulletproofs. The full implementation of the cloak protocol in Rust is available in

[23] and is known as SpaceSuit. Starlight payment-channel protocol [24] developed for the Stellar network is similar to bulletproof system where they aim to bring in optimized range proofs mechanisms. Table V list some of the technical advantages and disadvantages of the protocol.

TABLE V
ADVANTAGES AND DISADVANTAGES OF BULLETPROOF PROTOCOL

Advantages	Remarks
Aggregation of Proofs	Prove 'm' commitments lie in a certain interval in O(log(m)) time.
Applicability in blockchain	Well suited for trustless characteristics of blockchain and distributed systems.
Modified FiatShamir heuristic concept	Modification for the inner-product argument in FiatShamir heuristic concept helped in reducing the communications by a factor of 3.
Non trusted Setup	The Proofs can be used to build confidentiality in a non trusted setup.

Disadvantages	Remarks
Performance	Cryptographical algorithms and mathematical proofs relatively takes more time to achieve privacy when compared to Hardware based solutions like Ekiden.
Restricted to Range Proof	The proofs can be used only to check if a committed value lie in a certain interval.

D. Hawk

Hawk is a framework developed to bring in privacy in smart contracts. Similar to Enigma protocol a Hawk program is separated out into two sections: one containing private details and the other containing public details as shown in figure 4. The private portion helps in maintaining privacy in user data and exchange of money. The public portion does not deal with confidential data or money. Table VI list some of the technical advantages and disadvantages og the protocol. Cryptographic

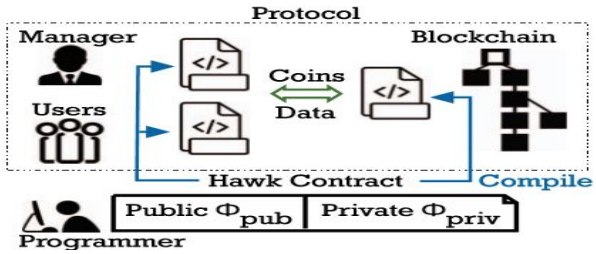

Fig. 4. Workflow of Hawk [4]

protocols between users, the manager, and the blockchain is defined but combining different modules of the Hawk program generated by the Hawk compiler. The modules generated by the compiler are as follows:

- blockchain program : executed by all the consensus nodes
- User program : executed by the users and
- Manager Program : executed by manager.

TABLE VI
ADVANTAGES AND DISADVANTAGES OF HAWK PROTOCOL

Advantages	Remarks
On-Chain Privacy	Transactional privacy is provided against the public.
Contractual Security	Protects parties in the contractual agreement from each other.

Disadvantages	Remarks
Trusted Third Party Requirement	The manager can see the users' inputs and is trusted not to disclose users' private data

V. PROPOSED METHODOLOGY

In this section we explain in detail our proposed methodology to select the right privacy preserving framework based on enterprise needs and requirement. Figure 5 shows the decision flowchart which can be used by developers, researchers and business owners to question themselves and arrive at the right privacy preserving framework for their usecases.

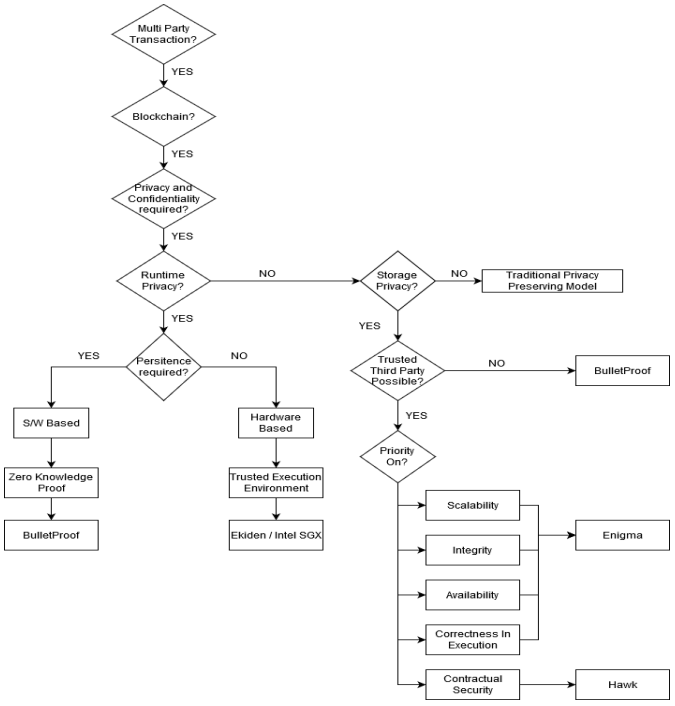

Fig. 5. Proposed Methodology to select privacy preserving model

VI. ANALYSIS AND RESULTS

A. Hardware V/S Software Approach

This section showcase the performance related comparison of hardware based and software based technologies used to preserve privacy in smart contracts.

In table VII some of software techniques like secure multi party computation, zero knowledge proof, homomorphic encryption etc is compared to the hardware based methodologies to preserve privacy in smart contracts. The comparison is performed based on the performance and also a brief description on the security mechanisms used is also mentioned.

TABLE VII
BLOCKCHAIN V/S CRYPTOGRAPHIC ALGORITHMS

	Performance	Security Mechanisms
Secure Hardware	● ● ●	Secure Enclaves
Secure Multi Party Computation	● ○ ○	Cryptography, Distributed Trust
Zero Knowledge Proof	● ○ ○	Cryptography, Local Computation
Fully homomorphic encryption	● ○ ○	Cryptography

B. Comparison of existing privacy preserving smart contract frameworks

For our analysis we have chosen four known privacy preserving frameworks namely Ekiden, Enigma, BulletProof and Hawk. Ekiden is a hardware based technique using Trusted Execution Environment to bring in privacy in computation while others are software based techniques. We have compared these techniques as shown in table VIII based on some of the parameters as mentioned below:

- **P1.** **Integrity** : Keeping data accurate and intact for the entirety of its existence.
- **P2.** **Availability** : Data is always available to all the members of the network.
- **P3.** **Privacy** : Protecting data from unauthorized access.
- **P4.** **Persistence** : Data available permanently.
- **P5.** **Performance** : Speed at which the technique can generate and verify proofs.
- **P6.** **Correctness in execution** : Ability to prove the correctness of execution.
- **P7.** **Scalability** : Ability to scale up the number of participants in the blockchain network.

C. Data Flow Model Based classification

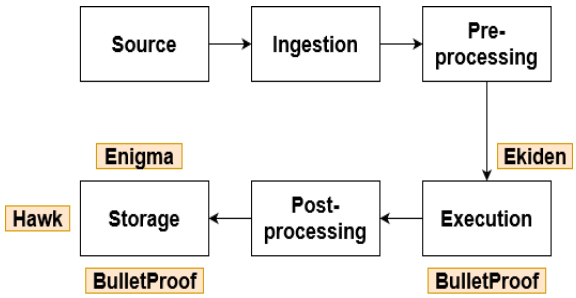

Fig. 6. Applicability of privacy preserving techniques in a typical data flow model.

This section aims at bringing the classification of the techniques based on the stages in a data flow model in which it provides privacy. Figure 6 shows the different stages in a data flow model and the the techniques are marked correspondingly indicating the stages in which they concentrate and tries to bring in privacy. Ekiden tries to bring in privacy during the computation and come up methodologies to prove the correctness of computation. Enigma and Hawk bring aims at bringing in privacy at the stage of storage. Both the protocols handles private data and public data separately to bring in confidentiality for user information.

VII. SUMMARY

Privacy preservation in smart contracts is one of the exciting research areas of cryptography. The techniques analyzed here require lots of effort to implement these in the right way. In this paper we studied various privacy preserving techniques available in blockchain. Our proposed methodology helps to carefully choose the right framework for achieving privacy and confidentiality while being informed about the trade-offs of these frameworks / techniques. There is much to be done on optimizing these techniques and it will be exciting to see the breakthroughs which are about to happen in this field. Many of these discussed frameworks are invented only a few year ago and yet to be tested in a large scale deployments. We firmly believe with blockchains getting adopted very rapidly privacy becomes an integral part of design of blockchain projects.

VIII. ACKNOWLEDGEMENT

We want to thank Sri Krishnan V, Mohan B V, Manojkumar Parmar, Himajit Aithal, Saha Dilip from Robert Bosch Engineering and Business Solutions Private Limited, India for their valuable comments, contributions and continued support. We are also grateful to all the opensource contributors and researchers advancing the research and implementation of the privacy preserving frameworks.

REFERENCES

[1] "How Will Blockchain Change the Way Organizations Work?", https://digitalmarketinginstitute.com/blog/how-will-blockchain-change-the-way-organizations-work. Accessed: 2020-2-26.
[2] Ethereum Foundation, "Ethereum: Blockchain App Platform", https://www.ethereum.org/. Accessed: 2020-2-28.
[3] "What is Ethereum Gas",https://blockgeeks.com/guides/ethereum-gas/.
[4] Kosba, Ahmed, Andrew Miller, Elaine Shi, Zikai Wen, and Charalampos Papamanthou. "Hawk: The blockchain model of cryptography and privacy-preserving smart contracts." In 2016 IEEE symposium on security and privacy (SP), pp. 839-858. IEEE, 2016.
[5] Al-Bassam, Mustafa, et al. "Chainspace: A sharded smart contracts platform." arXiv preprint arXiv:1708.03778 (2017).
[6] Sasson, Eli Ben, Alessandro Chiesa, Christina Garman, Matthew Green, Ian Miers, Eran Tromer, and Madars Virza. "Zerocash: Decentralized anonymous payments from bitcoin." In 2014 IEEE Symposium on Security and Privacy, pp. 459-474. IEEE, 2014.
[7] Zyskind, Guy, and Oz Nathan. "Decentralizing privacy: Using blockchain to protect personal data." In 2015 IEEE Security and Privacy Workshops, pp. 180-184. IEEE, 2015.
[8] Andrychowicz, Marcin, Stefan Dziembowski, Daniel Malinowski, and Lukasz Mazurek. "Secure multiparty computations on bitcoin." In 2014 IEEE Symposium on Security and Privacy, pp. 443-458. IEEE, 2014.
[9] Lindell, Yehida. "Secure multiparty computation for privacy preserving data mining." In Encyclopedia of Data Warehousing and Mining, pp. 1005-1009. IGI Global, 2005.
[10] Bentov, Iddo, Yan Ji, Fan Zhang, Lorenz Breidenbach, Philip Daian, and Ari Juels. "Tesseract: Real-time cryptocurrency exchange using trusted hardware." In Proceedings of the 2019 ACM SIGSAC Conference on Computer and Communications Security, pp. 1521-1538. 2019.
[11] Crosby, Michael, Pradan Pattanayak, Sanjeev Verma, and Vignesh Kalyanaraman. "Blockchain technology: Beyond bitcoin." Applied Innovation 2, no. 6-10 (2016): 71.
[12] Singh, Sachchidanand, and Nirmala Singh. "Blockchain: Future of financial and cyber security." In 2016 2nd international conference on contemporary computing and informatics (IC3I), pp. 463-467. IEEE, 2016.

TABLE VIII
COMPARISON OF PRIVACY PRESERVING METHODOLOGIES

	Ekiden	**Enigma**	**BulletProof**	**Hawk**
Parameters	Hardware	Software	Software	Software
P1. Integrity	Yes Using Intel Software Guard eXtensions (SGX) Enclaves	Yes By storing the private data off-chain Enigma maintains integrity of confidential user data	No The protocol aims at bringing range proof algorithm but not integrity. But when used along with blockchain can bring in integrity	No The private data is maintained by trusted party called manager. Dishonestful manager can modify the data without users knowledge.
P2. Availability	No The computations are performed in a hardware enclave and until the data is stored in blockchain its not available to the users.	Yes Private and public data is stored correspondingly off-chain and on-chain and is available to authorised users all the time.	Yes The cryptographical computations performed does not restrict the users from accessing data.	No Some of the confidential data is managed by third party and is not available to all the users.
P3. Privacy	Yes Using Intel Software Guard eXtensions (SGX) Enclaves	Yes Store confidential data off-chain	Yes Capable of bringing confidentiality in financial applications using range proof algorithms.	Yes Store Private separately and is managed by a trusted third party.
P4. Persistence	No If the hardware gets powered off all the data is lost.	Yes Data is stored in blockchain.	Yes The computations are performed by nodes in the network and stored in blockchain.	Yes Data is stored in blockchain.
P5. Performance	High 600 times increased throughput found during evaluation.	Low Uses cryptographic techniques to generate proof.	Low Uses cryptographic techniques to generate proof.	Low Uses cryptographic techniques to generate proof.
P6. Correctness in Execution	Yes Computations are performed in Trusted Execution Environment.	Yes Using SPDZ (pronounced speedz) algorithm the protocol brings in a method to compute correctness in execution.	No	No
P7. Scalability	Yes Anyone with a TEE-enabled platform can participate as a compute node.	Yes Computations on different part of the data is performed by a small subset of nodes in the network.	No	No

[13] "Blockchain technology explained", https://www.bosch.com/stories/blockchain-technology-explained/. Accessed: 2020-5-19.

[14] Parizi, Reza M., and Ali Dehghantanha. "Smart contract programming languages on blockchains: An empirical evaluation of usability and security." In International Conference on Blockchain, pp. 75-91. Springer, Cham, 2018.

[15] Ding, Yu, Ran Duan, Long Li, Yueqiang Cheng, Yulong Zhang, Tanghui Chen, Tao Wei, and Huibo Wang. "POSTER: Rust SGX SDK: towards memory safety in intel SGX enclave." In Proceedings of the 2017 ACM SIGSAC Conference on Computer and Communications Security, pp. 2491-2493. 2017.

[16] "Intel Software Guard Extensions", https://software.intel.com/en-us/sgx. Accessed : 2020-2-28.

[17] "Secure multi-party computation", https://en.wikipedia.org/wiki/Secure_multi-party_computation. Accessed : Accessed: 2020-2-27.

[18] Cheng, Raymond, Fan Zhang, Jernej Kos, Warren He, Nicholas Hynes, Noah Johnson, Ari Juels, Andrew Miller, and Dawn Song. "Ekiden: A platform for confidentiality-preserving, trustworthy, and performant smart contract execution." arXiv preprint arXiv:1804.05141 (2018).

[19] Zyskind, Guy, Oz Nathan, and Alex Pentland. "Enigma: Decentralized computation platform with guaranteed privacy." arXiv preprint arXiv:1506.03471 (2015).

[20] Bünz, Benedikt, Jonathan Bootle, Dan Boneh, Andrew Poelstra, Pieter Wuille, and Greg Maxwell. "Bulletproofs: Short proofs for confidential transactions and more." In 2018 IEEE Symposium on Security and Privacy (SP), pp. 315-334. IEEE, 2018.

[21] "Side-channel attack", https://en.wikipedia.org/wiki/Side-channel_attack. Accessed: 2020-2-27.

[22] Damgård, Ivan, Marcel Keller, Enrique Larraia, Valerio Pastro, Peter Scholl, and Nigel P. Smart. "Practical covertly secure MPC for dishonest majority–or: breaking the SPDZ limits." In European Symposium on Research in Computer Security, pp. 1-18. Springer, Berlin, Heidelberg, 2013.

[23] "Spacesuit: Interstellar's implementation of cloaked transactions". https://github.com/stellar/slingshot/tree/main/spacesuit. Accessed: 2020-2-27.

[24] "Starlight: Payment channels on Stellar", https://medium.com/interstellar/starlight-payment-channels-on-stellar-3ff833c0d0ca. Accessed: 2020-2-27.