


TAL TECH

 blockchain.taltech.ee

ADVANCED MODULE ON SMART CONTRACTS

27.03.2019

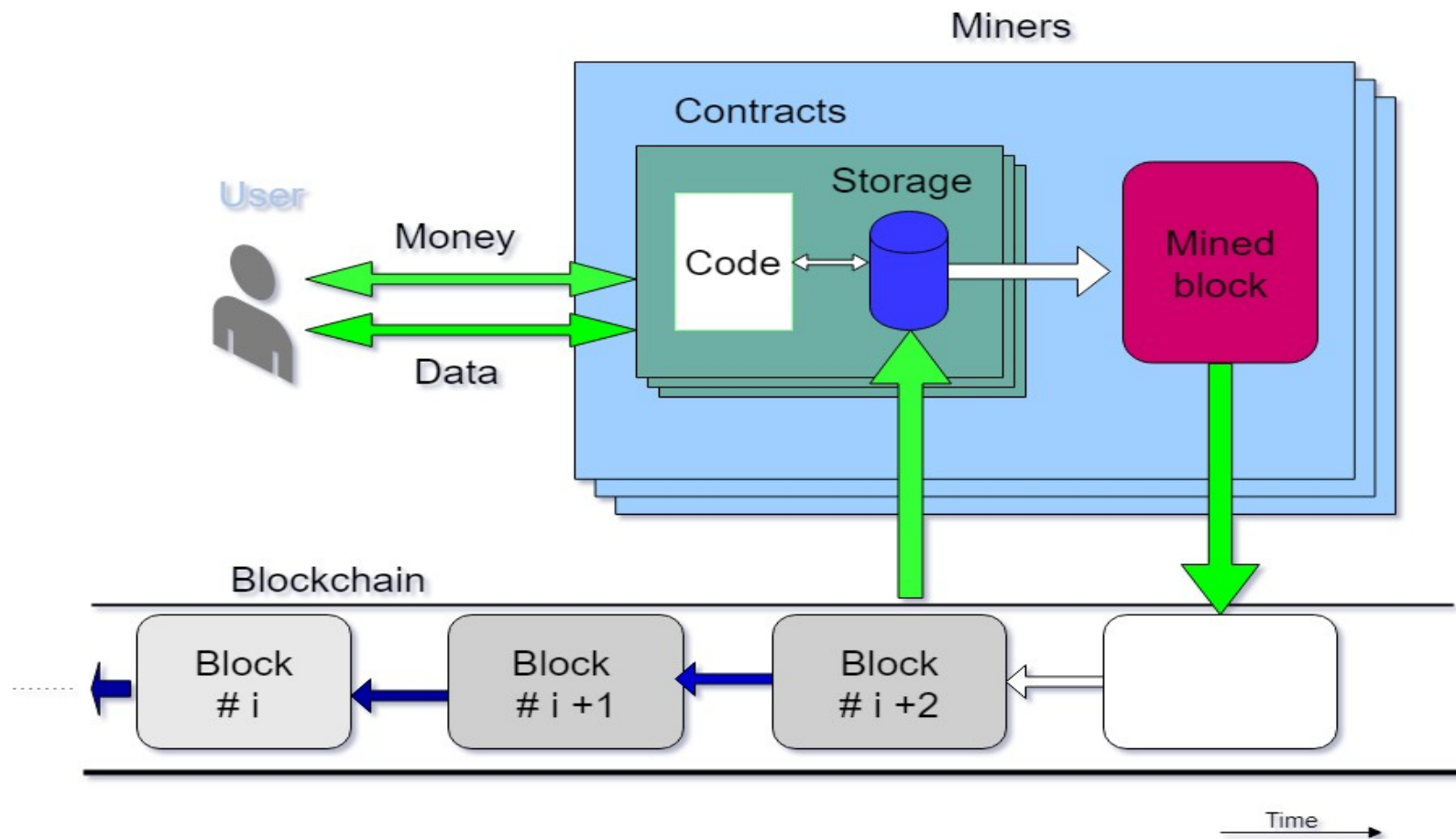
AGENDA

- INTRODUCTION AND STATE OF THE ART OF SMART CONTRACT USAGE
- PROBLEMS WITH HEAVY SMART CONTRACTS AND POW CONSENSUS
- DESIGN OF POS AND LIGHT WEIGHT SMART CONTRACTS SYSTEM FOR MOBILE USAGE

Introduction

- ❖ The blockchain is a distributed Ledger that stores smart contracts on a decentralized peer-to-peer network.
- ❖ Blockchain 2.0 supports smart contracts.
- ❖ A smart contract is a self-executable and self-enforceable computer program that starts executing after deployment on the blockchain.
- ❖ To deploy a smart contract on the blockchain, a consensus mechanism is required.
- ❖ The consensus mechanisms are protocols that make sure all nodes are synchronized with each other and agree on which transactions are legitimate and are added to the blockchain.
- ❖ The most popular consensus mechanisms are proof-of-work (PoW) and proof-of-stake (PoS).

Introduction



State of the Art

- ❖ Increasing adoption of smart contracts has raised concerns about their ability to scale. Many studies have been done to analyze fundamental and circumstantial bottleneck on the network and suggest solutions like reparameterization of block size [1].
- ❖ Vukolic compares the Proof-of-Work (PoW), and Byzantine Fault Tolerance (BFT) based protocols where PoW- based blockchain offers good node scalability with poor performance, whereas BFT-based blockchain provides better performance for small numbers of replicas, with not-well explored and intuitively very limited scalability [2].
- ❖ Loi Luu also proposes a secure sharding protocol for PoW based blockchain called ELASTICO to achieve the linear scalability [3].
- ❖ While improving the scalability of the blockchain systems, security is a major concern. OmniLedger: a scale-out secure protocol using PoW consensus algorithm [4].
- ❖ For scaling a blockchain, it is not necessary to compromise with security and decentralization if properties of value-transfer are fully explored [5].

State of the Art

- ❖ Bentov gives the protocol without PoW to avoid wasting of physical scarce resources. The pure PoS cryptocurrencies deteriorate when enough stakeholders wish to collude in an attack [6].
- ❖ Borge discusses the disadvantages of the Pow and PoS as PoW leads to massive amounts of wasted electricity and re-centralization, whereas major stakeholders in PoS might be able to create a monopoly. Thus proposes a new consensus algorithm called Proof-of-Personhood [7].
- ❖ The PoW method is uneconomical, and a few people can easily monopolize the PoS method. To cope with this issue, this paper introduces a Proof-of-Probability (PoP) method. The PoP is a method where each node sorts the encrypted actual hash as well as a number of fake hash, and then the first node to decrypt actual hash creates block [8].
- ❖ While Hashcash has been successfully adopted in both Bitcoin and Ethereum, it has attracted significant and harsh criticism due to its massive waste of electricity, and in PoS, a miner's chance of adding the next block is proportional to her current balance which can in the worst case lead to an oligopoly. In this paper, we propose Hybrid Mining: a new mining protocol that combines solving useful real-world problems with Hashcash [9].

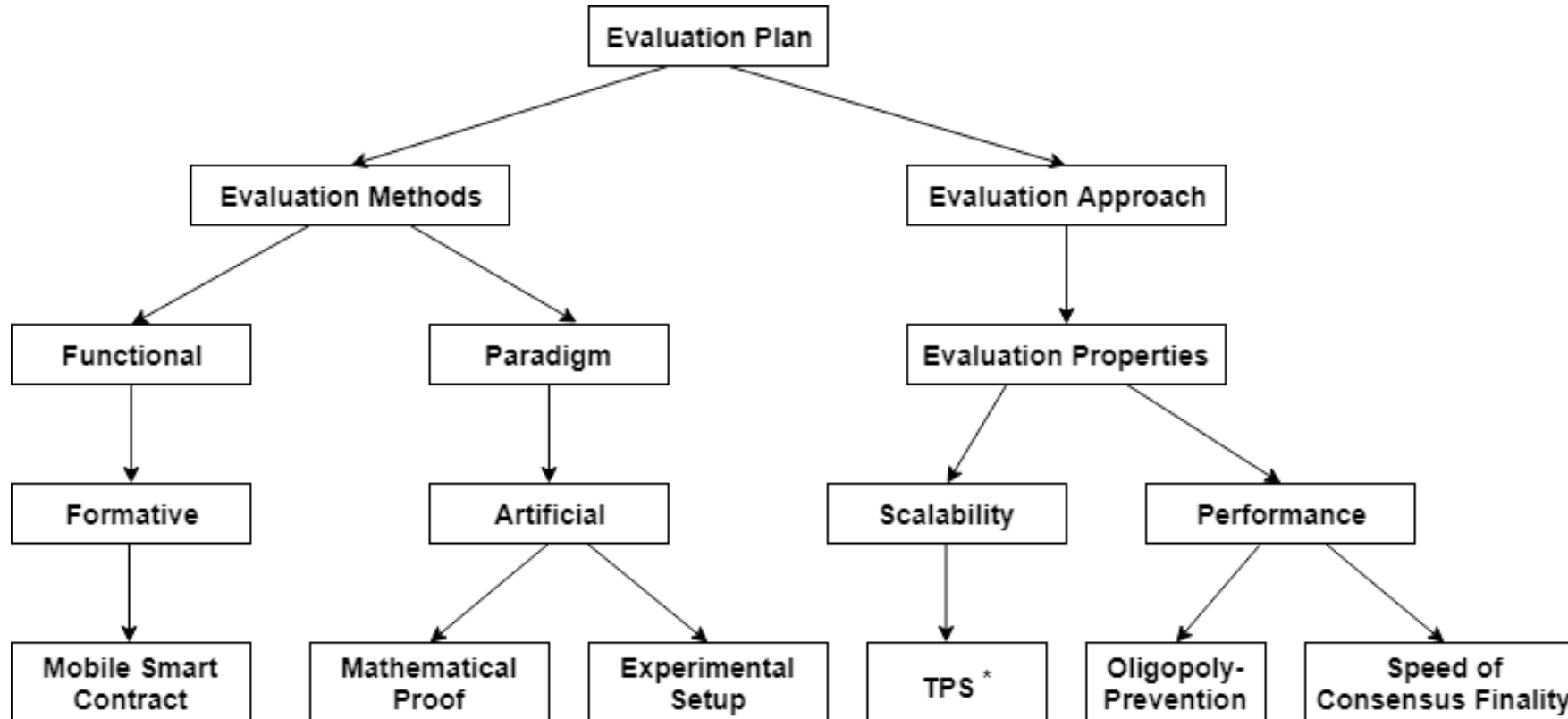
PROBLEMS

- ❖ Thus, state of the art shows that the current blockchain solutions are very heavy in size and computation; therefore, the latter can't be download and compute on mobile devices.
- ❖ Also, from the available consensus algorithms, the proof-of-stake (PoS) algorithm is better; however, the PoS algorithm leads to an oligopoly, where the set of nodes have complete control over the network. Oligopoly happens due to the absence of a mechanism to utilize the stakes in the PoS algorithm.

OBJECTIVES FOR MOBILE SMART CONTRACTS

- ❖ To fill this gap, we develop the mobile smart contracts lifecycle that democratizes the incentivized proof-of-stake consensus algorithm and thus enhances the scalability of the smart contracts.
- ❖ Also, we improve the proof-of-stake algorithm to prevent the oligopoly-formation in the network, thus increases the performance of the network and also increases the consensus finality.

EVALUATION PLANS FOR MOBILE SMART CONTRACTS



EVALUATION PLANS FOR MOBILE SMART CONTRACTS

- **Goal:** Emphasize on the consensus of the nodes in the mobile computing environment.
- **Environment:** Being a socio-technical system, the mobile smart contract is evaluated and analyzed as per consistency and harmony with people, organization, and technology
- **Structure:** In this dimension, we evaluated the mobile smart-contract lifecycle with the following criteria: completeness, transparency, clarity, level of details, consistency and readiness to change.
- **Activity:** This evaluation dimension is characterized by accuracy, performance, and efficiency
- **Evolution:** Finally, we evaluate our system by evolution capability based on the criteria of robustness.

REFERENCES

1. Kyle Croman, "On Scaling Decentralized Blockchains", International Financial Cryptography Association 2016, LNCS 9604, pp. 106-125, 2016.
2. Marko Vukolic, "The Quest for Scalable Blockchain Fabric: Proof-of-Work vs. BFT Replication", IFIP, LNCS 9591, pp. 112-125, 2016.
3. Loi Luu, "A Secure Sharding Protocol For Open Blockchains", ACM CCS'16, 2016.
4. Kokoris-Kogias, "OmniLedger: A Secure, Scale-Out, Decentralized Ledger via Sharding", IEEE Symposium on Security and Privacy 2018.
5. Zhijie Ren, "A Scale-out Blockchain for Value Transfer with Spontaneous Sharding", IEEE Crypto Valley Conference on Blockchain Technology 2018.
6. Iddo Bentov, "Cryptocurrencies Without Proof-of-Work", FC 2016 Workshop, LNCS 9604, 2016.
7. Maria Borge, "Proof-of-Personhood: Redemocratizing Permissionless Cryptocurrencies", IEEE European Symposium on Security and Privacy Workshops, 2017.
8. Sungmin Kim, "POSTER: Mining with Proof-of-Probability in Blockchain", ACN ASIA CCS-2018.
9. [Krishnendu Chatterjee](#), "Hybrid mining: exploiting blockchain's computational power for distributed problem solving", [SAC '19](#) Proceedings of the 34th ACM/SIGAPP Symposium on Applied Computing, 2019.