**Arbitrum: Scalable, private smart contracts**

Harry Kalodner, Steven Goldfeder, Xiaoqi Chen, S. Matthew Weinberg, and Edward W. Felten,  
Princeton University

A S M Nazrul Islam  
1018312016  
Institute of Information and Communication Technology (IICT), BUET

The titled paper presented a cryptocurrency system named ‘Arbitrum’. According to the authors, the proposed and implemented system differentiates itself from other existing systems by resolving the prevailing limitations of scalability and system privacy in supporting smart contracts.

According to the paper, the proposed cryptocurrency system, ‘Arbitrum’ is developed to solve the limitations of scalability, where previously, every miner i.e. verifier is required to emulate every step of execution of every contract for the purpose of verification. And security, where for this aforementioned verification process, the code and data of every contract is required to be public in the prevailing cryptocurrency systems.

Unlike other cryptocurrency systems like- Ethereum, Arbitrum allows parties to implement a smart contract by creating a virtual machine (VM) with the help of a special transaction type that encodes the rules or functionalities of the contract. To incentivize the parties Arbitrum allows off-chain agreement on deciding the functionality of the VM. Which eases the miners i.e. verifiers by needing only to verify the digital signatures to probe the party’s confirmation on VM’s behavior. Even, if the parties fail to reach a unanimous agreement off-chain, Arbitrum gives scope to the honest parties by allowing them to advance the VM state on-chain. And in cases of a party’s spurious statement about a VM’s behavior, using an efficacious protocol named **Bisection protocol** the verifier will be able not only to identify but also to penalize the crafty party. And these very features especially the off-chain verification of the VMs’ has **ensured** and **improved** scalability and security.

To execute this system four types of roles are in action. The **Verifier,** who/which verifies the transactions and publishes the accepted ones. The verifier could be a central global entity or a distributed protocol, as Arbitrum being an agnostic system. A **key,** which can own currency and place transaction is a participant in protocol and identified by the hash of a public key. A virtual machine (**VM)**, like key, can also own currency and can send and receive currency as well as message from and to other VM or party. VM is basically a virtually participant in this system but plays a significant role. Lastly, a **Manager** is a party of a VM, who can monitor the state and progress of a particular VM and can ensure the VM’s correct behavior. A manager can be identified by the hash of its public key.

According to the authors, Arbitrum improves **scalability** by allowing the managers to execute a machine indefinitely for a negligible transaction fee, which is small and independent of the complexity of the code that they are running. It is also stated that, all assertions should be unanimous and free from any kind of dispute, if participants follow incentives. But, even if a dispute occurs, the verifier is able to solve it at a negligible cost to honest party but substantial cost to the dishonest party.

And **privacy** is maintained and improved by zero exposure of internal state of the VM to the verifier. The verifier does not run a VM’s code. Even in case of dispute, the verifier is provided with a single step of the VM’s execution, whereas the vast majority of the VM’s state remains opaque to the verifier.

The above two features assist the managers to choose and to reset a VM to any state that they wish and take any action that they want with the precondition being in a unanimous agreement with all managers. And this optimized the feature **flexibility**.

**Comments**

As a research work, the authors of this paper did an incredible job by exploring this concept rigorously and introducing an optimized one in research area. The introduction and background sections of the paper give well description of the concept and provide a reader an appreciation of the necessity to look on this matter.

To get into the depth of the problem, the authors have studied the prevailing cryptocurrency systems diligently. They probed the prevailing systems like Ethereum to find out the causess of the limitations and what steps should be taken to make the system an efficacious one.

Based on the findings of their study, they identified the factors that could play important roles to ameliorate the prevailing system. Keeping in mind those factors, they proposed, designed and implemented a cryptocurrency system, which ensures scalability, security and flexibility.

The authors of this paper also have studied other proposed solutions for smart contract scalability like- Hawk, Ekiden, TrueBit, Plasma and systems using techniques like Secure Multiparty Computation and State Channels critically and pointed out their shortcomings and compared their systems with the presented one ‘Arbitrum’.

They also stated that ‘Arbitrum’ is - “consensus agnostic and is pluggable with any existing mechanism for achieving consensus over a blockchain”. And, to my view, this paved path for future research.

Overall, this paper has enriched the field of cyber-security by resolving prevailing limitations of a concept that has huge significance today and more impact to make in near future.