A Review of Usability and Security Evaluation Model of Blockchain Technologies

Pallab Banerjee¹, Biresh Kumar², Amarnath Singh³, Harsh Prasad⁴, Bittu Raj⁵

1,2,3 Assistant Professor, Dept. Of Computer Science & Engineering, Amity University, Jharkhand.
⁴,⁵ B.Tech Scholar, Dept. Of Computer Science & Engineering, Amity University, Jharkhand.
Email: pbanerjee@amity.edu

Abstract:

In the modern trends of evolution Blockchain has received extensive attention recently. In the race of digitalization, the world is looking on the technology that can fuel financial transaction significantly. Thus Blockchain provide such types of facilities. As we know, Blockchain is a decentralized peer-to-peer network which was designed in order to remove involvement of third party in transaction. But due to its extensive use on a large scale, there is a huge problem of security and scalability. This paper aims to provide a review of Usability and Security of some of blockchain Technology on different categories: Public, Consortium and Private on different application Model such as Smart contract, Internet of Things and Crypto-currency considering different parameters. This paper basically provides a comparative study and coordination between them. We also expand to provide a typical consensus algorithm comparison which governs the blockchain.

Keywords — Blockchain, Decentralized, Scalability, Usability.

1. Introduction

Blockchain is a open distributed ledger that can permanently record transaction between two parties efficiently in the network and the data in the given blocks cannot be altered without alteration of all subsequent blocks, which requires consensus of the network majority. It consist of a single universal ledger where every block added in linked with the last block which has its own hash value for inter connected network. Current blockchain system are categorized into three types: public blockchain, consortium blockchain and private blockchain. In public blockchain there is no access restrictions, anyone with the network connection can join and participate in the execution of consensus protocol. As, for consortium blockchain is a partial decentralized system which is granted to a group of approved individuals. In case of private blockchain most of the features are similar with public, only with a difference that is known as a permission based system, the block with read and write access are controlled by an entity.

In this paper we focused on some of the important application which is governed by the blockchain, such as Smart contract, Internet of Things and Crypto-currency. We also provide a comparative view on some of the most important consensus algorithms which includes Pow, Pos, Dpos, Ripple, Poa. The majority of researcher are more focused on revealing and improving limitations of blockchain security and privacy but lack on understanding different categories of blockchain and its uses on different applications. We wish to stress that the purpose of our paper is not to define the working principle of blockchain technology nor its consensus algorithms rather to provide a feasible basic comparison between its application and consensus algorithms for understanding its future limitations. We hope that our paper will increase more understanding of problem at stake and motivate further study and research in this field for future development.

2. Briefing

In the table 1 as shown below we did a comparative study and analysis on some of the applications of blockchain as Smart Contract, Internet of Things and Crypto-currency, keeping in mind about its Access Permission, In-commutable, Proficiency, Dominance, Litigation Perspective and Technical Failure. All the factors have different limitations on different platform, i.e. in case of smart contract its...
accessibilities are different on public, consortium or in private mode; same in case of Iot devices or crypto-currency.

<table>
<thead>
<tr>
<th>Property</th>
<th>Public</th>
<th>Consortium</th>
<th>Private</th>
</tr>
</thead>
<tbody>
<tr>
<td>Access Permission</td>
<td>Anyone can access/see or access.</td>
<td>Only selected nodes/people that are allowed to access/see.</td>
<td>Only particular organization can access/see.</td>
</tr>
<tr>
<td>Incomputable</td>
<td>It is not so easy or it may be impossible to tamper.</td>
<td>There is a chance to tamper.</td>
<td>High chances of tampering.</td>
</tr>
<tr>
<td>Proficiency/Efficiency</td>
<td>Not so efficient, but Best in case of (Smart Contract).</td>
<td>Can be efficient but not as compared to public.</td>
<td>As compared to other two not so efficient as it can provide advantage to particular node.</td>
</tr>
<tr>
<td>Dominance/Ownership</td>
<td>Nobody, Everyone has equal rights and Dominance throughout the system.</td>
<td>Multiple nodes/or selected people from the chain.</td>
<td>Single system.</td>
</tr>
<tr>
<td>Litigation Perspective</td>
<td>Is still a challenge, as who will bear the liability for any faults in the technical code and who has the right to enforce against them.</td>
<td>Is still a challenge, as who will bear the liability for any faults in the technical code and who has the right to enforce against them.</td>
<td>People within the system are responsible to bear for any sort of faults.</td>
</tr>
<tr>
<td>Technical Failure</td>
<td>Difficult to tract the bugs in the system if any system failure happens.</td>
<td>Bugs can be trace.</td>
<td>Bugs can be trace.</td>
</tr>
<tr>
<td>Timestamp</td>
<td>Time consuming.</td>
<td>Less time required.</td>
<td>Due to limited or restricted nodes it is very efficient in time consumption.</td>
</tr>
</tbody>
</table>

A smart contract is just a legal digital contract with the security of the consensus protocols governed by blockchain that automatically get executed when the defined terms and conditions of the contract are met successfully without alteration. A Cryptocurrencies are the group of tokens which are used within blockchain networks to send value and pay transactions without the need for a central authorization. When IoT and Blockchain come together, smart devices will be able to exchange data and communicate with one another through a decentralized system of blockchain where there will no longer be any dependence on a centralized authority.

3. Consensus Efficiency:

<table>
<thead>
<tr>
<th>Property</th>
<th>Public</th>
<th>Consortium</th>
<th>Private</th>
</tr>
</thead>
<tbody>
<tr>
<td>Access Permission</td>
<td>Anyone can access/see or access.</td>
<td>Only selected nodes/people that are allowed to access/see.</td>
<td>Only particular organization can access/see.</td>
</tr>
<tr>
<td>Incomputable</td>
<td>It is not so easy or it may be impossible to tamper.</td>
<td>There is a chance to tamper.</td>
<td>High chances of tampering.</td>
</tr>
<tr>
<td>Proficiency/Efficiency</td>
<td>Not so efficient, but Best in case of (Smart Contract).</td>
<td>Can be efficient but not as compared to public.</td>
<td>As compared to other two not so efficient as it can provide advantage to particular node.</td>
</tr>
<tr>
<td>Dominance/Ownership</td>
<td>Nobody, Everyone has equal rights and Dominance throughout the system.</td>
<td>Multiple nodes/or selected people from the chain.</td>
<td>Single system.</td>
</tr>
<tr>
<td>Litigation Perspective</td>
<td>Is still a challenge, as who will bear the liability for any faults in the technical code and who has the right to enforce against them.</td>
<td>Is still a challenge, as who will bear the liability for any faults in the technical code and who has the right to enforce against them.</td>
<td>People within the system are responsible to bear for any sort of faults.</td>
</tr>
<tr>
<td>Technical Failure</td>
<td>Difficult to tract the bugs in the system if any system failure happens.</td>
<td>Bugs can be trace.</td>
<td>Bugs can be trace.</td>
</tr>
<tr>
<td>Timestamp</td>
<td>Time consuming.</td>
<td>Less time required.</td>
<td>Due to limited or restricted nodes it is very efficient in time consumption.</td>
</tr>
</tbody>
</table>

As we know blockchain is governed by some of the major algorithm and the basic contract for fulfillment of the goal. In this paper we compared these listed popular algorithms and provided a comparative study of its contract in different forms of blockchain as shown in the table 2.

**Statements:**

**Pow:** Proof-of-Work: It is an algorithm which is use to provide the authentication of the data in the network. Its time consuming approach provide difficulty in operation but an easy verification and authentication of the node that is added in the chain.

**Pos:** Proof-of-Stake: Is a low energy consumption consensus algorithm for locking up crypto assets to secure the network which require nodes to purchase or receive the coin and commit it to authenticate the transactions.
Dpos: Delegated-Proof-of-Stake: It is bit similar to Pos only with a difference that its technology is maintained through democratic voting procedure to secure blockchain network. We believe that this paper will open up many research challenges in resource sharing on blockchain and its applications on different platforms.

Acknowledgement

All thanks must be sent to the management of Amity University Jharkhand (AUJ) and its team of Computer Science Department to facilitate accessing the resources used in this study.

References


