CS6290 55323707 Reading Summary 1

Yu SU
Dept. of Computer Science
ID:55323707

I. Summary of Paper [1]

A. Problem statement

The paper mainly demonstrated two aspects of problems.

First, the paper lists many problems that need to solve with the development of the times.

how to maintain the stability of bitcoin*:* Such as stability of transaction validity rules, stability of consensus protocol, stability of mining pools and stability of the peer-to-peer layer.

how to increase the security and privacy of bitcoin*:* For the security part, the main approach is about key management and for the privacy, the key is to improve the anonymity to confront the de-anonymization.

what other functions we could extend*:* Like add the function of atomicity, collateral and auditability to make realize the disintermediation with bitcoin; Or extend it as a data store; Even make the bitcoin's transaction semantics.

Second, to slove above problems, the paper introduced the some novel and appliable technique which could be used in bitcoin or other cryptocurrencies.

basic technical components of bitcoin*:* The technique about transactions and scripts, consensus and mining and peer-to-peer communication network.

varied approach of key management*:* Such as offline storage, air-gapped and hardware storage and hosted wallet.etc

alternative consensus protocols*:* Like parameter changes, alternative computational puzzles, new proof approach proof-of-stake and designed authorities.

B. Problem Significance

It is quite meaningful to research the above problem. There are two reasons.

One one hand, although bitcoin works surprising well, there is no an reliable theory foundation about why it could work well. What's more, we need to know whether it could always work in practice as the practice changes.

On the other hand, there are many extraordinary design in bitcoin, which could been applied in other areas to solve the problems, like its consensus protocol. So it is meaningful to research these approach.

C. State of the Art

The state of art for bitcoin is nearly mature at that time. A lot of good design source is available. And at that time the mining pools have already generated, many kinds of approach of key management have been proposed, bitcoin has encountered both soft and hard forks and varied alternative consensus protocols were proposed. Under the condition of this, the main research orientation of bitcoin at that time is try to maintain the bitcoin works well and try to optimize it in different ways.

There are two reasons why this problem was not solved before the paper. First is before the paper, bitcoin is still in the beginning stage, researchers focused more on whether it could work well, instead of whether it could continuely work well. The other reason is only with a certain amount of previous related accumulation of other researchers, the author could give a accurate perspective analysis.

D. Contributions

This paper has a good summary of the problems that the bitcoin faced and the varied novel technique at that time.

The paper clearly demonstrated most of advanced technique on the bitcoin or cryptocurrencies at that moment, which could help others know this area better and easier.

The extraordinary work is the challenge he figured out on bitcoin at that time is still the main research orientation of cryptocurrencies today, which means this paper exactly seized the research perspectives of bitcoin and cryptocurrencies.

E. Remaining Questions

The main remaining problem is even though we could find the drawback of bitcoin, it is hard to find a better way to improve it as the bitcoin is nearly the first technology succeed in practice without completely theory .

The key of this problem is it is hard to find a way to evaluate if a new cryptocurrency could do better than bitcoin. Because without a lot of practice test, only theory could not assess whether it could be stable under changed economic and social circumstance like bitcoin.

As a result, there is another problem. Similarly, we can not predict if the bitcoin or related other system will work well in the future and it is also hard for researchers to just easily succeed to optimize the cryptocurrencies to make it adapt to the new times, which is dangerous and unreliable.

II. Summary of Paper [2]

A. Problem Statement

The paper could be divided to two parts.

The first part is talking about the blockchain in following aspects.

how blockchains work: Demonstrate the general process of blockchain networks.

the consensus on the network: Introduced proof-of-work, proof-of-stake and also some other solution to solve the Byzantine Generals problem.

how asset transfer work: Use some example to explain the process of asset transfer.

how smart contract work: Introduced the smart contract and how it works on the blockchain.

blockchain taxonomy: Categorize the blockchain network in different ways.

The second part discussed the combination of IoT and blockchain.

advantage for combination of blockchain and IoT:

- Give IoT security through transparency
- Save money for maintain the system
- Billing layer paves the way for a marketplace of service between devices
- Make process completely automatically and efficient

issue about deployment:

- Keep user and transaction privacy
- Solve the problem of blockchain
- Enhance the legal enforceability
- Connect real world
- Solve the problem that caused by complete autonomy

B. Problem Significance

Before the blockchain came out, there are three main problems of Internet of Things, which are security, high expense and low efficiency.

Luckily, blockchain does not need trust party, there is little maintainance expense and run fast. It could just fit the IoT and make up its drawback.

So, research on blochchain and smart contract for the Internet of Things is very meaningful. Not only if the combination of blockchain and IoT is implemented, the IoT will have a better prospect. Even without a excellent end, researching on two kinds of advanced and immature technology is also quite valuable.

C. State of the Art

At that time, the basic technology of blockchain is nearly mature. Researcher focused on solving the privacy problem and try to optimize it in different consensus. And the Internet of Things is at the first stage. Although there are some implementations, there are still some problems not solved such as the security, expense and efficiency problems. As for the combination of Internet of Things and blockchain, the technology is completely new, even after this paper,which is still in the theory stage.

There are two reasons why the problem was not solved before the paper. First is blockchain and IoT are two separated areas. It is hard to figure out the combination of them. Second is only after the accumulation of previous paper work, such as smart contract that is just possible to realize this theory.

D. Contributions

On the one hand, this paper summarize the development situation of blockchain, smart contract and Internet of Things at that time.

On the other hand, the author subtly found the connection between the blockchain and the IoT and make a prospect about the possible trend of development and the issue need to attention on.

This is really an extraordinary work because he could find a technology fitting the requirement so well and give some of the basic theoretical support. If the Internet of Things in blockchain is really applied widely in the future, the value of this paper will be higher.

E. Remaining Questions

As the author said, the combination is only on the stage of theory. There will be a long way from real implementation and there are still lots of problems that can not be solved such as the deployment problem that I have talked in the part A.

Besides the problem about the combination, there are more problems for Internet of Things. Because the IoT includes the problem such as sensor technology, cloud computing and network technology, etc.

What's more, even if it is implemented, the practical result is maybe not as well as the theory, because the theory of blockchain is still not perfect. It is hard for people to predict the result only depending on the existing theory. So whether the combination of blockchain and Internet of Things will work well, we need time to prove.

References

[1] J. Bonneau, A. Miller, J. Clark, A. Narayanan, J. A. Kroll, and E. W. Felten, "Sok: Research perspectives and challenges for bitcoin and cryptocurrencies," 2015.

[2] K. Christidis, M. Devetsikiotis, and K. Christidis, "Blockchains and smart contracts for the internet of things," 2016.