Code 336.743

GENERAL OVERVIEW OF THE BLOCKCHAIN TECHNOLOGY. INVESTIGATION OF ITS SECURITY ISSUES AND ITS PRACTICAL USES

Rahman Mustafayev

Baku Engineering University, Khirdalan city, Hasan Aliyev str., 120 AZ0102, Absheron, Baku, Azerbaijan

Abstract

Blockchain, the foundation of Bitcoin, has received extensive attentions recently. Blockchain serves as an immutable ledger which allows transactions take place in a decentralized manner. Many implementations of blockchain technology are widely available today, each having its particular strength for a specific application domain.

Аннотация

Блокчейн, основа Биткойна, недавно привлекла к себе большое внимание. Блокчейн служит неизменным регистром, который позволяет децентрализованно осуществлять транзакции. Многие реализации технологии блокчейна сегодня широко доступны, каждая из которых имеет свои преимущества для конкретной области применения.

What is Blockchain technology?

"The blockchain is an incorruptible digital ledger of economic transactions that can be programmed to record not just financial transactions but virtually everything of value." [2]

A blockchain is, in the simplest of terms, a time-stamped series of immutable record of data that is managed by cluster of computers not owned by any single entity. Each of these blocks of data (i.e. block) are secured and bound to each other using cryptographic principles (i.e. chain).

So, what is so special about it and why are we saying that it has industry disrupting capabilities?

The blockchain network has no central authority — it is the very definition of a democratized system. Since it is a shared and immutable ledger, the information in it is open for anyone and everyone to see. Hence, anything that is built on the blockchain is by its very nature transparent and everyone involved is accountable for their actions.

The blockchain is a simple yet ingenious way of passing information from A to B in a fully automated and safe manner. One party to a transaction initiates the process by creating a block. This block is verified by thousands, perhaps millions of computers distributed around the net. The verified block is added to a chain, which is stored across the net, creating not just a unique record, but a unique record with a unique history. Falsifying a single record would mean falsifying the entire chain in millions of instances. That is virtually impossible. Bitcoin uses this model for monetary transactions, but it can be deployed in many others ways.

Blockchain technology has been studied by a wide variety of academic disciplines. For example, some researchers have studied the underlying technology of blockchain, such as distributed storage, peer-to-peer networking, cryptography, smart contracts, and consensus algorithms ([1]). Meanwhile, legal researchers are interested in the regulations and laws governing blockchain-related technology [3]

How does blockchain work?

Picture a spreadsheet that is duplicated thousands of times across a network of computers. Then imagine that this network is designed to regularly update this spreadsheet and you have a basic understanding of the blockchain.

Information held on a blockchain exists as a shared — and continually reconciled — database. This is a way of using the network that has obvious benefits. The blockchain database isn't stored in any single location, meaning the records it keeps are truly public and easily verifiable. No centralized version of this information exists for a hacker to corrupt. Hosted by millions of computers simultaneously, its data is accessible to anyone on the internet.

Security issues in blockchain technologies

51% Attacks

In due part to HBO's Silicon Valley, 51% attacks are one of the most recognized blockchain security issues. In a 51% attack, one, or several, malicious entities gain majority control of a blockchain's hash rate. With the majority hash rate, they can reverse transactions to perform double-spends and prevent other miners from confirming blocks. In 2018, several notable cryptocurrencies such as ZenCash, Verge, and Ethereum Classic fell victim to 51% attacks. Overall, attackers walked away with over $20 million last year due to this blockchain security issue. If your blockchain utilizes a Proof-of-Work (PoW) consensus mechanism, you need to have security measures in place to prevent a 51% attack. Being vigilant of mining pools, implementing merged mining on a blockchain with a higher hash rate, or switching to a different consensus mechanism are all viable options. [4]

Social Engineering

Another blockchain security issue that you and your employees should be aware of is social engineering. Social engineering comes in many forms, but the goal is always the same: to obtain your private keys, login information, or more directly, your cryptocurrency. Phishing is one of the most common forms of social engineering. In a phishing attempt, a malicious actor sends you an email, message, or even sets up a website or social media account imitating a company brand you trust. Often, they'll ask that you send over your credentials under the guise of a giveaway or critical issue to force a sense of urgency. If you hand over your information, there's little you can do to stop them from clearing out your account.

Software Flaws

Most of the big-name blockchains (Bitcoin, Ethereum) have proven their resilience to all types of attacks. However, the apps built on top of them are still susceptible to bugs. Last year, software bugs in wallets and decentralized apps (dApps) led to over $24 million in damages. It's important that any software using blockchain technology under the hood undergo rigorous testing and review. This process should include code reviews, penetration testing, and smart contract audits. Additionally, any reputable application should have redundant security measures in place. It's inevitable that a bug or two will slip through the cracks, so you want to be prepared when they do. When using any blockchain-based software, check to see that, at the very least, it's gone through a third-party security audit. Ideally, the code behind it is also open-source so that anyone can go in and review it for flaws or loopholes. Even with those precautions, you should have your own set of security practices in place as many software-level blockchain security issues go undiscovered for years.

Conclusion

As an important emerging technology, blockchain will play a role in many fields. Therefore, I believe that the issues related to commercial applications of blockchain are critical for both academic and social practice. There are several promising research directions. The first important research direction is understanding the mechanisms through which blockchain influences corporate and market efficiency. The second potential research direction is privacy protection and security issues. The third potential research direction is how to deeply integrate blockchain technology and fintech. The blockchain technology will become an increasingly important topic as time goes on.

References

1.Lansiti M, Lakhani KR the truth about Blockchain. Harvard Business Review (2017) Corporate Governance and Blockchains (Yermack 2017)

2.Don & Alex Tapscott, authors Blockchain Revolution (2016).

3.Swan M, Blockchain: Blueprint for a New Economy, O'Reilly Media, Inc. (2015)

4.Ethereum White Paper. A next generation smart contract & decentralized application platform By Vitalik Buterin.