Cover Page

Blockchain Report

Danyil Tymchuk &
Matvii Vasylenko &
Artem Surzhenko

04.12.2023

Personal & Professional Development
Group Project

Table

Introduction (Artem)

Blockchain and Cryptocurrency

(280 words)

Cryptocurrency is a type of digital currency that does not have a physical embodiment and a single center that controls it. It works in the so-called “blockchain” or a chain of blocks with information.

Unlike servers, which are usually located in one place, in a blockchain, data is stored on computers in different parts of the world. The unit of account for a cryptocurrency is a “coin” or “token,” depending on the type of electronic money.

The lack of centralization also has some disadvantages - for example, a bank can freeze money if it suspects that the transfer was made by fraudsters. And transactions with cryptocurrency are irreversible - in which case you will not be able to cancel or dispute the transaction.

Cryptocurrencies have convenient peering functions, which allow users to make exchange transactions with each other directly, bypassing various intermediaries and their commissions (for example, banks).

Another important feature of cryptocurrencies is the increased security of storing and transferring coins. Information about the transaction is known only to its participants, and it will not be possible to withdraw the currency - this will require physical access to the owner’s wallet.

An important distinguishing feature of many electronic money is their limited quantity. This eliminates the possibility of issuing additional currency and protects its value from inflation.

For example, more than 21 million units of Bitcoin, the most famous and expensive digital asset now, cannot exist simultaneously.

Today, virtual currencies are mostly considered not the most reliable way to invest, since their rate is almost impossible to predict, and is often influenced by third-party factors, including the statements of media persons.

How is cryptocurrency different from regular money?

(350 words)

To better understand the structure of cryptocurrencies and how they differ from fiat money, you should first understand the main mechanism of how coins work - the blockchain.

Let's imagine a situation: you decide to transfer 1000 euro to a friend. To do this, you go to your bank's mobile application, and after a few clicks, your friend's account is replenished. In this case, no physical movement of money occurs. The bank simply changes the transfer records in the database. Such databases are usually stored on servers that are in one specific location.

The diagram above shows how the blockchain works:

1.User A sends money to User B.

2.The transaction is “formatted” in the blockchain in the form of a block of information.

3.Each blockchain user receives a notification about the appearance of a new block.

4.Most users approve of adding a block to the chain.

5.The block is added to the chain, in this form it can no longer be changed or removed from the blockchain.

6.The transaction is completed, and user B receives his money.

Additional security of this system is provided by the principles of cryptography. All transactions occur thanks to a complex system of exchanging encrypted keys and electronic signatures, which confirm that the transaction has not been tampered with.

It is possible to bypass such algorithms, but this will require enormous computing power, which is currently inaccessible to humanity.

According to scientists, full-fledged quantum computers can theoretically cope with this task, but now only small prototypes exist. Even according to the most optimistic forecasts, cryptocurrency lovers can sleep peacefully for at least another 30 years.

The blocks are connected to each other using the same cryptography, as well as the generation of unique indicators that compress information in a special way for each of the subsequent links.

With each new element of the chain, information is compressed more and more, which is why an “avalanche effect” is formed. This is the reason why cryptocurrency mining is becoming more expensive every year.

Another reason why blockchain is so difficult to hack is that changes to blocks must be accepted by a large portion of users. When you try to make changes to one of the links, all participants in the blockchain immediately receive a notification about this and decide what to do.

Cryptocurrency extraction and mining

(170 words)

Cryptocurrency mining means adding new blocks to the blockchain chain. This process is difficult and requires enormous computing power.

Mining is the solution of complex mathematical calculations using your equipment. Moreover, every year the tasks become more and more difficult, and the required power increases, which makes it almost impossible to mine tokens at home. This is especially true for popular cryptocurrencies.Industrial mining still exists, but it is expensive and takes a long time to pay off.A standard mining farm looks something like this - a guarded, well-ventilated room in which there are system units with many video cards and coolers for cooling them. There must also be a backup power source for uninterrupted operation of the network.

In addition to mining, you can get cryptocurrency on the exchange by purchasing it in dollars or other fiat currency, and you can also store it there.

In Conclusion

(200 words)

There are now more than 1,000 different tokens on the cryptocurrency market with a total capitalization of more than $2 trillion.

To summarize, it can be noted that now cryptocurrencies are in an ambiguous position. Many are afraid to invest money in them, because... don't understand how coins

work.Technical difficulties in introducing cryptocurrency into business operations also cause great difficulties, as well as the fact that they are almost not regulated by legal legislation.

In addition, not everything is so clear with electronic money and with the prospect of investment. This is potentially one of the most profitable earning tools, but it is almost impossible to predict.

On the other hand, the cryptocurrency market is actively developing, and every year new platforms and opportunities for the development of electronic money appear. This is not to mention the fact that countries are beginning to take cryptocurrencies more seriously, trying to introduce them into their economies.

References

Martino, Pierluigi, et al. "An introduction to blockchain, cryptocurrency and initial coin offerings." *New frontiers in entrepreneurial finance research*. 2020. 181-206.

Chen, Long, Lin William Cong, and Yizhou Xiao. "A brief introduction to blockchain economics." Information for Efficient Decision Making: Big Data, Blockchain and Relevance. 2021. 1-40.

Swan, Melanie, and Primavera De Filippi. "Toward a philosophy of blockchain: a symposium: introduction." *Metaphilosophy* 48.5 (2017): 603-619.

Chithaluru, Premkumar, Kulvinder Singh, and Manish Kumar Sharma. "Cryptocurrency and blockchain." *Information security and optimization* (2020): 143-158.

Banking and Bitcoin (Matvii)

1. Online Banking – money goes digital

In the late **20th** and early **21st** centuries banking has begin evolving currencies to digital banking, which in its earliest forms dates back to the **1980s** – with evolution of payment cards and standards like **VISA & MASTERCARD.**

But the real rise of **digital banking** began in the mid-1990s, when dozens of countries started to create their own online banking network: USA, United Kingdom, France, Japan, China, Canada. Significantly impacted payment systems reserved with the rise of contactless payments was huge!

- Digital banking has been gradual, remains ongoing, and is constituted by differing degrees of banking service digitization.

The **2002-2008** growth of the smartphone market and its rapid technological leap transferred banking to another evolution step like mobile bank, mobile wallets, and digital payment platforms to and it further accelerated the trend. How big is this trend?

From the 2023 report of an independent marketing platform GITNUX:

- Online banking usage in the United States increased from 36% in 2005 to 73% in 2021.
- 51% of US adults use digital banking, with 81% of them accessing their accounts via mobile platforms.
- The global online banking users is expected to reach 3.6 billion by 2024.
- 89% of UK adults now use online banking, and 64% use mobile banking apps.

KEY TAKEAWAYS

1. *Online banking allows you to conduct financial transactions via the Internet.*
2. *You aren't required to visit a bank branch in order to complete basic online banking transactions.*
3. *You need a device, an Internet connection, and a bank card to register for online banking.*

2. Digital Currencies - money in air

After the trend rapidly started.
Central Banking Systems around the world - started to create and convert their currencies into "*Digital Format*" such currency is subject to all legal regulations of the government where this currency is based. Honourably the first steps in this direction are taken by the **USA**, after which all other big nations joined in: **Japan, EU, Canada, UK.**

Thus it does not differ from the real cash currency, thanks to which today we can pay for purchases in a shop not walking out of houses, paying bills in the same way and even no more worrying about currency conversion, as it now happens automatically at a fixed rate - We are not just spending some “charging number of digits” from the account, but a certain amount from a personal electronic bank account from the bank.
No more check books! It's a thing of the past!

> But not everyone likes to be "*controlled by the government*" - there are many reasons.

But the main thing is the freedom from big private or government structures and the desire for privacy. In response to concerns about government control, invasion of privacy, and the desire for financial autonomy, a group of innovators decided to rethink the very essence of currency. Result? Decentralized cryptocurrencies are a revolutionary concept that combines freedom, security and digital anonymity - **decentralized** means free, **crypto** means safety.

> A new modern and absolutely digital currency independent of manipulation by the state, private individuals or corporations and completely created on modern absolute private cryptography technology - making each user Incognito in the process of transferring/purchasing.

A glimpse into the future telling us that the decentralized cryptocurrency space is dynamic, with constant innovations such as privacy-focused coins, scaling solutions, and environmental sustainability efforts.
As users increasingly aware and seek financial freedom and freedom of choice, the future promises of the Cryptocurrency is to enhance people's financial awareness through decentralized technologies.

KEY TAKEAWAYS

1. *Cryptocurrency was developed as an alternative to the dollar, and its functions can make it an attractive investment.*
2. *Blockchain, the underlying technology that powers crypto, is seen as a tech disruptor.*
3. *Much like dot-com investing in the 1990s, crypto may hold promise, but there will likely be winners and losers.*

3. How Bitcoin works?

I. **I. Getting Started with Bitcoin:**

For new users, initiating Bitcoin transactions requires the installation of a Bitcoin wallet on a computer or mobile phone. This wallet generates a unique Bitcoin address, functioning similarly to email addresses. Users can share these addresses with others for transactions, emphasizing the practice of using addresses only once for enhanced security.

II. **The Blockchain - Public Ledger:**

The blockchain serves as a shared public ledger integral to the entire Bitcoin network. It records all confirmed transactions, allowing Bitcoin wallets to calculate spendable balances. The blockchain's integrity and chronological order are maintained through cryptographic mechanisms, ensuring transparency and security.

III. **Transactions and Private Keys:**

Transactions involve the transfer of value between Bitcoin wallets. Each wallet possesses a private key or seed, a secret piece of data used to sign transactions. This signature provides a mathematical proof of ownership and safeguards transactions from unauthorized alterations. Transactions are broadcast to the network and confirmed through a mining process within 10-20 minutes.

IV. **Mining - Confirming Transactions:**

Mining is a distributed consensus system that confirms pending transactions by incorporating them into the blockchain. It enforces chronological order, protects network neutrality, and prevents centralized control. Strict cryptographic rules govern block creation, ensuring the immutability of previous blocks. Mining introduces a competitive lottery system, preventing individuals from easily adding new blocks consecutively and maintaining the decentralized nature of the blockchain.

In conclusion

In my conclusion i will say that this new decentralized cryptocurrencies, which take all emphasize to the values of our freedom, privacy, and security in modern days, represent a paradigm shift in how we look at our cash currency. As this shift of our view takes a place, it is challenging our preconceived notions about what constitutes money, compelling us to reevaluate the place of central banks systems in the financial system and envision a time when people have unprecedented control over their financial lives. Will this be our future, though? How will these things work out for us? All we can do is dream.

References:

What is Online Banking? Definition and How It Works. (2023, April 9). Investopedia. Retrieved December 7, 2023, from https://www.investopedia.com/terms/o/onlinebanking.asp#toc-advantages-of-online-banking

Beattie, A. (n.d.). *The Evolution of Banking Over Time*. Investopedia. Retrieved December 7, 2023, from https://www.investopedia.com/articles/07/banking.asp#toc-banking-goes-digital

How does Bitcoin work? (n.d.). Bitcoin.org. Retrieved December 7, 2023, from https://bitcoin.org/en/how-it-works

Hacking (Danyil)

Introduction

(150 words)

Overview of Blockchain Technology

Blockchain is like a digital ledger, but instead of being kept in one place, it's spread out across a whole network of computers. Think of it as a record book that everyone can see, but no one owns. This setup is really cool because it means there's no central control - it's all about teamwork across many computers.

Importance of Security

Now, why is this security thing a big deal? Imagine you're using blockchain for something super important, like transferring money or keeping sensitive data. You don't want anyone messing with that, right? That's where blockchain's security shines. Each piece of data (or block) is tied to the previous one using complex cryptography. This makes it super tough for anyone to change anything without everyone else noticing. So, in a world where we're doing more and more online, having a safe and secure way to handle our digital stuff is super important, and that's exactly what blockchain offers.

The Nature of Blockchain Hacking

(200 words)

How Hacking Differs in Blockchain

Hacking in the blockchain world is a different beast compared to traditional hacking, mainly due to blockchain's unique structure. In traditional systems, hackers often target central points of control or vulnerabilities in a single system. But with blockchain, there's no central point to attack because the data is distributed across a network of computers, each holding a copy of the ledger. This means to hack a blockchain, a hacker would need to alter the majority of the copies simultaneously, a task that's not only incredibly difficult but also requires immense computational power.

Common Misconceptions

However, there's a common misconception that blockchain is totally invulnerable. While it's true that blockchain's design makes it tough to hack in the traditional sense, it's not foolproof. For instance, if someone gains control over more than half of the network's computing power, a scenario known as a 51% attack(I will talk about it later), they could potentially alter the blockchain. Even with blockchain's strong security, there are still some weak spots. Think about smart contracts or the software that runs the blockchain - if they're not set up perfectly, hackers could sneak in through those gaps. So, while blockchain is really secure, it's not completely unbeatable.

Types of Blockchain Hacks

(250 words)

51% Attacks

This happens in a blockchain network when a single person or group controls more than 50% of the network's mining power. In blockchain, "mining" involves validating transactions and creating new blocks. If someone has over half the network's power, they can potentially manipulate the blockchain. They could stop new transactions from getting confirmations, allowing them to halt payments. Even scarier, they could reverse transactions they made while they're in control, which could lead to double-spending. However, pulling off a 51% attack is tough, especially on larger networks like Bitcoin, because it requires immense computational resources.

Backdoor (Code Exploits and Smart Contract Vulnerabilities)

Code Exploits and Smart Contract Vulnerabilities: Imagine the blockchain as a complex machine running on code. Sometimes, there are hidden flaws in this code. Hackers love to find and use these flaws. It's like finding a secret door into a bank vault. Smart contracts are like automatic agreements on the blockchain. If they're not written carefully, they can have weaknesses too. Hackers can use these weak spots to do things like steal digital money.

Sybil Attacks

This is like one person pretending to be many people on the blockchain. They create a bunch of fake identities to gain more power or control in the network. It's like one person wearing lots of different masks to trick others. With all these fake identities, they can mess with the network by spreading false information or overwhelming it with fake transactions. It is somewhat similar to a 51% attack but much smaller, because sybil attacks can occupy a maximum of 1-2% of the network.

Notable Blockchain Hacks

(200 words)

Historical Examples

Blockchain technology, known for its security, has still faced some notable hacks over the years. A prime example is the DAO attack on Ethereum in 2016. The DAO (Decentralized Autonomous Organization) was a complex smart contract on the Ethereum blockchain, designed to function as a sort of investor-directed venture capital fund. However, due to a flaw in its code, a hacker managed to drain about a third of the DAO's funds, amounting to around $50 million in Ethereum.

Impact of These Hacks

When these big hacks happen, it's not just about losing money. People start to doubt how safe blockchain really is. Take the DAO attack on Ethereum as an example. It was a huge

deal because a lot of money was stolen. But the reaction to the hack was even more dramatic. The Ethereum community decided to essentially go back in time and create a new version of Ethereum where the hack never happened. This move was called a "hard fork". It's like taking a road and then splitting it into two different paths.

This decision caused a lot of arguments. Some people thought it was the right thing to do to fix the problem. Others thought it went against the whole idea of blockchain being unchangeable and secure. So, Ethereum split into two: Ethereum (ETH) and Ethereum Classic (ETC).

Mitigating Hacking Risks

(150 words)

Security Measures

To keep blockchain safe from hackers, a couple of smart moves are key. First, think of regular audits like a health check for blockchain. Experts look over the code, hunting for any sneaky bugs that hackers could use to cause trouble. It's all about catching issues early.

Then there's the cool idea of multi-signature systems. It's like needing several thumbs up instead of just one to make something happen. In blockchain land, this means more people need to say 'okay' before a transaction goes through. It's like having a bunch of people double-checking each other, making things a lot safer.

Role of the Community

The power of the people!
The blockchain community is super important. Everyone needs to keep their eyes peeled and report anything fishy. It's like having a neighborhood watch for the digital world. By everyone chipping in and staying sharp, the blockchain stays strong and secure. It's teamwork at its best!

Conclusion

(50 words)

Finally, I would like to say that no system is 100% secure, but blockchain technology wants to provide unlimited freedom and decentralization, as well as a large part of security. Don’t forget the importance of great security. because without it there will be no life for any project.

The main thesis

“No matter how advanced the system is, anything can be hacked”

References

Behanan, J. V. (n.d.). *OWASP Smart Contract Top 10*. OWASP Foundation. Retrieved December 4, 2023, from https://owasp.org/www-project-smart-contract-top-10/

Cobb, M. (2023, May 25). *9 smart contract vulnerabilities and how to mitigate them*. TechTarget. Retrieved December 4, 2023, from https://www.techtarget.com/searchsecurity/tip/Smart-contract-vulnerabilities-and-how-to-mitigate-them

51% Attack: The Concept, Risks & Prevention. (2023, June 29). Hacken.io. Retrieved December 4, 2023, from https://hacken.io/discover/51-percent-attack/

John, F., & Luciano, C. (2023, February 16). *Sybil Attack in Blockchain: Examples & Prevention*. Hacken.io. Retrieved December 4, 2023, from https://hacken.io/insights/sybil-attacks/

Seher, S. (2022, July 8). *Smart Contract Vulnerabilities & How to Prevent Them*. Hacken.io. Retrieved December 4, 2023, from https://hacken.io/discover/smart-contract-vulnerabilities/

Sergeenkov, A. (n.d.). *Sybil Attack Definition*. CoinMarketCap. Retrieved December 4, 2023, from https://coinmarketcap.com/alexandria/glossary/sybil-attack

7 Smart Contract Vulnerabilities & How to Prevent Them [2023]. (2022, December 15). PixelPlex. Retrieved December 4, 2023, from https://pixelplex.io/blog/smart-contract-vulnerabilities/

Sybil Attacks Explained. (2018, December 6). Binance Academy. Retrieved December 4, 2023, from https://academy.binance.com/en/articles/sybil-attacks-explained

What Is a 51% Attack? (2018, November 27). Binance Academy. Retrieved December 4, 2023, from https://academy.binance.com/en/articles/what-is-a-51-percent-attack

What is a 51% attack and how is it prevented? (n.d.). Bitpanda. Retrieved December 4, 2023, from https://www.bitpanda.com/academy/en/lessons/what-is-a-51-attack-and-how-is-it-prevented/

What is Sybil attack: How Blockchains Prevent Sybil Attacks. (2021, March 26). Phemex. Retrieved December 4, 2023, from https://phemex.com/academy/what-is-a-sybil-attack

Zykov, G. (2023, April 10). *51% Attacks on the Blockchain Explained: What Are the Dangers?* BeInCrypto. Retrieved December 4, 2023, from https://beincrypto.com/learn/51-attacks-explained

Copyright

All words in this text were formulated and written by us (indicated below), this work was not copied from any other works, all references we used in writing were indicated.

Part 1 – Introduction (Artem) – Written by Artem Surzhenko
Part 2 – Banking and Bitcoin (Matvii) – Written by Matvii Vasylenko
Part 3 – Hacking (Danyil) – Written by Danyil Tymchuk