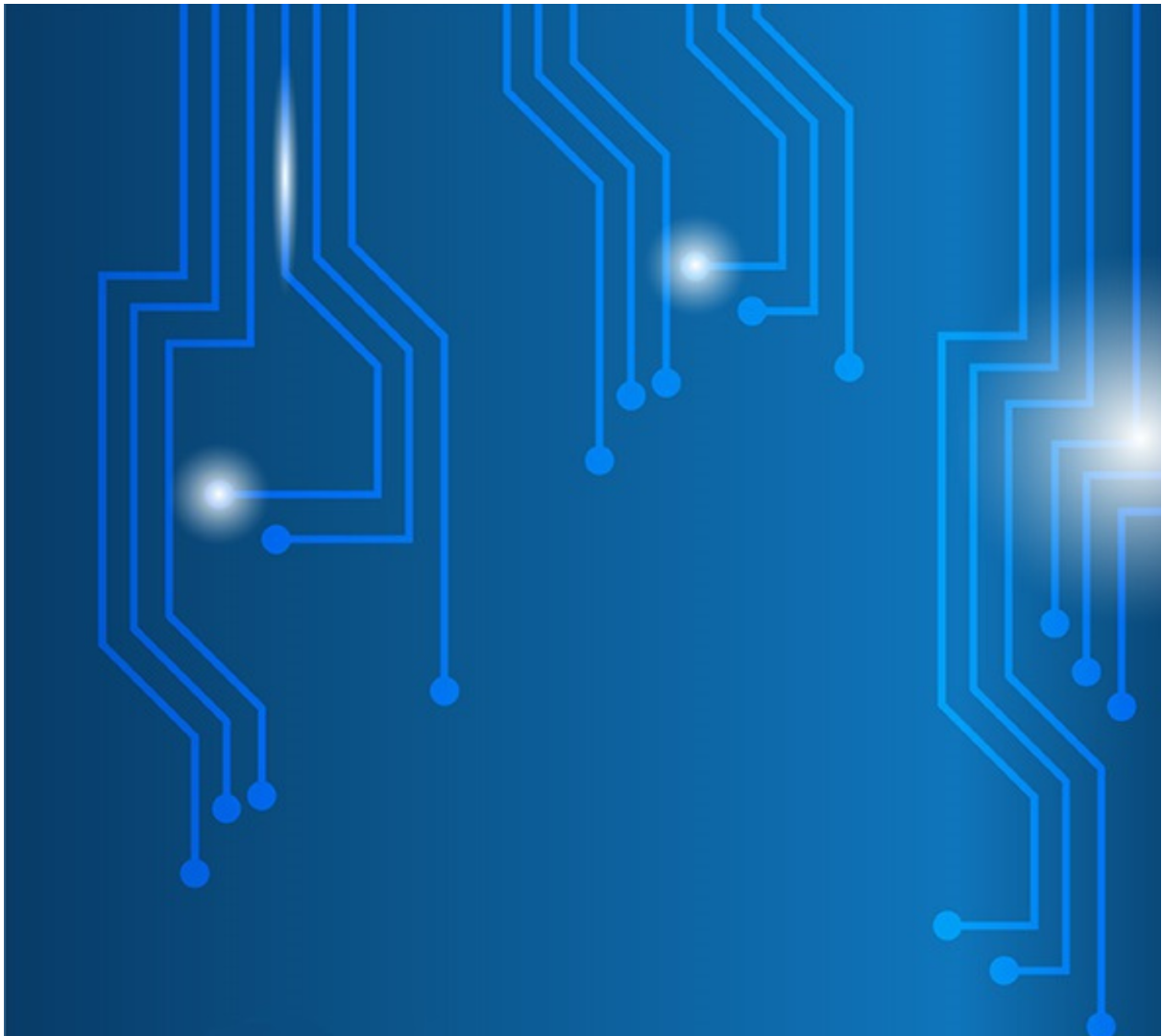




**Journal of University of Information Science
and Technology "St. Paul the Apostle" - Ohrid**
ISSN: 2955-182X

Publisher University of Information Science and Technology "St. Paul the Apostle" - Ohrid

Volume 3 | Issue 1 | 2023

EDITORIAL - Preface to Volume 3 Issue 1 of the Journal of University of Information Science and Technology “St. Paul the Apostle” – Ohrid

Dear Readers,

Journal of University of Information Science and Technology “St. Paul the Apostle” – Ohrid is an international, peer-reviewed journal published annually since 2016. It is an open access Journal available at the website of the University of Information Science and Technology “St. Paul the Apostle” – Ohrid (<https://journal.uist.edu.mk/>)

This Journal is committed to publishing and disseminating high-quality and novel scientific research work in the broad field of Applied Mathematics, Automation & Robotics, Blockchain, Business, Economy, Entrepreneurship & Management, Communication & Network Technology, Cybersecurity, Data Science, Distributed and Parallel Computing, Digital Art and New Media Art, Metaverse, Virtual and Augmented Reality, Communication & Network Technology, Smart Systems & IoT, Information Society & Digital Transformation, Biomedical Engineering.

As editor-in-chief of the Journal of the University of Information Science and Technology “St. Paul the Apostle” – Ohrid, I am pleased to present Volume 3, an issue mainly devoted to ...

This Issue of the Journal contains the most current research findings in the field of ...

I thank all the authors for contributing to this Issue and all the reviewers for providing detailed and timely evaluations of the submitted manuscripts.

It is an excellent challenge for the editor members to bring a new journal issue into the world, primarily when the Journal aims to publish high-quality manuscripts. I want to express my sincere gratitude to all of them for their excellent work, remarkable contribution, enthusiasm and support.

Sincerely Yours,

Associate Professor, Atanas Hristov, PhD

June 2023



Journal of University of Information Science
and Technology “St. Paul the Apostle” - Ohrid
ISSN: 2955-182X

IMPRESUM

FOUNDER AND PUBLISHER

University of Information Science and Technology “St. Paul the Apostle” – Ohrid

EDITORIAL OFFICE

University of Information Science and Technology “St. Paul the Apostle” – Ohrid

Address: Partizanska bb, 6000 Ohrid

Web page <https://journal.uist.edu.mk/>

EDITOR IN CHIEF

Associate Professor, Atanas Hristov, PhD

TECHNICAL EDITOR

Assistant Professor, Aleksandar Karadimche, PhD

EDITORIAL ADVISORY BOARD

EDITORIAL BOARD

Professor Ivan Bimbilovski, PhD

Professor Ustijana Reckoska Shikoska, PhD

Associate Professor, Dijana Capeska Bogatinoska, PhD

Associate Professor, Aneta Velkoska, PhD

Associate Professor, Jovanka Damoska Sekuloska, PhD

Associate Professor, Anis Sefidanoski, PhD

Associate Professor, Jane Bakreski, PhD

Assistant Professor, Goran Shibakovski, PhD

Assistant Professor, Aleksandar Karadimche, PhD

Assistant Professor, Mersiha Ismajloska, PhD

Assistant Professor, Ile Dimitrieski, PhD

Assistant Professor, Rasim Salkoski, PhD

Assistant Professor, Jovan Karamachoski, PhD

Assistant Professor, Ljubinka Sandjakoska, PhD

ISSN 2955-182X

CONTENTS

S. Mitrevska, A. Sefidanoski, E. Vrangalovska

Cryptocurrencies: impact, risks, benefits and analysis of its prevalence in Macedonia 5

N. Skenderov, A. Karadimche

Non-Fungible Token Model for Wildlife Conservation 14

E. Vrangalovska, S. Baloska, S. Mitrevska, A. Sefidanoski

Will Cryptocurrency replace money/cash? 27

M. Bukalevska, A. Karadimce

Modern Threats in Online Social Networks, Privacy Solutions offered by OSN Providers and
Commercial Solutions 36

T. Saferi, F. Doko, A. Hristov

Overview and preformance analysis of the latest supercomputer 49

Cryptocurrencies: impact, risks, benefits and analysis of its prevalence in Macedonia

Svetlana Mitrevska BSc ¹.

Anis Sefidanoski PhD ². Emilija Vrangalovska BSc ³.

Email(s): svetlana.mitrevska@mir.uist.edu.mk

1. University of Information Science and Technology, St. Paul the Apostle, Ohrid

2. University of Information Science and Technology, St. Paul the Apostle, Ohrid

3. University of Information Science and Technology, St. Paul the Apostle, Ohrid

Abstract

The essence of this research paper lies in the significant changes that the cryptocurrencies impose on the payment systems and the e-commerce evolution with an overview on the predictions on how cryptocurrencies might evolve in the future, looked at from an economic point of view. Migrating from a tangible world to a virtual world takes on real importance and imposes a lot of changes. We will also analyze the risks and benefits of the cryptocurrency, and an overview of the cryptocurrency prevalence in Macedonia, as a country that just recently started adopting the concept. This article aims to explain the various features of cryptocurrencies, which are mainly aimed at explaining how they work and why they are used. Although it's not yet clear when cryptocurrencies will become mainstream, financial institutions should still consider them as an alternative form of payment.

Keywords: *cryptocurrencies, blockchain, payment systems, risks, benefits, e-commerce*

Introduction

Cryptocurrencies, from their beginnings, were conceived as a new alternative within innovative payment mechanisms. Cryptocurrencies are powered by a distributed ledger technology, often a blockchain. Blockchain is a computer protocol used for digital recording and storing information on multiple computers or multiple nodes (Kitsantas, Vazakidis and Chytis 2019 [1]). Blockchain is not hosted in only one specific location, which not only creates redundancy, but raises its security to a high level, so if one node has been compromised, the rest of the nodes will remain intact.

Due to their decentralized nature, cryptocurrencies are becoming more prevalent in different countries. They can offer various advantages to investors. But nevertheless, there are various problems that revolve around this type of currency; a major problem is the lack of knowledge that people have about their operating mechanisms, in addition, of the distrust in the technological systems and what is found in the digital platforms in terms of computer security.

Cryptocurrencies are based on a peer-to-peer technology that enables people to make transactions without the need for a central institution. So, what has changed since the rise of the cryptocurrency? Well, at the beginning, back in 1983, when the concept was presented for the first time by the cryptographer David Chaum, who created electronic money, called e-cash, not much. But, since the introduction of Bitcoin, in 2009, when a person, or a group of people under the pseudonym Satoshi Nakamoto used hash function in its proof of work scheme to mine the very first block and launch the world's first cryptocurrency, a lot of changes have been made in the way how currencies operate. The answer to the question why people decide to purchase cryptocurrencies lies in the following: some people might choose to use cryptocurrencies as an investment opportunity or a way to avoid paying transaction fees. They can buy them through a credit card, or a process known as mining, as mentioned above.

Related Work

Cryptocurrency has the potential to disrupt our lives in a way that's similar to how mobile phones used to do. Initially, it was thought that it would be used to solve the physical gap between people. Although the technology behind cryptocurrency is still evolving, it is widely believed that the financial system will not work the same way it used to. As cryptocurrencies' use is emerging in today's world, there are many researches done on the topic: how do they impact the tangible world and the tangible currencies. A. Seetharaman et al (2017) [2] conducted research on what impact does Bitcoin have as a world currency. The findings are that Bitcoin has

huge potential, but its current form can't affect the USD much, as long as its exchange rate remains at a reasonable level. This is mainly due to its regulatory hurdles. Due to the limited supply, Bitcoin is considered a risky venture. Its potential value should be high enough to be used in transactions. Another important aspect of Bitcoin is its scarcity, which is mainly due to the number of units. The positive message that can be derived from this is that people are open to experimenting with virtual currencies and are willing to adopt different formats of them provided their currency has a regulatory backing. (Moritz Holtmeier, Philipp Sandner, 2019) [3] illustrated a comparison of different kind of money that can be seen in Table 1:

Traits of money	Gold	Fiat money (Euro)	Cryptocurrency (Bitcoin)
Way of exchange	Physical	Physical and digital	Digital
Controlled	Market	European Central Bank	Algorithm
Highly divisible	○	+	+
Globally transferable	+	+	+
Durable	+	+	+
Acceptable	+	+	○
Centralization	○	+	-
Secure (counterfeiting)	+	○	+
Stability (Volatility)	○	○	-
Predictable supply	+	○	+
Collateral	+	○	-

+ High
 ○ Medium
 - Low

The volatility of crypto currencies is considered their main issue since they cannot maintain a consistent value. In order to avoid experiencing large volatility, many crypto currencies eventually move toward a more formal regulated approach. According to Merrick Wang [4] eventually, the government might intervene in Bitcoin's and generally, cryptocurrencies' operations. This could cause them to become smaller and more competitive, which

could make it less valuable as it gets harder to mine. The global financial system is in a phase of change due to the effects of cryptocurrencies and other electronic currencies (Efremenko et al., 2018) [5]

Risks associated with cryptocurrencies

There are many risks associated with the use of cryptocurrencies, hence the distrust that many people have towards them. I will try to sum up the biggest risks that are associated with the cryptocurrencies. First, there are the **technology risks** (Arsi et al., 2021) [6], such as outages in the infrastructure components, which even though might be innocent looking, can lead to devastating consequences, such as the theft of 150, 000 ETH (Bosu et al., 2019) [7], then cybersecurity issues, scalability etc.

Then we have the **regulations**, as one of the major drawbacks. For example, our country, Macedonia, still hasn't accepted cryptocurrencies as a valid payment method. Then, we have China the world's second-largest economy which in 2021 effectively banned the ownership or mining of any type of digital currency. These are just two examples of how regulations can be set around the world. Since governments have the power to control the monetary supply and taxation of their citizens, they are unlikely to give up control over Bitcoin. As a result, countries that ban cryptocurrencies are unlikely to attract talent and innovation. [8]

At the end we have **volatility**. For some people, it might not be risky at all, since they tend to follow Bitcoin's example who rose very rapidly, but there are many cryptocurrencies whose value rapidly fell, and its future is uncertain, which was a huge loss for people that invested a lot in those cryptocurrencies, such as Terra Classic, as it

can be seen
from the
figure below



Benefits associated with cryptocurrencies

While there are many risks and drawbacks, there are also many benefits and advantages of owning and trading with cryptocurrencies. Let's start with the **inflation protection**. One of the main advantages of investing in cryptocurrencies is their ability to provide protection against inflation. Because of Bitcoin's hard cap, the

number of coins that can be issued each will never be exceeded. This means that as the money supply grows faster than the amount of coins that can be issued, the price of Bitcoin will increase.

Then, there are the **security and privacy**. Due to the nature of cryptocurrencies, anyone can't access your funds or sign transactions unless they have the necessary access to your private key. This means that even if you lose your private key, you can't recover it. These transactions are secured by the blockchain technology. The increasing number of computing power that can be added to the blockchain ensures that it is even more secure, private and transparent. (Navamani T M (2021), Bucko et al., 2015) [9,10]. Any attack on the network would require a huge amount of computing power to successfully change the blockchain's integrity. For major blockchains such as Bitcoin and Ethereum, this kind of attack is very expensive.

Transaction speed and low transaction costs are also a major advantage. One of the biggest advantages of cryptocurrencies is that they can be completed quickly. Unlike traditional financial transactions, which take a long time to complete, transactions in cryptocurrencies can be completed in just a few minutes. It also costs lot less than traditional transactions.

Prevalence of cryptocurrencies in Macedonia – a survey

While investigating the cryptocurrencies and analyzing them, their benefits and risks and their general impact, I was trying to find info on how the things stand in my country, the Republic of Macedonia. Due to the limited sources of information, I decided to publish a survey in two Facebook Groups. The first one is Federal Committee of Developers of the Republic of Macedonia (Сојузен Комитет на Програмери на Република Македонија) and the second one is Cryptocurrencies Macedonia (Криптовалути Македонија). The survey was conducted during the month of February 2022, and there was a total of 264 responses. The following questions were the subject of the survey:

1. What is your age?
2. Have you heard or read about the concept of cryptocurrencies, such as Bitcoin or Ethereum?
3. Do you own any cryptocurrencies?
4. Do you think investing in cryptocurrencies is risky?
5. Do you think investing in cryptocurrencies is profitable?
6. How likely are you to invest in cryptocurrencies in the future?
7. In 10 years from now, do you think that cryptocurrency will be more or less worthy?
8. Do you think our country's system is educating and motivating us to invest in crypto?

The answers and the corresponding charts can be found on the figures below:

What is your age?

264 responses

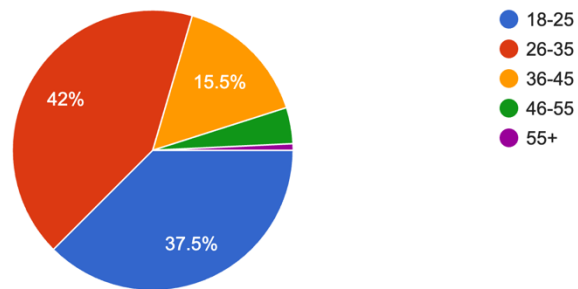


Figure 2- First question

Have you heard or read about the concept of cryptocurrencies, such as Bitcoin or Ethereum?

264 responses

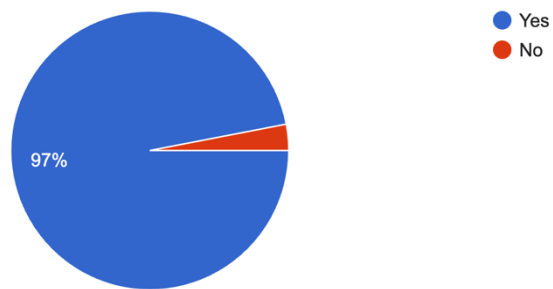


Figure 3- Second question

Do you own any cryptocurrency?

264 responses

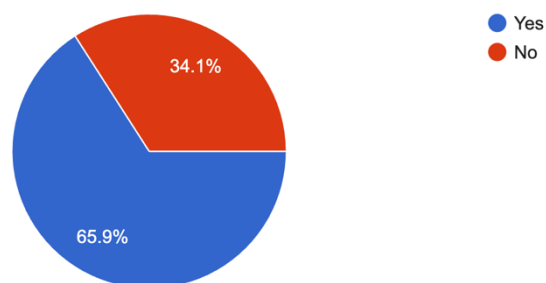


Figure 4 - Third question

Do you think investing in cryptocurrencies is risky?

264 responses

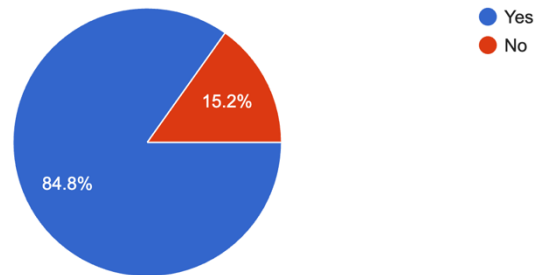


Figure 5 - Fourth question

Do you think investing in cryptocurrencies is profitable?

264 responses

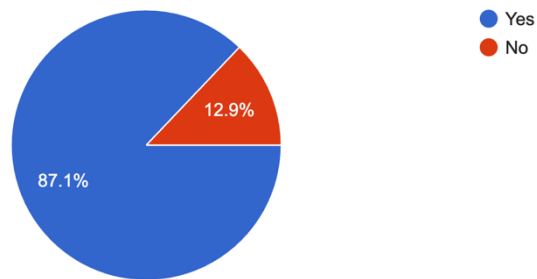


Figure 6 - Fifth question

How likely are you to invest in cryptocurrencies in the future?

264 responses

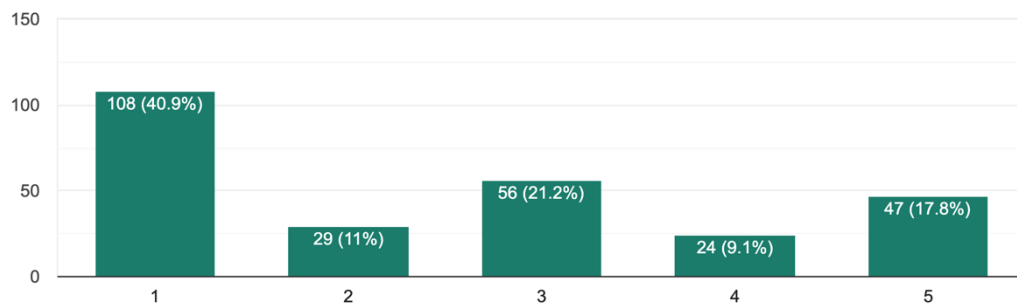


Figure 7 - Sixth question.
1 being very likely, 5 being not at all likely

In 10 years from now, do you think that cryptocurrency will be more or less worthy?

264 responses

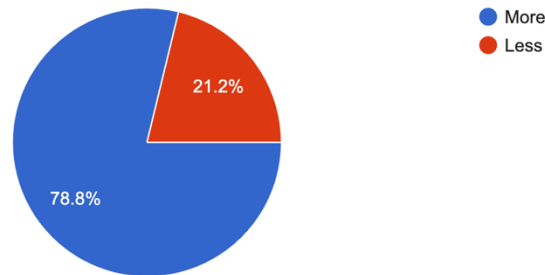


Figure 8 - Seventh question

Do you think our country's system is educating and motivating us to invest in crypto?

264 responses

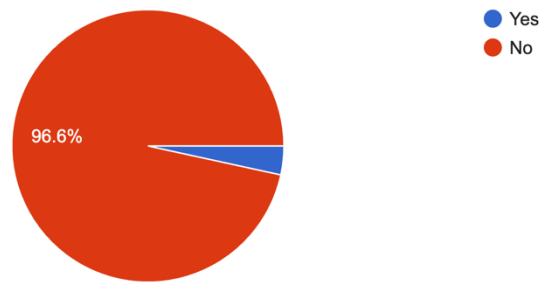


Figure 9 - Eighth question

On the survey mentioned above, we were able to collect a lot of information. However, for a detailed perspective on how different age groups feel about this new concept, here is a small breakdown by age:

Figure 10 shows how different age groups responded to “Have you heard about the concept of cryptocurrencies, such as Bitcoin or Ethereum”. Figure 11 shows how different age groups responded to the question “Do you own any cryptocurrency”. Figure 12 shows how the age groups are defined when asked whether they consider cryptocurrencies to be risky. On the other hand, Figure 13 shows how the different age groups think when they are asked whether they consider cryptocurrencies to be profitable. Figure 14 shows how the different age groups see the cryptocurrency in 10 years, more or less worthy, and Figure 15 shows how the different age groups think when it comes to our country’s system, whether they think it’s educating and motivating people to invest in cryptocurrencies or not.

Legend: Red=Yes, Blue=No (except for Figure 14 where Red = more and Blue = less)

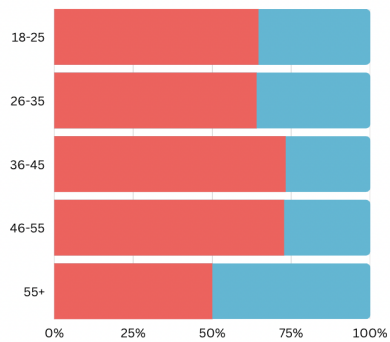


Figure 10

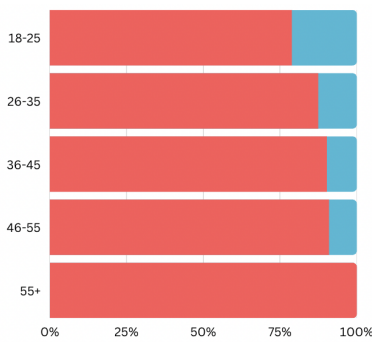


Figure 11

Figure 12

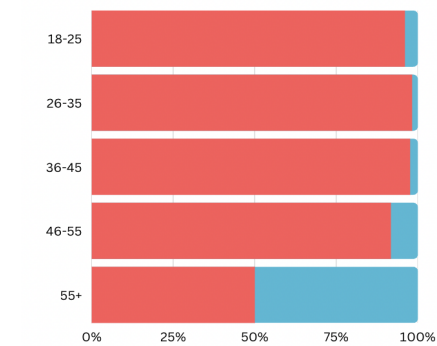


Figure 13

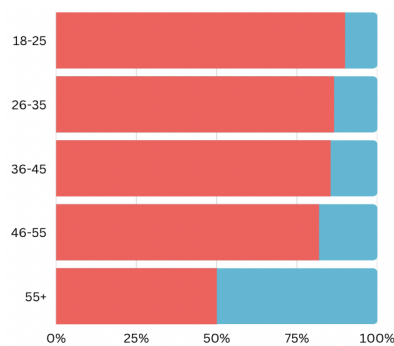
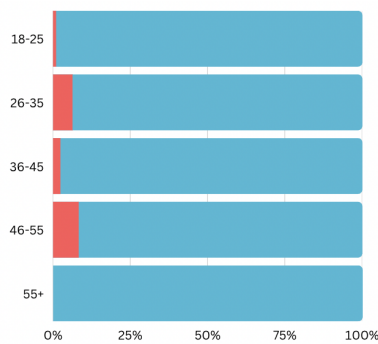
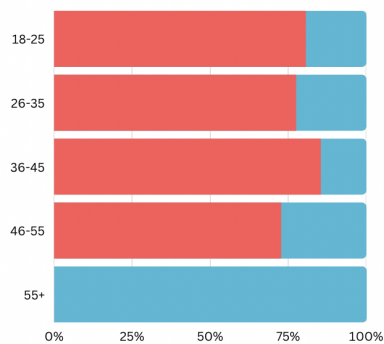


Figure 14

Figure 15



From the above answers we could conclude that this survey was mainly answered by young adults and adults, between the age of 18-45 years. 97% of the questioned have heard about cryptocurrencies, and 65.9% own a cryptocurrency, while 40.9% of those who hadn't are extremely likely to invest in the future. 84.8% think that investing in cryptocurrencies is risky, while 87.1% think that it's profitable, which makes the weight to go more towards profitable than risky. 78.8% think that cryptocurrencies will be more worthy in 10 years from now, while on the final question, whether they think our country's system is educating and motivating us to invest in cryptocurrencies, 96.6% answered that it doesn't.

Additionally, most of the younger people have heard about the concept of cryptocurrencies, and they own cryptocurrencies, and most of them think that cryptocurrencies will be more worthy in the future. That percentage falls among older generations (older than 55 years). Younger generations agree that the cryptocurrencies are profitable, while people older than 55 years are split half-half on this matter. However, most of them agree that the cryptocurrencies are risky and that our country doesn't do enough when it comes to educating and motivating people to invest.

Conclusion

In conclusion, a lot of young people are eager to invest, willing to take the risk, as they see more profit than risk in investing, and our country's regulations are currently not playing in young investors' favor, not just here, but in many countries. The regulatory hurdles play a big role now, cause cryptocurrencies are not widely accepted as a payment method, but we are probably up to see big changes in the future, meaning that the whole payment world will become a digital payment world and cryptocurrencies have a great chance to get to lead the new change.

References

1. A review of Blockchain Technology and its Applications in the business environment. Available: https://www.researchgate.net/publication/334615432_A_Review_of_Blockchain_Technology_and_Its_Applications_in_the_Business_Environment
2. Impact of Bitcoin as a World Currency. Available: https://www.researchgate.net/publication/317134650_Impact_of_Bitcoin_as_a_World_Currency
3. The impact of cryptocurrencies on developing countries. Available: http://explore-ip.com/2019_The-Impact-of-Crypto-Currencies-on-Developing-Countries.pdf
4. Bitcoin and its impact on economy. Available: <https://arxiv.org/pdf/2010.01337.pdf>
5. Efremenko, I.N., Panasenкова, T.V., Artemenko, D.A. and Larionov, V.A. (2018) 'The role of crypto-currencies in the development of the global currency system', European Research Studies Journal, 21(1). Available from: https://www.ersj.eu/dmdocuments/12.%20EFREMENKO_XXI_S1_18.pdf
6. Sonia Arsi, Soumaya Ben Khelifa, Yosra Gharbi, Nela Mzoughi (2021) CryptoCurrencies: Key Risks and Challenges. https://www.researchgate.net/publication/355407027_Cryptocurrencies_Key_Risks_and_Challenges/citations
7. Bosu, A., Iqbal, A., Shahriyar, R., & Chakraborty, P. (2019). Understanding the Motivations, Challenges and Needs of Blockchain Software Developers: a Survey. Empirical Software Engineering, 24, 2636–2673. <https://doi.org/10.1007/s10664-019-09708-7>
8. The Motley Fool – Bitcoin 3 biggest risks. Available: <https://www.fool.com/investing/2022/05/11/here-are-bitcoins-3-biggest-risks/>.

9. Navamani T M (2021) A Review on Cryptocurrencies Security. Available: https://www.researchgate.net/publication/352343090_A_Review_on_Cryptocurrencies_Security
10. Jozef Bucko, Dana Palova, Martin Vejacka (2015), Security and Trust in Cryptocurrencies
https://www.researchgate.net/publication/317955860_Security_and_Trust_in_Cryptocurrencies/citations
11. TerraClasic to USD. Available: <https://coinmarketcap.com/currencies/terra-luna/>

Non-Fungible Token Model for Wildlife Conservation

Nikola Skenderov[†], Aleksandar Karadimche[‡]

Email(s): nikola.skenderov@cns.uist.edu.mk, aleksandar.karadimce@uist.edu.mk

[†] Department of Communication Networks and Security, University of Information Science and Technology, “St. Paul the Apostle”, Ohrid, 6000, Republic of North Macedonia

[‡] Department of Information and Communication Sciences, University of Information Science and Technology, “St. Paul the Apostle”, Ohrid, 6000, Republic of North Macedonia

Abstract

Blockchain technology significantly impacted the previous decade with the creation of the popular cryptocurrency Bitcoin. Decentralization, the core property of the technology, was used for developing various successful applications such as Non-Fungible Tokens (NFT). On the other hand, the world is facing difficult challenges in funding activities to preserve endemic wildlife. In this paper, we investigate the current climate for funding for wildlife conservation, initial attempts for wildlife conservation using NFT and propose a model for wildlife conservation using NFT.

Keywords *Wildlife conservation, non-fungible token (NFT), Blockchain, Green business, Digital art, collectible.*

1 Introduction

The technology experienced enormous growth in the past thirty years. All the improvements in electronic devices and the rise of the Internet simplified many operations and communication between people across larger distances, paving the way for many opportunities. Blockchain technology is still in the early phase of adoption, but it has the potential to make the same impact in the future as the invention of the Internet. Internet nowadays is a significant platform for people to map wildlife worldwide and simultaneously join forces in conserving endemic species. Blockchain technology (particularly non-fungible tokens (NFT)) can offer a newer way to fund projects for wildlife conservation. This paper starts by describing blockchain technology and NFT in particular to capture the essential characteristics that make it unique. Then it continues with examples of current traditional ways of funding projects for wildlife conservation. Later in the paper are analyzed current attempts for wildlife conservation using NFT. In the final sections of the paper, we form the model based on the previous sections.

2 Blockchain technology and NFT

The origins of blockchain technology as we know it today were traced in 2008 with the whitepaper Bitcoin: A Peer-to-Peer Electronic Cash System by the pseudonym Satoshi Nakamoto [1]. The goal of Blockchain technology is to create a decentralized environment where no third party is in control of the transactions and data [2].

The blockchain is a decentralized ledger where the nodes are users who send data through transactions. The cryptocurrency Bitcoin is the prime example of the application of the technology because it enables the transfer

of money between two parties without needing an intermediate. The money transfer is fast, removing the need for banks as intermediates to approve the transaction and, at the same time, removing the additional costs for the money transfer. With the decentralization itself, the technology brings a couple of advantages, such as increased security and immutability. Because there is no central authority, any attempt to compromise the system is almost impossible because the attacker will have to own at least 51% of the nodes on the network, and usually, the network consists of a larger number of nodes. This leads to the advantage of immutability. Each node has a copy of the ledger with all transactions. The transactions are chained in a chain of blocks in the order of approval, and because of this structure, most attackers cannot compromise a single block. If they attempt to compromise one block, all the subsequent blocks will be invalid. Because of the confirmed transactions on the ledger, the attackers' attempts will be quickly discarded.

Verification and addition of transactions into the blockchain are achieved using the more widely used concepts of Proof of Work (PoW) and Proof of Stake (PoS). Proof Of Work requires the participants to mine a block and requires them to solve an increasingly difficult problem to ensure the mined block is valid [1]. To validate and add a block into the blockchains, users called miners compete with each other in solving complex cryptographic mathematic problems. To solve the problem, each miner uses large computing power in order to increase the chances of him validating the block. For validating the block, the miner receives a cryptocurrency transaction fee, hence the mining incentive. One block of transactions with this system is usually added to the blockchain in approximately ten minutes. This concept is used in the Bitcoin blockchain for the transfer of cryptocurrencies. Because of this level of organization, the system is secure and decentralized. The main disadvantage of this approach is the usage of larger computing power. Miners compete with each other to mine a block, and for one block to be mined, expensive equipment is used. This is why in recent times, the concept of Proof of Stake is widely used, especially in various decentralized applications aside from cryptocurrencies. Proof of Stake works by providing the user who has the highest stakes in each network with the opportunity to exploit [3]. Here the miners are called validators and compared to the concept of Proof of Work, and they do not need expensive equipment and large computing power in order to validate and add a block to the blockchain. Each validator must own a large amount of cryptocurrency. The selection of a validator is randomized, allowing each validator an equal chance to validate blocks. After validating the block, most validators must agree that the block is valid. This concept ensures reduced computing power and faster validation of transactions. As a disadvantage, this concept is suitable for a private network when all the validators are known and non-malicious. Proof of History, on which Solana Blockchain operates, focuses on a faster number of transactions per second [4]. Proof of Stake validators is used for validating and adding blocks in the blockchain. The difference is in the calculation of time. In Proof of Stake, nodes rely on network time, and that makes the network slower. In Proof of History, the Verifiable Delay Function is used to calculate the time based on historical occurrences.

Since the second half of the previous decade, various concepts of the technology such as smart contracts and non-fungible tokens gained in prominence in various decentralized applications. This occurred at a time when cryptocurrency transactions were at their peak.

In a smart contract, contract clauses written in computer programs will be automatically executed when predefined conditions are met. Smart contracts consisting of transactions are essentially stored, replicated, and updated in distributed blockchains [5].

The following phases of smart contract lifespan are discussed by Zheng:

1. Creation. Just like a physical contract, the terms of the contract are defined in advance between multiple parties, such as lawyers, stakeholders, and software engineers. Then, those terms are developed in a computer program.
2. Deployment. The next step is deploying the smart contract. The contract is stored on top of the blockchain, and it is available for access by any party. At this point, the digital assets of the two parties involved in the smart contract are frozen.
3. Execution. When the conditions are met, the contract will be executed, which means some statements will be executed in the form of a transaction and put on the blockchain.
4. Completion. The states of the involved parties are updated, and the transfer of digital assets between the two parties occurs. The digital assets are unlocked.

Smart contracts utilize the advantages of blockchain technology compared to physical contracts, such as speed, elimination of intermediates, and immutability. In addition, they remove human error and corresponding costs, and the whole process is automated.

Non-fungible token (NFT) is a cryptographically unique, indivisible, irreplaceable and verifiable token that represents a given asset, be digital or physical, on a blockchain [6]. We can compare non-fungible tokens to their counterparts in blockchain technology - fungible tokens. Fungible tokens are the cryptocurrencies such as Bitcoin, Ether, etc., because one token has the same value as another token, just like fiat currencies. On the other hand, non-fungible tokens are unique, and one non-fungible token has a different value from another token. For example, if digital art is sold on the market, just like physical one, each digital art has a different value from another. NFTs are minted(created) on the blockchain using smart contracts. The smart contract assigns the creator of the contract as the initial owner of the NFT. When a purchase of the NFT occurs, the ownership of the asset is assigned to the buyer based on the rules defined in the smart contract. With any potential resales of the NFT, the history of the previous owners can be traced in order to determine the original owner (the creator of the NFT). This is useful for proving asset ownership and potential monetizing for resale (especially for musical artists or gamers).

The most popular blockchain where NFTs are minted is Ethereum Blockchain. Ethereum is a standard choice for minting NFT because it has its own cryptocurrency and provides an environment for developing decentralized applications. Solidity is the language used for creating smart contracts on Ethereum. Developers use well-defined standards which guarantee the proper creation and transfer of an asset. [7]

ERC721 Standard

The initial standard for NFT. Each asset is unique from other assets and represented with tokenId.

The two core functions of the standard describe the owner of the asset with mapping to the corresponding address and transferring the asset between two addresses displayed with the following interface.

```
interface ERC721 {  
    function ownerOf(uint256 _tokenId) external view returns (address);  
    function transferFrom(address _from, address _to, uint256 _tokenId)  
external payable;  
}
```

ERC1155 Standard

It groups multiple non-fungible tokens with one Id. This is useful for the transfer of multiple unique assets (each with a quantity specified) from one user to another. This is represented with the following interface.

```
interface ERC1155 {  
    function balanceOf(address _owner, uint256 _id) external view returns  
    (address);  
    function transferFrom(address _from, address _to, uint256 _id, uint256  
    quantity) external payable;  
}
```

Each NFT smart contract is stored on the blockchain, but the asset associated with the contract itself is stored off-chain. There are two options: centralized servers such as Amazon Web Services (AWS) and decentralized InterPlanetary File System (IPFS). IPFS is the preferred option since it is a peer-to-peer storage system. One asset is replicated across multiple nodes and it is always available. Centralized servers are not preferred since if a centralized server stops operating, and the data will be lost forever.

NFT assets can be any physical or digital item. The most popular assets sold on the marketplace are collectibles, digital art, games, etc. According to NonFungible [8], current daily sales average around 25 000 – 30 000 compared to an average between 150 000 – 200 000 during the same period last year.

The experts attribute the fluctuation of the NFT sale volume to the fluctuation of the cryptocurrency values and current economic crises attributed to the 2022 conflict in Ukraine.

The following graph shows the number of sales throughout the years.

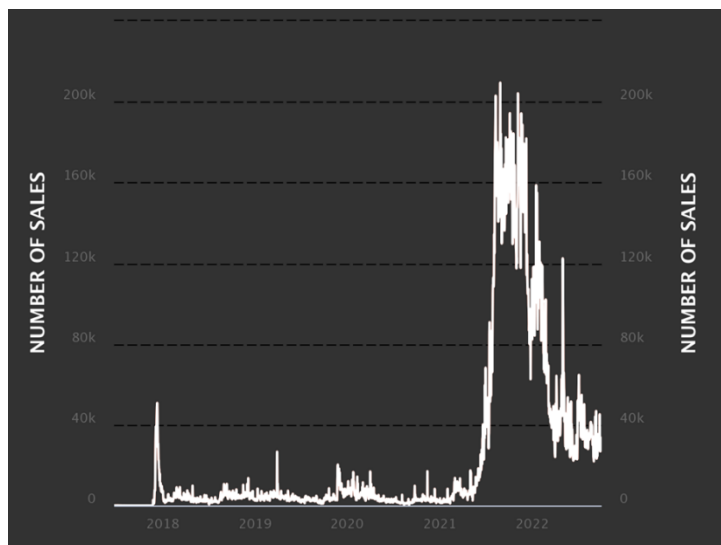


Figure 1: Number of sales NFT Source: NonFungible

Nevertheless, the volume in U.S. dollars in the first quarter of 2022 reached around 11 billion dollars, to 8 billion dollars in the second quarter.

NFT's can be bought and sold in NFT marketplaces. Each marketplace has its own specific characteristics, such as types of blockchains, transaction fees, types of assets sold, etc.

Popular blockchains aside from Ethereum include Solana, Polygon, Flow, Tezos, etc. Until 15 September 2022, Ethereum used the Proof of Work mechanism and was criticized for environmental pollution because of the

higher processing power and for the low number of transactions per second (13-15). On 15 September 2022, Ethereum switched to a Proof-of-Concept mechanism and promised energy reduction by 99% and a larger number of transactions per second [9]. Because of the long usage of the Proof of Work mechanism on Ethereum, larger competitors emerged. In *Solana*, blockchain developers can create programs using well-used languages such as C, C++ or Rust. Twenty million NFTs have been minted on the blockchain as of October 2022. The Proof of History mechanism speeds up the number of transactions per second which range from around 50 000 – 60 000 per second [10]. *Polygon* is another blockchain whose main purpose is to return transactions to the Ethereum blockchain with improved scalability and lower transaction costs. It is built on top of Ethereum and can operate up to 65 000 transactions per second using the Proof of Stake mechanism. Developers can write the contracts using Golang, Solidity, Vyper programming languages [11]. Dapper Labs created flow blockchain, the team behind the most popular NFT products, CryptoKitties and NBA Top Shot. The blockchain uses the Proof of Stake mechanism but what it makes unique from the rest is that not all nodes are equal. Nodes are divided by the work they accomplish. Collection nodes collect transactions for validation. Consensus nodes form and propose blocks using the Proof of Stake mechanism. Execution nodes are the most power-intensive nodes responsible for the execution of the blocks. Verification nodes are responsible for confirming the correctness of the work done by Execution nodes. Access nodes route transactions to the appropriate Collection nodes. The design of the contracts is done using Cadence programming language. It is one of the more eco-friendly blockchains with a total annual energy usage of 0.18 gWh [12]. Another blockchain for developing NFTs is *Tezos*. It uses the Proof of Stake mechanism, and smart contracts can be built using the programming languages Archetype, LIGO, and Python [13].

OpenSea is arguably the largest and oldest NFT marketplace. It supports various blockchains, including Ethereum, Solana, and Polygon. Multiple types of NFTs are sold, including art, collectibles, photographs, music, etc. Popular NFTs on the platform include CryptoKitties and CryptoPunks. The items can be sold at a fixed price or at timed auctions. For each item sale, OpenSea receives a fixed 2.5%, excluding transaction fees. Creators define how much royalties will receive from resales [14].

Rarible is another NFT marketplace. It supports the following blockchains Ethereum, Solana, Flow, Polygon and Tezos. In addition to cryptocurrencies, users can buy NFTs with fiat currencies. Art, collectibles, photographs, music, etc. can be sold in this marketplace. The items can be sold at a fixed price or at timed auctions. Rarible receives 1%, excluding the transaction fee for each NFT sold. Creators decide how much royalties will receive from resales. It is a community-owned marketplace, meaning holders of the native token RARI can decide the marketplace policies [15].

SuperRare is an NFT marketplace specializing in selling digital artworks. It operates under the Ethereum blockchain (ERC-721 protocol). The items can be sold at a fixed price or at timed auctions. For each sale of digital artwork, SuperRare receives 3%. For primary sales, the commission fee is 15%, and for secondary 10% of royalty. The marketplace makes a strict selection of established artists and digital artworks in order to sustain quality [16]. Figure 2 displays the interface of the homepage of the marketplace.

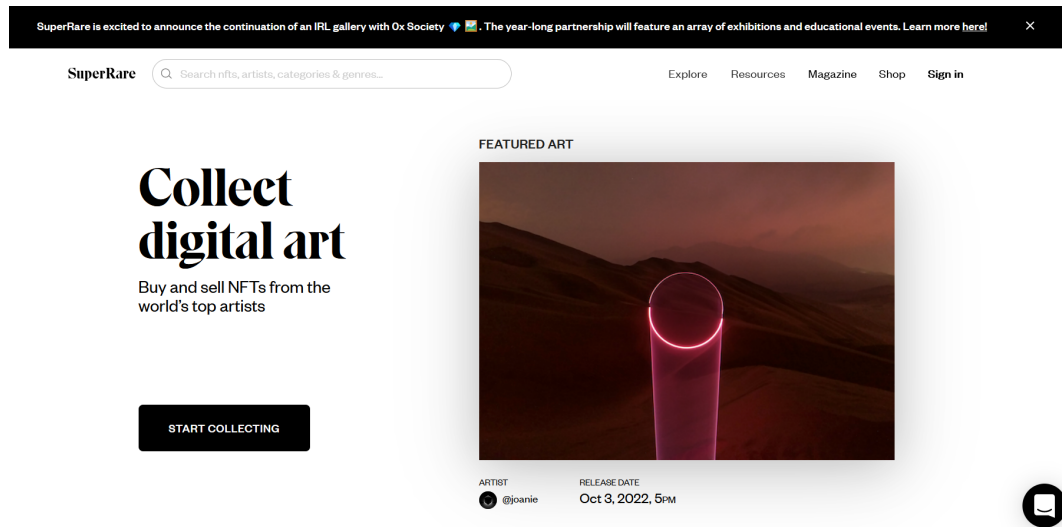


Figure 2: SuperRare homepage

Foundation is another NFT marketplace specialized for selling digital artworks. It also operates under the Ethereum blockchain. The items can be sold at a fixed price or in timed auctions. 15% for the initial sale of the digital art is reserved for commission fee. The artist of the digital art receives 10% of the resale of the item [17].

NBA Top Shot is one of the marketplaces that generate the largest volume of sales of NFTs. Created by Dapper Labs, it operates on Flow blockchain. The digital video collectibles in the form of video highlights from The National Basketball Association (NBA) players' present and past are sold on the marketplace [18].

3 Traditional channels of funding wildlife conservation

Most of the current projects for wildlife conservation are implemented by different types of organizations such as: charities, trusts, non-governmental organizations, governmental organizations or intergovernmental organizations. The organizations can be global, national, regional or local.

Notable examples of such organizations and the ways of funding are the following:

1. *World Wide Fund for Nature (WWF)* is the world's largest conservation organization operating in nearly 100 countries. Its partnership with communities, companies and governments is focused on developing and delivering innovative solutions that protect wildlife and the places in which they live.

The organization's annual report as of 2020 year shows a net income of 888 million dollars (up by 16%) which comes from various sources: 65% of funding from individuals, 17% from the public sector (such as World Bank, DFID, and USAID), 9% from trusts and foundations and 8% from corporations. The rest is from other unspecified resources and earned income [19], [20].

2. *United States Fish and Wildlife Service* is a government agency responsible for conserving and managing fish wildlife and their habitats. It is the world's oldest conservation agency, back to 1871. The annual budget for 2021 was 1583.9 million dollars and the funding is organized in the following manner.

The Federal Aid in Wildlife Restoration Act, popularly known as the Pittman-Robertson Act, was approved by Congress in 1937 and began functioning in 1938. The purpose of this Act was to provide funding for the

restoration, rehabilitation, and improvement of wildlife habitats, wildlife management research, and the distribution of information produced by the projects.

Funds are derived from an 11 percent federal excise tax on sporting arms, ammunition, and archery equipment and a 10 percent tax on handguns. These funds are collected from the manufacturers by the U.S. Department of the Treasury and are apportioned each year to the States and Territorial areas by the U.S. Department of the Interior based on formulas set forth in the Act. Appropriate State agencies are the only entities eligible to receive grant funds.

Each state's apportionment is determined by a formula that considers the total area of the state and the number of licensed hunters in the state. The program is a cost-reimbursement program where the state covers the full amount of an approved project (options include research, surveys, management of wildlife and/or habitat, and acquisition or lease of land) and then applies for reimbursement through Federal Aid for up to 75 percent of the project expenses. The state must provide at least 25 percent of the project costs from a non-federal source [21], [22], [23].

3. *Ezemvelo KZN Wildlife* is the provincial government agency mandated to carry out biodiversity conservation and associated activities in the province of KwaZulu-Natal in the Republic of South Africa. The primary focus of the organization is biodiversity conservation - the management of more than 120 protected areas that include two World Heritage Sites, which are the Maloti-Drakensberg Park World Heritage Site and the Isimangaliso Wetland Park World Heritage Site. A secondary but nevertheless vital aspect is the management of one of the largest eco-tourism operations in South Africa. The Ezemvelo KZN Wildlife administration model has been shown to work well, whereby the eco-tourism operations provide financial support for conservation operations. The annual report for 2021 shows a total income of around 1 million rands (around 645 000 dollars), 84% of which comes from non-exchange transactions such as transfers and 16% from exchange transactions such as the sale of goods, accommodation, conservation levy, admission, funder revenue, donations, etc [24],[25].

4 NFT projects for wildlife conservation

One of the earliest NFT implementations with respect to wildlife conservation came in the domain of video games. *CryptoKitties* is one of the first successful blockchain games and is still operating today. In the game, users breed so-called CryptoKitties, digital pets, each with specific attributes. CryptoKitties is an app built on the ERC-721 protocol and the Ethereum network. Each CryptoKitty is unique and cannot be replicated. In 2018 one specific CryptoKittie called Honu (half cat, half turtle) was created and raised 50 000 dollars in an auction for two non-profit organizations Ocean Elders and ACTAI Global, for conservation projects of turtles in the Caribbean. Figure 3 displays the crypto kitties Honu displayed on the game's website.

Another project created specifically for the purpose of wildlife conservation (particularly pandas) is *PandaEarth*. The project was licensed by China Panda Conservation and Research Center and still operates to the present with a total statistic of 1173 users and 63474 dollars volume as of September 2022. This application, like CryptoKitties, was also built on the ERC-721 protocol on the Ethereum network. Similarly, like CryptoKitties, pandas with specific characteristics are created for collecting and breeding [26].

With the boom of NFT in 2021, many individuals and organizations have the opportunity to use blockchain technology as a new way of raising money for wildlife conservation.

One of the most popular ways of raising money is by selling digital art. Many artists began creating digital paintings or photos and selling them like NFTs. Here are some examples:

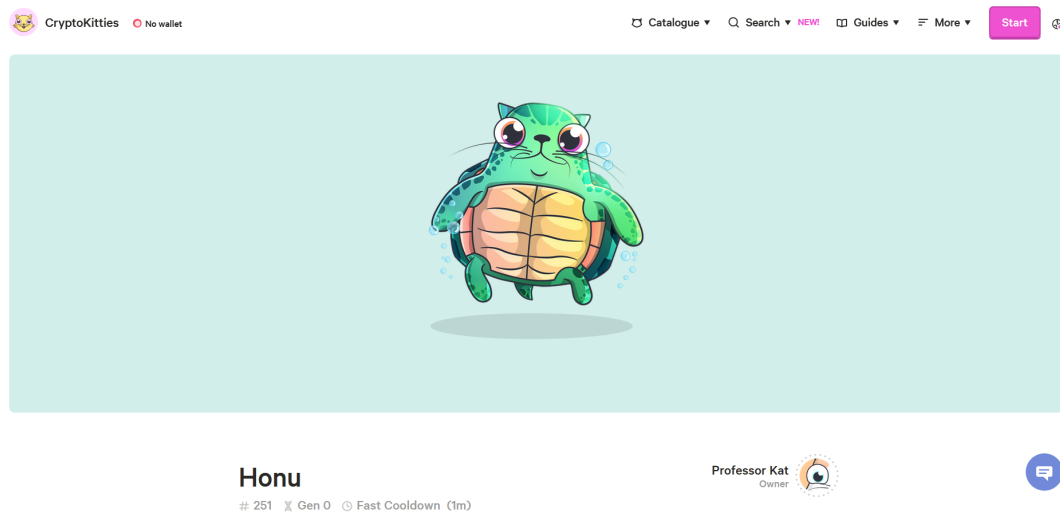


Figure 3: Honu CryptoKittie displayed on the game's website

Sam Price is a multimedia artist whose paintings, in addition to traditional marketplaces, are selling as NFTs on the website SuperRare specializes in the market of digital art. In collaboration with Lady Rocket and her Foundation Saving the Survivors, created animated "Satellite Rhino" NFTs which are animated digital art sold as NFT. With the money collected will be used for funding for satellite technology for locating wounded wildlife and support for constructing wildlife emergency rescue and recovery hospitals for wildlife. Figure 4 shows one piece of art displayed on SuperRare [27].

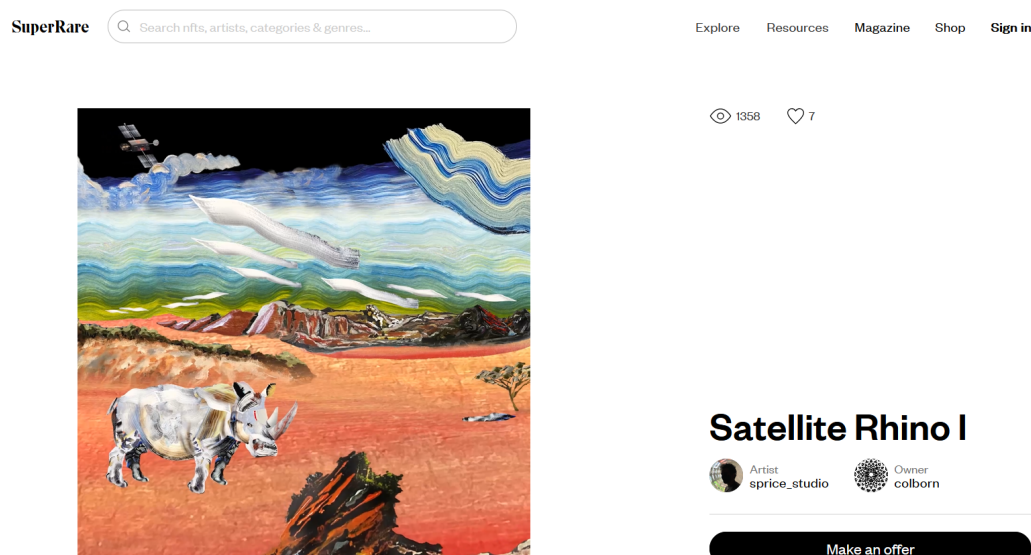


Figure 4: Satellite Rhino animated NFT on SuperRare

Richard Bernabe is a wildlife and travel photographer and author. His clients are renowned names such as

National Geographic, The New York Times, Time, Apple, Microsoft, etc. His collection Living Legacies consists of black-and-white images of African wildlife. The collection is minted on the Foundation marketplace, and 15 % of the sale will be donated to African wildlife conservation groups, including African Wildlife Foundation, WildAid, Born Free Foundation and others [28].

Ryan Hevern is a nature photographer and naturalist who has lived in Asia for decades. His NFT collection of digital photos, *The Night is Alive*, minted on the OpenSea platform, consists of photos of endemic species subspecies and other wildlife captured during the night throughout the forests of Taiwan. 10% of each sale will go to The Society for Wildlife and Nature (SWAN) International [29].

The NFT collection of digital photos, *No Kingdom without Kings*, is centered around 13 big cats (lions, tigers and leopards). 50% of the sale of the collection, which also is minted on OpenSea marketplace, is reserved for Glen Garrieff (G.G.) conservation. *Simon Needham* is a photographer and director and he is involved in advertising [30].

In terms of organizations so far, *The Worldwide Fund for Nature Inc.* is the largest organization that decided to use the NFT for additional resources for collecting wildlife conservation donations. The campaign *NFA Non-Fungible Animals* by the branch of WWF Germany was initiated in November 2021. It is centered around selling a limited number of crypto artworks of ten endangered species created by ten renowned artists. The total number of artworks per species is equal to the current number of animals in the wild. It operates under the Polygon blockchain. The collection operates on the OpenSea marketplace and, so far, are raised 272468 euros which will go for the protection of endangered species (preservation of their habitat, the creation of new protected areas, or the fight against poaching and overfishing). The campaign from the branch WWF United Kingdom in February 2022 NFT collection Tokens for Nature received backlash from environmentalists and was immediately canceled. The reason is that environmentalists deem NFT as not eco-friendly. Even though the Polygon blockchain is used for low power consumption, environmentalists estimated that the transactions produce an unacceptable level of CO2. An example of the page is displayed in Figure 5 [31],[32].

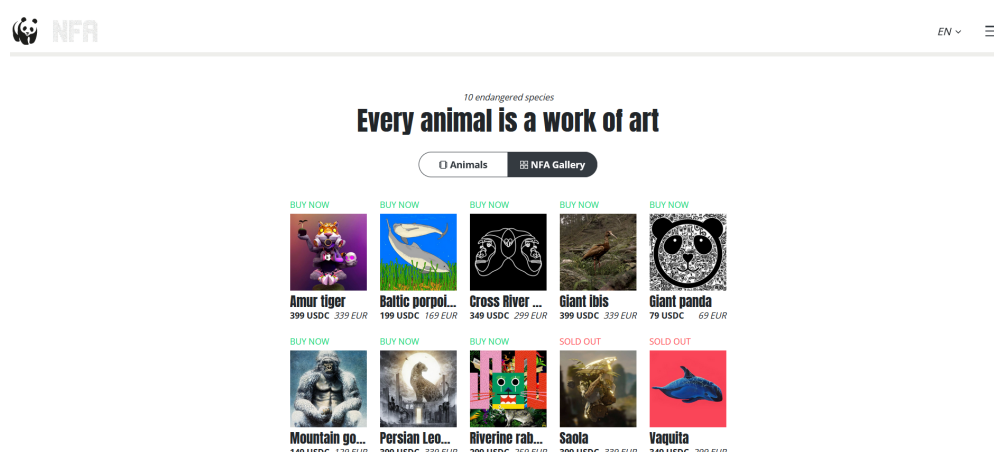


Figure 5: NFA Non-fungible animals of World-Wide Fund for Nature

Australia Zoo, opened in 1970, is a zoo located in the Australian state of Queensland, and it is a member of the

Zoo and Aquarium Association. Opened by the parents of Steve Irwin, popular Australian environmentalist, conservationist, wildlife expert and television personality, currently, the zoo is operated by his wife Terri. The money generated from the park goes into wildlife conservation projects, namely Australia Zoo Wildlife Warriors.

In 2002 Steve, with his wife Terri, opened the non-profit charity Australia Zoo Wildlife Warriors in order to make more impact on the protection of injured, threatened, or endangered wildlife.

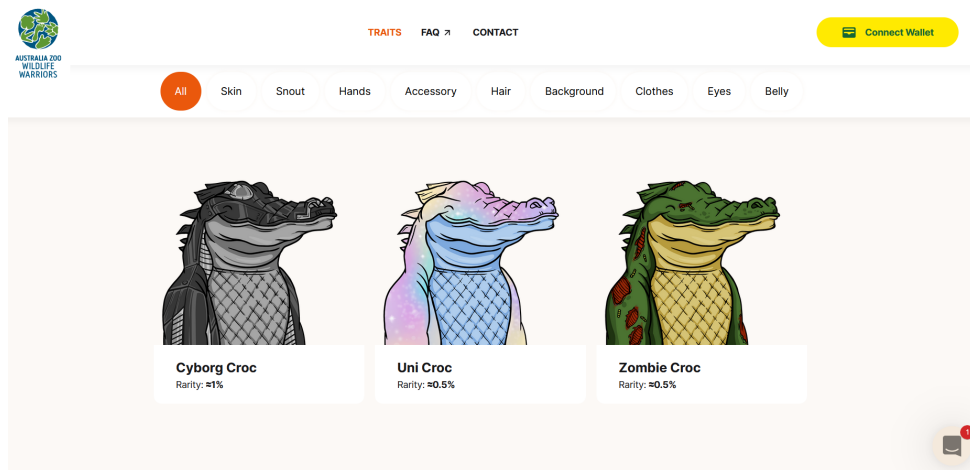


Figure 6: Example of Crocodile traits of Wildlife Warriors NFT project

In May 2022, in the 20th anniversary of Wildlife Warriors, it launched Wildlife Warriors NFT project. In partnership with Meadow Labs, a technology startup, it is run on the Algorand blockchain, the first carbon-negative blockchain with 0.01 gas and transaction fees. Users can buy collectible animal NFT. Each collectible can be customized with 100 + traits, each with its own different rarity. The sales go directly to wildlife conservation projects for Australia Zoo Wildlife Warriors. The NFT project is displayed in Figure 6 [33], [34],[35],[36].

Wildcards are a blockchain tech startup starting in 2019 and still operating today. Animals are sold as artwork collectibles. After buying, the users can resell them for a larger price, thus making a profit and donating from the resale to wildlife conservation projects for around 30 organizations across different continents. The startup changed the blockchain network from Mainnet Ethereum to a more eco-friendly Polygon. As of September 2022, the startup raised a total of around 85000 dollars for conservation [37].

Another NFT project is *The Munchie Mafia* appearing in 2022. It sells 2100 NFT of 12 hand-painted characters, each representing a currently endangered species. 2% of all mint sales and 1% of resales will be donated to The International Rhino Foundation and the Rainforest Trust. The creators promise an additional increase of % of mint sales donation with each character they create. As of September 2022, on OpenSea, the total volume is around 3878 dollars with 140 owners [38].

5 Proposed model

We propose a model named Wildlife NFT Eco-Friendly model. The model is displayed in the following figure.

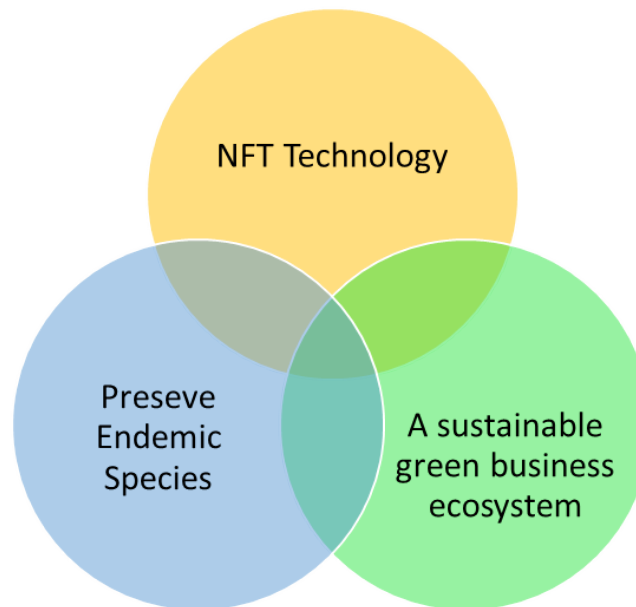


Figure 7: Wildlife NFT Eco-Friendly model

The proposed model will benefit from the relationship between NFT and preserving endemic species. The blockchain technology with NFT smart contracts made initial steps for preserving endemic species with different initiatives such as selling digital art, collectibles, etc. In the future, many different ideas will be developed using smart contracts. NFT can bring different generations of potential funders for wildlife collection. Younger generations would be interested in NFT smart contracts through games and collectibles. Older generations, especially wealthy businessmen, are potential customers for digital art, just like physical. The smart contracts are programmed to execute statements when some condition happens. This would transfer the assets to the right place and prevent any potential attacks on the system.

Also, because of the decentralization of the system, it prevents potential loss of assets, and at the same time, it ensures interoperability between different platforms. Assets from one no longer existing project can be utilized for another project.

NFT smart contracts are an excellent choice for a sustainable green business ecosystem because they can be minted on an eco-friendly blockchain, and at the same time, the developers can design them to gain constant revenue for multiple parties. Content creators and wildlife conservation organizations can gain constant revenue from reselling the assets. Another advantage is the speed of transfer of assets. The process of wildlife conservation can continue without interruptions if the funding is at a steady pace.

Because there are many variations of NFT smart contract implementations this model includes some of the important parameters:

tokenId – Token ID of the corresponding asset

owner – address of the owner of the asset (the creator of the smart contract is the owner initially)

artist – address of the artist (the designer of the asset)

foundation – address of the foundation where the money of the sale of the NFT will go.

value- the value of the asset

Some of the main functions that will execute when certain conditions are satisfied are the following:

buy (tokenId, value) – function for executing the payment

transferOfAsset(currentOwner,newOwner, tokenId)- function for transferring the ownership of the asset after the payment.

transferOfProvisionToArtist(tokenId, artist, price) – function for transferring the royalty to the artist from selling and reselling of the NFT

transferOfProvisionToFoundation(tokenId, foundation, price)- to transfer the money from selling and reselling of the NFT to the appropriate foundation.

The sustainable green business ecosystem is important to preserve endemic species. People interested in investing in wildlife conservation will tend to support eco-friendly businesses. The International Union for Conservation of Nature, the main international organization behind wildlife conservation, helps businesses, from extractives, energy and infrastructure to finance and agriculture, including forest and farm producers' organizations, investors, project developers and policymakers, implement practices that conserve nature and benefit people, whose lives and livelihoods depend on natural resources. The resources collected from the sales of NFT will create better habitat for the endemic species in more natural environment.

Even though the model is initial, this is probably the first model that covers in great detail the NFT technology in the domain of wildlife conservation and blockchain technology in that area. The elements of the model can be used as a resource for different entities. Developers can choose the appropriate technology consisting in the model for designing future projects. Future investors can utilize the model to help them support new startups. Also, regulators can use this classification in order to create future policies to enhance and enlarge the adoption of the technology in the context of preserving endemic species. Future research can create future classifications based of the proposed concepts in this model.

6 Conclusion

Wildlife conservation has come a long way since the last century. There were many initiatives for wildlife conservation. In this paper, we presented that NFT is a strong option for wildlife conservation. Many funds were collected by selling digital arts, collectibles, and games using NFT. NFT can attract a larger audience because it offers possibilities for any demographic. The development of decentralized applications is easy and, on the rise, thanks to the most used programming languages. The advantages the NFT gives is the decentralization, speed and security, and that can be crucial for future successful wildlife conservation projects.

References

- [1] Nakamoto, S., 2008 Bitcoin: A Peer-to-Peer Electronic Cash System
- [2] Yli-Huumo, J, Ko, D, Choi, S, Park, S, Smolander, K, 2016. Where Is Current Research on Blockchain Technology? —A Systematic Review, PLoS ONE 11(10): e0163477.
- [3] Nair P. R. and Dorai D. R., 2021, Evaluation of Performance and Security of Proof of Work and Proof of Stake using blockchain. 2021 Third International Conference on Intelligent Communication Technologies and Virtual Mobile Networks (ICICV) (pp. 279-283).
- [4] Yakovenko, A., 2020 Solana: A new architecture for a high performance blockchain v0.8.13

- [5] Zheng, Z., Xie, S., Dai, H.-N., Chen, W., Chen, X., Weng, J, Imran, M., 2020, An overview on smart contracts: Challenges, advances and platforms, *Future Generation Computer Systems*, (Vol.105, pp. 475-491)
- [6] Valeonti, F., Bikakis, A., Terras, M., Speed, C., Hudson-Smith, A., Chalkias, K., 2021, Crypto Collectibles, Museum Funding and OpenGLAM: Challenges, Opportunities and the Potential of Non-Fungible Tokens (NFTs), *Applied Science*, (Vol. 11, 9931)
- [7] Ethereum Improvement Proposals (EIPs) <https://eips.ethereum.org/>
- [8] Market Trends <https://nonfungible.com/market-tracker>
- [9] The Merge <https://ethereum.org/en/upgrades/merge/>
- [10] Solana Blockchain <https://solana.com/>
- [11] Polygon Blockchain <https://polygon.technology/>
- [12] Flow Blockchain <https://flow.com/>
- [13] Tezos Blockchain <https://tezos.com/>
- [14] OpenSea marketplace <https://opensea.io/>
- [15] Rarible marketplace <https://rarible.com/>
- [16] SuperRare marketplace <https://superrare.com/>
- [17] Foundation marketplace <https://foundation.app/>
- [18] NBA Top Shot marketplace <https://nbatopshot.com/>
- [19] World Wide Fund for Nature <https://www.worldwildlife.org/>
- [20] World Wide Fund for Nature Annual Report
https://wwfint.awsassets.panda.org/downloads/wwfintl_annualreview2020.pdf
- [21] United States Fish and Wildlife Service <https://www.fws.gov/>
- [22] United States Fish and Wildlife Service Annual report
<https://crsreports.congress.gov/product/pdf/IF/IF11470>
- [23] Federal Funding for Fish and Wildlife
<https://portal.ct.gov/DEEP/Wildlife/Federal-Funding-for-Fish-and-Wildlife#PR>
- [24] Ezemvelo KZN Wildlife <http://www.kznwildlife.com/>
- [25] Ezemvelo KZN Wildlife Annual report
https://provincialgovernment.co.za/entity_annual/711/2021-kwazulu-natal-ezemvelo-kzn-wildlife-annual-report.pdf
- [26] Mofokeng, M., Matima, Tk., 2018, Future tourism trends: Utilizing non-fungible tokens to aid wildlife conservation. *African Journal of Hospitality, Tourism and Leisure*, (Vol.7).
- [27] Satellite Rhino on SuperRare <https://superrare.com/artwork-v2/satellite-rhino-i-25142>
- [28] Richard Bernabe <https://richardbernabe.com/>
- [29] Ryan Hevern <https://www.ryanhevern.com/>
- [30] Simon Needham <https://www.simonneedham.com>
- [31] World Wide Fund for Nature Non-Fungible Animals <https://www.wwf-nfa.com/en>
- [32] How the World Wildlife Fund tried — and failed — to create an eco-friendly NFT
<https://www.theverge.com/2022/2/8/22923530/world-wildlife-fund-nft-polygon-layer-2-blockchain-energy-emissions>
- [33] Australia Zoo <https://www.australiazoo.com.au/>
- [34] Wildlife Warriors NFT <https://australiazoonfts.com/>
- [35] Australia Zoo launches NFT project to help protect wildlife on Algorand, the world's greenest blockchain.
<https://www.algonews.io/news/australia-zoo1.html>
- [36] Wildlife Warriors <https://wildlifewarriors.org.au/>
- [37] Wildcards <https://wildcards.world/#>
- [38] The Munchie Mafia <https://www.themunchiemafia.com/#>

Will Cryptocurrency replace money/cash?

Main Author: Emilija Vrangalovska
Co-Author: Sofija Baloska
Co-Author: Svetlana Mitrevska
Co-Author: Anis Sefidanoski

1. University of Information Science and Technology, St. Paul the Apostle, Ohrid
2. University of Information Science and Technology, St. Paul the Apostle, Ohrid
3. University of Information Science and Technology, St. Paul the Apostle, Ohrid

Abstract

Currencies have been evolving. From the first known form of currency almost 5,000 years ago, when people used it to exchange goods and services, to today, when the world revolves around money. In the world that has evolved, a new currency called Bitcoin has emerged, invented by a mysterious man named Satoshi Nakamoto, who imagined Bitcoin as a transaction sign used by would-be widely used around the world to protect against inflation. The purpose of this paper is to examine the functions and roles of money and to find out whether cryptocurrencies could exercise them.

Keywords: *Bitcoin, money, currency, Blockchain, money, cash, cryptocurrency.*

1. INTRODUCTION

Money is an economic entity that serves as a widely accepted medium of exchange in an economy for transactional purposes. Money serves the purpose of reducing transaction costs, namely the double coincidence of desires. Money is created as a commodity with a physical property that can be used by market participants as a medium of exchange. As society has changed over the years, the time has come when people needed a new way of exchanging goods and services and not just the classic cash society. Technology has taken center stage in recent years, particularly with the emergence and discovery of Blockchain technology. This technology provides a secure, distributed database that can function without the need for a central authority or administrator. The transaction, represented in a cryptographically signed block, is automatically validated by the network [1].

Bitcoin is the most famous example that is deeply connected to Blockchain technology. It is also the most controversial aspect because it enables a multi-billion-dollar market for anonymous transactions without government oversight. As a result, it must address a multitude of regulatory issues involving national governments and financial institutions. (Blockchain technology beyond Bitcoin) It has the same basic structure as when it was founded in 2008, but repeated instances of global market change have created a new demand for cryptocurrencies that is far greater than when it started. Users can digitally exchange value without the intervention of a third party by using a cryptocurrency. Cryptocurrency is based on the theory of solving encryption algorithms to generate unique hashes with a finite number of possibilities. This allows users to exchange hashes as if they were exchanging physical currencies when combined with a network of computers verifying transactions.

Before starting this article, it is important to understand the term cryptocurrency and what it means. So, what is cryptocurrency, in simple terms? According to investopedia.com:

“A cryptocurrency is a digital or virtual currency secured by cryptography, making it impossible to counterfeit or double spend. Many cryptocurrencies are decentralized networks based on Blockchain technology; a distributed ledger enforced by a diverse network of computers. A peculiarity of cryptocurrencies is that they are generally not issued by a central authority, which theoretically makes them immune to government interference or manipulation” [2]. While according to kaspersky.com, “Cryptocurrency, sometimes called cryptocurrency or crypto, is any form of currency that exists digitally or virtually and uses cryptography to secure transactions. Cryptocurrencies don't have a central issuing or regulating authority, instead using a decentralized system to record transactions and issue new units” [3]. Even though there can be many definitions explaining what cryptocurrency

means, we all agree that this is digital money, in short.

The first part of the paper provides a review and theoretical background of cryptocurrencies. The main focus of the research will be put on the comparative analysis of the fundamental roles and functions between money and cryptocurrencies. On the basis of the analysis, we can identify whether cryptocurrencies are capable to overtake the role of money. At the end of the paper, we summarize the main opportunities and potentials that cryptocurrencies provide in the payment system.

2. Review and theoretical background of cryptocurrencies

2.1. The idea and beginning of cryptocurrency:

Every decade has its notable invention and things for which it will be remembered. We may not know it, but the 80s was a time that brought great technological advances and new inventions like the personal computer, the artificial heart, the DNA fingerprint and the space shuttle among many other things. You may be wondering why we are discussing this, but this is the time when an idea came to life.

The idea of cryptocurrency started in the 80s when they planned to send a currency untraceable and not need centralized entities like banks to do it. It all started as a good idea that later had to be realized and implemented in everyday life.

David Chaum, an American cryptographer, implemented this idea in 1995 as anonymous cryptographic electronic money called Digicash. This early form of cryptographic electronic payment required user software to be withdrawn from a bank and required certain encrypted keys before they could be sent to a recipient. We can argue that even in the early years of new technological inventions, there was a time when people had big ideas for currency and money as well.

Nick Szabo designed Bit Gold in 1998 and is often cited as the direct precursor to Bitcoin. This new invention required a participant to expend computing power to solve cryptographic puzzles, and whoever solved the puzzle received the reward. By putting these two inventions together, we will have something similar to today's Bitcoin. What held Szabo down was that he couldn't solve the conundrum of the double-spending problem (digital data can be copied and pasted) without the use of central authority [4].

As Jei Young Lee said in his article "A decentralized token economy: How blockchain and cryptocurrency can revolutionize business" ,” The Economist [5] called blockchain ‘The Trust Machine’ and predicted that the blockchain will be performing reliable transactions without human intervention in the future. In human history, the issuance of money has always been controlled and managed by public authorities such as a central government. Bitcoin’s significance lies in the fact that it is a new currency system created by an anonymous developer in the private sector. Since there is no centralized issuing entity, a cryptocurrency is quite different from fiat managed money by the government.

As we have already seen the extreme price change of bitcoin in the past, cryptocurrencies may have limits in terms of monetary value stability. Thus, it could be premature to replace fiat money completely with cryptocurrencies. [6].”

2.2 Types of cryptocurrencies

Despite the fact that most cryptocurrencies use a blockchain-based infrastructure, there are some notable variances among them. Coins and tokens are the two main groups into which cryptocurrencies may often be divided [7].

•Coins and altcoins

Every cryptocurrency that employs a separate, autonomous blockchain is referred to as a coin. For instance, because it relies on its own infrastructure, Bitcoin is referred to as a "currency". The Ethereum blockchain is also used to run Ether.

Any cryptocurrency except Bitcoin is referred to as an "altcoin." Similar to how Bitcoin works, several other currencies also operate. Some, like Dogecoin, on the other hand, are quite unique. In contrast to Bitcoin, which has a limit of 21 million coins, Doge, for example, has an endless supply of coins.

•*Tokens*

Tokens are digital assets that are just like currencies and can be purchased and traded. Tokens, however, are a non-native asset, which means they rely on the setup of another network. They include TerraUSD, Chainlink, Uniswap, and Polygon, as well as the Ethereum-hosted Tether cryptocurrency.

2.3 Forms of cryptocurrency

To successfully introduce a new type of currency into widespread use, a thorough examination of the theoretical foundations of the issue is required, followed by legal research. The countries that are the first to implement a regulatory framework confirming the legitimacy of cryptocurrencies are Malta, Japan, Germany, China, Belarus, Georgia, Estonia, Slovenia, Gibraltar, Switzerland, Singapore and many more. These countries welcome cryptocurrencies' business and organizational capabilities.

There is currently no widely accepted system for classifying digital currencies, but the systematization of the data obtained will allow for a more in-depth study of this phenomenon. To forecast the potential future of cryptocurrencies, distinguish between their origin, purpose, functions, and properties.

The author of this article Alexey Mikhaylov [8] has classified the cryptocurrency based on their purpose of creation and original code:

“Cryptocurrencies can be classified depending on their purpose of creation. The following types are distinguished:

1. Target cryptocurrencies, the nature of the origin of which is a specific intention of the developers. These digital currencies have an original purpose.
2. Non-targeted—the creation of such cryptocurrencies most often occurs involuntarily, as a result of software failure and a branch of the development scheme of the indigenous digital currency. This rebuilding of the system is called a fork.

By the original code, they are distinguished as:

1. Original digital currencies—the process of their creation began with a completely new code, different from the previously used cryptocurrencies.
2. Forks—modernization or strong change in the source code of a certain existing cryptocurrency to create a new one—a subsidiary .”

2.4 The future of cryptocurrency according to experts

In one Consumer News and Business Channel article that has been published on July 5, 2021, the journalist Annie Nova asked some experts from a variety of fields to describe their vision for the currencies 50 years from now. The answers have been edited by CNBC for clarity. Purposely for this paper they have been quoted as followed [9]

•*Ivory Johnson*, certified financial planner, and founder of Delancey Wealth Management

“Cryptocurrencies will disrupt traditional finance because one of their most attractive utilities is the ability to efficiently transfer payment across borders with little to no cost, delay or foreign currency fluctuations. Concerning Bitcoin, 50 years is a long time and Bitcoin could either become the world

reserve currency or the next AOL that made a lot of people wealthy until it was unseated by better technology.”

- *Frederick Kaufman*, author of “The Money Plot: A History of Currency’s Power to Enchant, Control, and Manipulate”

“Way before 2071, the dollar will have more in common with crypto than with silver or gold, so there is no need to doubt the longevity of encrypted algorithms as stores of value and media of exchange. All money is a form of encryption. It’s been that way from the start, and as our lives converge ever more closely with the digital universe, the drive to invest in tokens will only accelerate. Ironically, that impulse will connect us to primitive instincts, and do its part to keep us human.”

- *Dan Egan*, vice president of behavioural finance and investing at Betterment

“Cryptocurrencies like Bitcoin have proven themselves useful for money movement and speculation, and they’re unlikely to go away. But where and how we’ll generate the energy to meet the demand of a growing crypto market is worth considering, as well as whether state actors who view it as a competitor to fiat power will make it even more of a black-market commodity.”

- *Dragan Boscovic*, founder and director of the Blockchain Research Lab at Arizona State University

“Central bank authorities are busy developing regulations on cryptocurrency. They recognize that digital currencies are native to the digital economy and, as such, are on their way to becoming mainstream in the next 10 years.”

- *Barbara Roper*, director of investor protection for the Consumer Federation of America

“Sorry. I decided a while back that I’m too old for this issue.”

2.5 Advantages of Bitcoins compared with existing currencies

As per his supporters, this currency has two advantages that make him more suitable than the existing currencies.

Firstly, Bitcoin’s supply is limited, thus making it impossible for a central authority to issue it in quantities that would devalue it. However, a limited supply can also be a weakness, since it makes it impossible to control deflation, a phenomenon that can also lead to very severe economic consequences [10].

Secondly, every transaction is permanent and immutable. Let's say that a certain amount of money is held in a bank account, that bank account could theoretically expropriate the money from its user and claim that it never existed. However, with Bitcoin, this theory is impossible because the database on which the transactions are recorded cannot be edited by any central authority. This currency is often referred to as trustless as it does not require its holders to trust any financial institution lest be expropriated.

Nevertheless, the main benefit of Bitcoin is its anonymity, thus allowing it to be used for breaking the law with a reduced risk of prosecution. A 2019 study found that 46% of all Bitcoin transactions involved illicit activity, accounting for approximately \$76 billion per year [11]. The most common forms of illegal activity involving Bitcoin are buying illegal drugs and money laundering. It is also commonly used to solicit anonymous payments during blackmail and extortion schemes.

2.6 Disadvantages of Bitcoin compared to existing currencies

In economic theory, money is said to have three main functions: a medium of exchange; a store of value, and a unit of account. As per the previous discussion in regard to the advantages of Bitcoin, this currency is an excellent medium of exchange for transactions that require anonymity. However, it is prohibitively expensive for other transactions. On average, the transaction fee in 2020 ranged from 28 cents on January 2nd to 13.41 US dollars on October 31st.

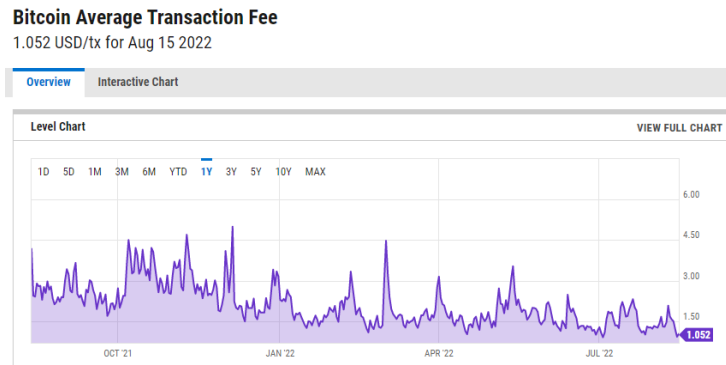


Figure 1: Bitcoin Average Transaction Fee [12]

In addition, Bitcoin can be transferred without going through a third party such as a crypto exchange, which poses a logical challenge for those without background knowledge in computer science. Therefore, most traders use an exchange or virtual manager by a third party. However, this means that the currency is no longer trustworthy and Bitcoin holders have historically lost large sums of money to unwary or fraudulent third parties.

3. Comparative analysis of main functions and roles between money and cryptocurrencies

In this part of the paper, we will mainly focus on the functions and roles between money and cryptocurrencies according to a monetary dialogue paper from the European Parliament's Committee on Economic and Monetary Affairs [13].

Money is something that people use every day. We earn and spend, but we don't think about it often. Economists define money as any commodity that is widely accepted as the final payment for goods and services.

Firstly, we need to understand the functions and role of money which can be divided into three layers:

- Primary function relates to the medium of exchange and measure of economic value.
- Secondary function relates to value, and standard of payments.
- Tertiary functions relate to basis of credit, liquidity to wealth, distribution of income, measurement and maximisation of utility.

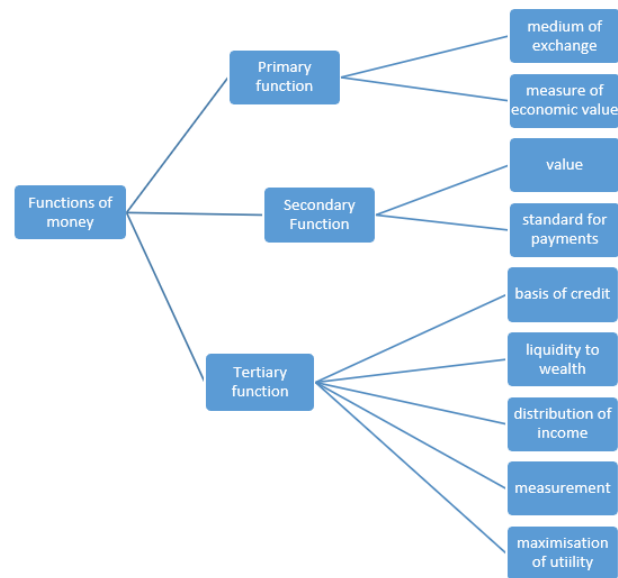


Figure 2: Functions of money

In the economy, money plays three roles, this will later help us understand whether digital currencies can become money or not, by analysing how they can fulfil these three different roles:

3.1 Medium of exchange

The most common function attributed to money is as a medium of exchange, a means of purchase, and trade of goods, thus eliminating the need for a double coincidence of demand as in barter. Anyone who wants to sell wheat in exchange for rice can sell it for money and buy rice. This means that money is extensively accepted as a system of payment.

3.2 Measure of value

Money also serves as a general measure of value. The value of various commodities is expressed in money. This measurement is accepted and standardized all over the world. Money as a measure of value has made transactions easy and fast. Currencies also serve as units of account. In a barter economy, the price of a good or service must be established in relation to all other goods or services produced and exchanged.

3.3 Store of value

People store cash for rainy days and to deal with unexpected circumstances. Furthermore, according to Keynes, people also hoard money to take advantage of changes in interest rates. Thus, money preserves value over time and space. Money as a store of value involves deferring future consumption and therefore the link between present and future is important. In this regard, money becomes an "asset" because it is a claim. This is the most convenient way to request these goods and services. Therefore, instead of holding their assets as liquid assets (houses, stocks, etc.), people prefer keep their wealth in the form of money.

Money, also known as currency or cash, is the most liquid form of asset since it can be instantly and cheaply exchanged for goods and services, and because its value is stable, at least temporarily. All assets, including bonds, savings accounts, treasury bills, government securities, inventories, and real estate, serve as stores of value, but their liquidity varies. Currency is stored in advanced economies as bank deposits.

4. *Digital currencies*

To determine whether digital currencies can be considered money, we need to see how they handle the roles that money has historically played. So far, limited evidence has been collected which indicates that digital currencies are mainly used as storage of value rather than as a medium of exchange. Currently, there is not much evidence of digital currencies being used as a unit of account.

According to a study [14] [15], anybody with an internet-enabled computer or device could make digital currencies serve as money. Nevertheless, this feature sometimes occurs, only for a small number of users and to some extent and it is always in line with users' traditional currencies. Rather, digital currencies review a speculative investment similar to internet stocks in the late 1990s.

4.1 *Digital currencies as a store value*

It is necessary to distinguish between the long-term and the short-term in order to study the use of digital currencies as a store of value. For an asset to become a long-term store of value, it is essential to know what to expect from its future supply and demand. The supply of digital currencies is fully guaranteed due to the algorithmic nature of the production process; however, demand is more uncertain.

Secondly, the public's belief that digital currencies will continue to be required is crucial for them to function as a store of value. Therefore, the value of digital currencies as a long-term store of value is directly linked to their needs and this is linked to the user's perception of success in the future of this currency. However, in the short term, it is difficult for digital currencies to act as a store of value. These currencies have highly volatile exchange rates relative to traditional currencies.

Another issue when considering digital currency as a store of value is safety. It is very important to protect them against theft since they are not physical, they cannot be hidden in a "secret place" in our homes. Rather they need to be stored in computer accounts known as "digital wallets". Although the consumer is the one that needs to be in charge of the safety of the wallet, they sometimes contact some insurances that can take over their safety.

4.2 *Digital currencies as a medium of exchange*

As long as retailers accept their payment, concurrency can be used as a medium of exchange. Over the years, the number of retailers that are willing to accept this kind of payment is increasing. Nevertheless, just because retailers accept these currencies does not guarantee that they will be widely utilized. To determine if a digital currency is truly a medium of exchange, the volume of transactions in these currencies must be tracked over time.

The fixed supply is one downside that can make digital currencies a medium of exchange. Therefore, it is not possible to avoid the obligation of having digital currency before purchasing products and services from a merchant. Thus yet, there are no digital currency credit cards or consumer loans.

4.3 *Digital currencies as a unit of account*

There is a limited indication that any digital money is being employed as a unit of account. The excessive volatility of digital currency exchange rates is also an issue when it comes to being a usable unit of account. For example, the value of a Bitcoin in comparison to other currencies fluctuates dramatically basis daily. Retailers must recalculate pricing basis regularly, which may be costly and complicated. Because digital currencies have unpredictable market value, they would be impossible to utilize as a credible reference point for establishing consumer pricing.

Another aspect of difficulty for digital currencies to become units of account is the fact that merchants quote the prices in more than four decimals. Mathematically this does not cause any problem, however, consumers find the decimal points to be challenging.

5. *Results of the analysis*

Based on the analysis in the previous paragraphs, digital currencies barely fulfil the requirements associated with the functions of money. As a result, digital currencies do not appear to act as money in the economy and may pose certain concerns if extensively adopted in the long term. Then, in their current state, these types of currencies are highly unlikely to be the primary form of money for the economic system. Additionally, other concerns that may arise are connected to the fact that people are not very familiar with the technology, applications are not very user-friendly, they are not very safe in comparison to deposits, and their exchange rates are highly volatile [15].

Furthermore, digital currencies lack several additional characteristics associated with money in the economy. Digital currencies, for example, cannot be held as bank deposits; instead, they are often part of "digital wallets," which are subject to several hazards and expenses. As with deposits, there is no standard insurance for these wallets. Additionally, digital currencies are not legal tender for loans or mortgages. No credit or credit cards are issued in digital currency [14].

Digital currencies, unlike traditional money, are not a claim therefore they may be considered a commodity. They are, however, immaterial, not physical like gold. Digital currencies may only be utilized if users consent to do so. The fact that they are not a central bank obligation does not prevent them from functioning as money, but it distinguishes them from cash and notes [15].

Digital currencies are analogous to older types of money in several aspects. For example, the central bank does not control its supply, and payments are done directly, without the use of an intermediary. In Figure 3 we can see the difference summarized in a table.

Functions and roles	Money	Cryptocurrencies
Medium of exchange	Universally accepted	Accepted by a small number of retailers
Unit of account	Fiat currency (e.g American dollars)	Own unit of account
Store of value	Stable, consistent with the central bank price stability mandate	Tend to be volatile, depending on the market price

Figure 3: Comparison between money and cryptocurrencies

6. CONCLUSION

Cryptocurrency will become much more stable as it develops, making it easier to transfer and a store of value that will increase its use by businesses, the government, and everyone else in daily life. Although cryptocurrency is still in its infancy and some people are still dubious of it, it is here to stay, has been incorporated into our lives, and will eventually become a universally accepted form of payment. It is simply a question of time. The acceptability of cryptocurrency and how frequently it is discussed indicate that it has a promising future.

On the other hand, there are still several significant challenges and obstacles that must be overcome before cryptocurrencies can become a mainstream alternative to cash/money. One of the most significant challenges is regulatory uncertainty, with many countries and jurisdictions grappling with how to classify and regulate cryptocurrencies. In addition, cryptocurrencies still face issues related to scalability, usability, and volatility, which can make them challenging for some users to use and accept as payment.

It is possible that cash will be replaced by other forms of currencies, however, to this day we still do not know the correct answer to this question. It is clear that cryptocurrencies represent a significant

innovation in the world of finance and have the potential to transform how we think about and use money.

References

- [1] Angraal, S., Krumholz, H. M., & Schulz, W. L. (n.d.). Blockchain technology - circulation: Cardiovascular quality and outcomes. ahajournals.org. Retrieved March 20, 2023, from <https://www.ahajournals.org/doi/10.1161/CIRCOUTCOMES.117.003800>
- [2] Frankenfield, J. (2023, February 23). Cryptocurrency explained with pros and cons for investment. Investopedia. Retrieved March 20, 2023, from <https://www.investopedia.com/terms/c/cryptocurrency.asp>
- [3] Kaspersky. (2022, February 9). What is cryptocurrency and how does it work? www.kaspersky.com. Retrieved March 20, 2023, from <https://www.kaspersky.com/resource-center/definitions/what-is-cryptocurrency>
- [4] Cointelegraph. (2022, October 21). How and when did bitcoin start? the complete bitcoin history. Cointelegraph. Retrieved March 20, 2023, from <https://cointelegraph.com/bitcoin-for-beginners/the-history-of-bitcoin-when-did-bitcoin-start>
- [5] The Economist Newspaper. (n.d.). The trust machine. The Economist. Retrieved March 20, 2023, from <https://www.economist.com/leaders/2015/10/31/the-trust-machine>
- [6] Jei Young Lee, A decentralized token economy: How blockchain and cryptocurrency can revolutionize business, Business Horizons, Volume 62, Issue 6, 2019, Pages 773-784, ISSN 0007-6813, from <https://www.sciencedirect.com/science/article/pii/S0007681319301156>
- [7] 10 popular types of cryptocurrency and how they work. N26. (n.d.). Retrieved March 20, 2023, from <https://n26.com/en-at/blog/types-of-cryptocurrency>
- [8] Alexey Mikhaylov | Head of LAB | Phd - researchgate. (n.d.). Retrieved March 20, 2023, from <https://www.researchgate.net/profile/Alexey-Mikhaylov>
- [9] AnnieReporter. (2021, July 5). Here's what cryptocurrencies will look like in 50 years according to experts. CNBC. Retrieved March 20, 2023, from <https://www.cnbc.com/2021/07/03/what-cryptocurrencies-will-look-like-in-50-years.html>
- [10] BIS working papers - Bank for International Settlements. (n.d.). Retrieved March 20, 2023, from <https://www.bis.org/publ/work186.pdf>
- [11] Sean Foley, Jonathan R Karlsen, Tālis J Putniņš, Sex, Drugs, and Bitcoin: How Much Illegal Activity Is Financed through Cryptocurrencies? The Review of Financial Studies, Volume 32, Issue 5, May 2019, <https://doi.org/10.1093/rfs/hhz015>
- [12] Bitcoin average transaction fee (I:BATF). Bitcoin Average Transaction Fee. (n.d.). Retrieved March 20, 2023, from https://ycharts.com/indicators/bitcoin_average_transaction_fee
- [13] Virtual money: How much do cryptocurrencies alter the fundamental ... (n.d.). Retrieved March 20, 2023, from <https://www.europarl.europa.eu/cmsdata/207652/12.%20PE%20642.360%20LSE%20final%20publication-original.pdf>
- [14] Yermack, D. (2014, October 28). Is bitcoin a real currency? an economic appraisal. EconPapers. Retrieved March 20, 2023, from <https://econpapers.repec.org/RePEc:nbr:nberwo:19747>
- [15] The economics of digital currencies - Bank of England. (n.d.). Retrieved March 20, 2023, from <https://www.bankofengland.co.uk/-/media/boe/files/digital-currencies/the-economics-of-digital-currencies>

Modern Threats in Online Social Networks, Privacy Solutions offered by OSN Providers and Commercial Solutions

Marija Bukalevska[†], Aleksandar Karadimce[‡]

Email(s): marija.bukalevska@mir.uist.edu.mk
aleksandar.karadimce@uist.edu.mk

[†] Faculty of Applied IT, Machine Intelligence and Robotics, University of Information Science and Technology “St. Paul the Apostle”, Ohrid, 6000, Macedonia

[‡] Faculty of Information and Communication Sciences, University of Information Science and Technology “St. Paul the Apostle”, Ohrid, 6000, Macedonia

Abstract

Online social networks (OSNs) have significantly increased in popularity over the past few years due to the rapidly developing and continually evolving technology. The main driver of this trend is the potential of OSNs to give people a channel for connection with their loved ones as well as the opportunity to make new acquaintances, engage in conversation with like-minded people, and exchange ideas and thoughts. Given the vast amount of information shared on social networks and how quickly this information spreads, attackers are drawn to it wanting to exploit the information to harm others while also gaining personal advantage. Security and privacy issues are brought up by the user's shared information, especially when the user uploads sensitive media like photos, videos, and audio. The attacker can nefariously use shared information for improper ends, which could result in the user suffering substantial damage. Attackers target social networks for their own advantage for a variety of reasons, including impersonation for amusement or fraud, money theft via getting a credit card and financial information illegally, theft of other personal information, and other ways to illegally obtain information of users. This paper, written with the general reader in mind, will provide a review of modern security threats on OSNs and existing solutions to privacy risks and security threats provided by OSN platform providers and commercial solutions.

Keywords

Online Social Networks, Modern Threats, Solutions to OSN threats, Social Networking Platforms, Privacy settings, Authentication factors, and Commercial Solutions.

1 Introduction

Social networking services have significantly grown in popularity among people of all ages in recent years. With the emergence of many social networking services like Facebook, Twitter, Instagram, YouTube, and Whatsapp, social networking has become a worldwide phenomenon and trend, with many individuals signing up as users on these networking platforms, thus creating large user bases. Social networks have mostly replaced the use of email and the phone as traditional forms of communication. People can stay in touch by exchanging photos and stories, and in most situations, they will also exchange personal information. Additionally, users spend much

time conversing, playing games, and making friends on these websites. Social networks have ingrained themselves into people's daily lives.

These websites and applications are so popular because social networking allows users to meet new individuals from all over the world. Since the majority of well-known social networking sites, like Facebook, Twitter, LinkedIn, and MySpace, are free, anyone may easily access them. Users of these websites have access to millions of profiles from across the globe. Due to the introduction of profiles on social networking sites, people may now learn more about a person before connecting with them. Popular social networking sites have incredibly user-friendly designs. Because most websites are so easy to use, very little internet knowledge is needed. Compared to more conventional forms of communication like face-to-face meetings and email, they provide a more effective means of communication. Even more, people can interact through these mobile versions of social networking sites because they are so user-friendly. On the majority of well-known social networking sites, users can create groups. In these communities, people can meet others who share their hobbies and interests. On social networks, communications are very dynamic, interactive, and yet personal.

On the other hand, despite social networks' popularity and positive traits, the widespread use of these platforms brings risks and threats.

Users' security and privacy are in danger to a greater extent the more information you disclose on social networking platforms. Social media can put private information in danger, despite being useful for communicating with family and friends. People create social network accounts that could reveal their private information. Each user's data is accessible to malicious attackers who can misuse it for their benefit. Personal information such as emails, passwords, credit card details, phone numbers, social security information, relationship status, religious beliefs, and more are examples of personal data that attackers can exploit and misuse. There are numerous ways to obtain personal information illegally. Malware, phishing scams, internet fraud, clickjacking, de-anonymization, and other methods can all be used to do this. Other times, users put themselves in danger by disclosing their locations and whereabouts on social networking sites. This allows individuals to find users in person or gives criminals the chance to target a property while the owners are away. Our study aims to inform users of social networks and increase their knowledge about the privacy and security options offered by the platforms they use. Users can customize these options to their preferences and provide as little or as much information about themselves on these networks as they prefer. This way users can better protect themselves and their personal information from any malicious activities and people. It also offers insights about commercial companies' solutions that can help in better protection and add more layers of security to their profiles and personal information. The paper is outlined as follows: Section 2 lays out the related work. Section 3 describes the numerous modern threats to which OSN platform users are exposed. Furthermore, Section 4 discusses the solutions provided by OSN service providers, focusing on the privacy settings and authentication mechanisms in social networking platforms. Section 5 covers some commercial solutions regarding security and privacy on OSN platforms. Section 6 discusses the results and outcome of this study. Section 7 concludes the paper.

2 Related Work

We defined OSNs and discussed the factors contributing to their popularity in a previous study [33]. We also spoke about the security and privacy concerns surrounding OSN platforms. Furthermore, we described traditional threats that OSNs are subject to and provided a table based on our research that provides data on whether popular OSNs have been subject to traditional threats.

Jain, Sahoo, and Kaubiyal [1] discuss a number of issues regarding privacy and security on social networks, as well as existing preventative methods that can help protect users. This study also looks at OSN's popularity, advantages, and disadvantages, as well as its major difficulties and suitable security measures for safeguarding account information.

The paper [2] presents a classification into groups of social networks according to their purpose, and it also covers potential security threats to social networking. Additionally, they discuss the importance of passwords and give several recommendations when it comes to choosing passwords. Likewise, they provide a definition of risks and vulnerabilities that can be exploited by threats and provide steps and suggestions for dealing with threats that users face on social networking sites.

A taxonomy of many security threats that endanger the safety of OSN users and children was presented by Fire, Goldschmidt, and Elovici [4] along with an overview of the solutions provided by OSN platform operators, commercial manufacturers, and academic solutions that have been put in place to enhance OSN user privacy, security, and protection.

By offering a classification and description of threats, the paper [6] provides a thorough examination of various security and privacy threats that target every user of social networking sites. They presented recent attack statistics and security reports from a variety of security organizations and blogs to better understand the dangers related to security and privacy issues. Additionally, they emphasize many risks and threats that result from the sharing of multimedia information on social networking sites. They also talk about current defense strategies that can shield users of social networks from these threats.

The authors [7] aim to draw attention to certain security issues that social network users may face. They suggest an algorithm and a model to address security issues that are broken down into user authentication, data confidentiality, and data integrity. They provide a discussion of their results by explaining their proposed algorithms for authenticating account owners based on behavioral profiles.

3 Modern Threats

We discussed traditional threats on OSN platforms in another paper [33]. In this paper, we will focus on threats that can affect OSN platforms and users. In the category of modern threats, we have clickjacking, de-anonymization attacks, fake profiles (social bots), identity clone attacks, inference attacks, information leakage, and location leakage. Other authors add to this category of face recognition and software [3][4][25].

Clickjacking - "clickjacking" involves tricking the user into clicking on a link different from the one they intended to click on [1]. This can lead users to unintentionally download malware, visit fraudulent and deceptive websites, disclose sensitive information, make online purchases, and more. The clickjacking attack comes in a variety of forms, including likejacking, cursor-jacking, drag-and-drop, strokjacking, and others [2][14]. The Twitter social network was the target of a major clickjacking attack about ten years ago that quickly propagated a message, making use of people's inherent curiosity to get them to click on a link. Tweets that contained the

words "Don't click" and a link spread quickly across thousands of accounts on Twitter. A tweet was posted from the users' accounts when they clicked the link. The malicious link was posted along with the message "Don't click" in that tweet. The attack itself turned out to be harmless, and it served as a warning about the possible risks associated with Twitter clickjacking efforts [16].

De-Anonymization - In social networks, anonymization enables individuals to conceal information that might identify them. These details could contain things like their names, photos, addresses, and other private information. The purpose of this anonymity is to shield users from third parties who might violate their privacy, such as advertising, program developers, and data mining researchers. However, some studies have demonstrated that it is possible to de-anonymize users of online social networks [7]. A third party can easily determine a user's real identity by simply combining the data made public by several social networking sites [1]. By combining limited but shared data sets with readily available online data sets, de-anonymization reverses the anonymization process. Data miners can extract some data from each set of accessible data to piece together a person's identity. To find out a user's name and typical activities, for instance, a data miner might retrieve data sets supplied by a telecommunications firm, a social media website, an e-commerce platform, and other sources [12]. By employing techniques like tracking cookies, network topology, and user group memberships, these attacks aim to determine the user's true identity [3].

Fake profiles (social bots) – Due to the openness of social networking sites, malicious parties are able to take advantage of the service by setting up various fake profiles to engage in illegitimate, hostile, illegal, misleading, or harmful activities like spamming, promotion and advertising, stalking, bullying, defamation, etc [5]. Online bots, commonly referred to as web robots or simply bots, are computer programs that quickly and automatically carry out a variety of tasks that would be impossible for a human to carry out on their own [5]. There are five categories of fake bots based on their functionality: spam bots, social bots, like bots, influential bots, and botnets. Social bots are very complex automatic or semi-automatic computer programs that create profiles that imitate human behavior in OSNs [4][5]. Fake profiles are frequently used to gather user personal information from social networks. The social bots can obtain a user's private information that should only be visible to the user's friends by sending friend requests to other OSN users, who frequently accept the requests. Fake profiles can also be used to launch sybil attacks, distribute spam, or even alter OSN statistics [4]. In 2018 Facebook claimed that it deactivated around 1.3 billion "fake" accounts over the previous two quarters, many of which were bots used "to propagate spam or carry out illegal operations like a fraud"[17].

Identity clone attacks - Identity profile cloning is a method by which hackers make a fake profile using pictures, videos, and other private data that has been taken from the original profile of a targeted user. Attackers might create a duplicate user profile that closely resembles the target's profile, more so if the majority of the user profile is set to the public [2]. The attacker can set up this duplicate profile on the same or a different social networking site to build a relationship of trust with the friends of the legitimate user [1]. Malicious people carry out these attacks in order to gain more personal information about the victim and the victim's friends, spread spam, or engage in other types of fraud like stalking, defamation, and financial theft [5]. A wave of fake Twitter accounts claiming to be banks began to appear, responding right away to clients who had tweeted their own bank to ask for assistance. Many users unknowingly sent their bank account information and security details to

the fraudulent accounts via direct messages because they looked exactly like the legitimate accounts, had names that were very similar to those of the legitimate accounts, and were frequently the first to respond to the original question [18].

Inference attacks - Using additional details that have been made public about the user on OSNs, an attacker can predict the user's private sensitive information, which the user has not decided to share, including their sexual preference and religious beliefs [4] [6]. Data from a user's friends list and network topology are two examples of publicly accessible SNS data that an attacker can mine for this purpose [6]. Consider the following simplified scenario: Facebook data collection includes user variables such as gender and self-declared political opinions. Assume that Alice, the user, has her profile set to private. According to the Facebook group information, Alice is a member of four organizations: Crochet Mastery, the National Coalition for Health Care, Health Care for America Now, and Hand Embroidery. The group-based classification model can correctly predict Alice as a female and a liberal based on these available public data. There are substantial privacy consequences from the stated inference issue. OSN users are less likely to hide their friendship links, but even if they do, those links can still be built through the backlinks from their friends with public profiles. Inference attacks on OSN users may also be driven by the attackers' own self-interests, such as targeted advertising, insurance screening, email phishing, or political surveillance [11].

Information leakage - With features like status updates, friend requests, photo and video uploads, third-party applications, and links to other websites, typical OSN sites are possible channels for information leakage [8]. If attackers mine this data, it could result in an information leakage attack [25]. Examples of how information leakage can be caused include: careless acceptance of friend requests from strangers could lead to the appearance of malicious individuals with bad intentions on your friend list rather than real friends. Openly accessible photo albums and videos provide anyone access to materials that can be sensitive in nature and put the user's security and privacy at risk [8].

Location leakage - On online social sites, many users share their location-related information. Many people willingly share this information, but sometimes users of social media also unknowingly expose their location information by uploading photos and videos that contain geotags about their present and prior locations without their knowledge, making it possible to determine where they are [4]. In addition to the city or geographical area you're in, certain geolocation tags may provide the precise address of your location. In other words, if you share your location on social media, everyone who can see your posts could be able to locate you in person. If you have kids, they might be using social media to share their whereabouts, which puts them at risk of unwanted attention from strangers. Oversharing could put your assets in danger because, for instance, if you post that you're on vacation, you're essentially letting everyone know that you're not at home. If criminals know where your home is, including identity thieves, they may use this as an opportunity to target it [19].

4 Solutions to privacy risks and security threats provided by OSN platform providers

Various authors [2][9][10] discuss basic anti-threat strategies and solutions in regard to threats on online social networking platforms.

Other authors [1][3][4][6][25] discuss various solutions regarding privacy and security threats on online networking platforms, including solutions provided by platform operators, commercial solutions, and academic solutions.

In this section, we focus on solutions provided by platform operators, in particular authentication mechanisms and privacy and security options on OSN sites and applications.

4.1 Authentication factors

OSN providers make an effort to keep their users safe by turning on security features, including user authentication mechanisms and user privacy options [4].

A unique type of security credential known as an authentication factor is used to confirm a user's identity and authorization before allowing them access to, or authorizing them to send messages to, or request data from, a secured network, system, or application [13]. A person must provide a certain type of evidence known as an authentication factor to demonstrate their identity [15].

There are three main authentication factors [15]:

- **Knowledge factor** – something you know (e.g., passwords, security questions, PIN)
- **Possession Factor** – something you have (e.g., mobile phone, token, smart card, SIM card)
- **Inherence Factor** – something you are (e.g., fingerprint, face recognition, iris recognition)

The three primary authentication factors are mapped with popular online social networks in the table below, demonstrating which authentication factors these social networking platforms feature.

Table 1: Popular OSN platforms mapped with the authentication factors they feature

Authentication factors	Facebook	Instagram	Twitter	LinkedIn	WhatsApp	Viber	Telegram
Knowledge factor	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Possession factor	Yes	Yes	Yes	Yes	No	No	No
Inherence factor	Yes	No	No	Yes	Yes	No	Yes

The knowledge factor (something you know) is the most frequently used factor, and it might be a password, a basic PIN (PIN), or even a security question [20]. Strong passwords should always be used when using passwords. An effective password combines capital and lowercase letters, numbers, and special characters. Personal information like a user's name or username shouldn't be included in passwords. Furthermore, a dictionary word should not be used as a password. A dictionary attack searches all the words in a database that resembles a dictionary for matches [20].

All the social networking websites and applications in the table have the knowledge factor because all of them require a password (Facebook, Instagram, Twitter, LinkedIn, Snapchat) to create an account and to log in to it, whereas PINs on WhatsApp and Viber and a password on Telegram are used as a part of two-factor authentication to add more security to the account, but are not required to create an account on these apps.

The possession factor (something you have) refers to objects like tokens or smart cards that can be carried around [20]. According to Table 1, the social networks Facebook, Instagram, Twitter, and LinkedIn have the possession factor. As a part of their two-factor authentication option, the mentioned networks require users to

choose to authenticate their identity by using an authentication app or by sending a text message (SMS) code to the user's phone. In this case, the SIM card with its specific phone number that belongs to the user is the possession factor. As for the rest of the networks – Whatsapp, Viber, and Telegram don't have this factor.

The Inherence factor (something you are) refers to biometric techniques. Among all the authentication factors, the Inherence Factor is frequently regarded as the strongest one. The Inherence Factor requests that the user provides evidence of their identity that is inherent in their distinctive features [15]. Fingerprints, hand geometry, retinal or iris scans, handwriting, and voice analysis are a few examples of biometric techniques that can be applied [20]. Given the table, Facebook, LinkedIn, Whatsapp, and Telegram have the option for biometric authentication, while the other networking platforms don't have that option.

4.2 Authentication mechanisms on social networks

CAPTCHA - Hackers are employing more complex automated programs to exploit security systems. CAPTCHAs are intended to eliminate this danger. This authentication approach looks to ascertain whether a user is indeed human rather than verifying a specific user. The acronym CAPTCHA stands for "completely automated public Turing test to tell computers and humans apart," and it was first used in 2003. The user is presented with a distorted image of letters and numbers by the system, and they are instructed to enter what they see. These aberrations are difficult for computers to handle, but people can usually identify them. By adding a CAPTCHA, you may further protect your network from automated hacking tools [22].

Multi-Factor Authentication (MFA) – It is an authentication technique that necessitates the usage of two or more distinct methods of user identification. Examples include the user's smartphone's generated codes, Captcha puzzles, fingerprints, voice biometrics, or facial recognition. Users' trust is increased by MFA authentication methods and technologies since they add several layers of protection [23].

Password authentication - The requester must remember what he knows in order to receive this kind of authentication. This technique consists of two parts. The user must first enter their username and then their password. The password is a secret combination of letters, numbers, and symbols that the user knows [21].

Two-factor Authentication – Also commonly referred to as 2FA. It is an additional security measure used to confirm that users attempting to log into an online account are who they claim to be. A user must first enter a username and password. After that, they won't be granted access right away but rather will need to supply further information [24]. The following categories that could be responsible for the second factor are the ones we previously explained and mentioned above: something you know, something you have, and something you are.

Biometric authentication - A method of identifying a user and/or verifying their identity based on the measurement of their distinctive physiological attributes or behavioral characteristics is known as biometric user authentication. Fingerprint, facial recognition, iris scanning, hand geometry, and retina scanning are examples of physiological biometrics. Voice recognition, gaits, keystroke scanning, and signature scanning are all behavioral biometrics. One biometric technique that is currently most frequently used is fingerprint recognition [21].

Certificate-based authentication - Digital certificates are used in certificate-based authentication solutions to identify individuals, machines, or devices. A digital certificate is an electronic document that is modeled like a passport or a driver's license [23]. Digital certificates essentially guarantee to the recipient of communication

that the message is originating from a specific individual by sharing public key and private key information. To promote safer communication and stop fraud on the Internet, the digital certificate verifies the sender's identity. Digital certificates protect private data by encrypting your communications, such as emails, logins, or online banking transactions, preventing the information from being seen by unauthorized people [21].

The table below outlines the user authentication methods used by the social networks shown in the table.

Table 2: Authentication methods used on various OSN platforms

Authentication methods	Facebook	Instagram	Twitter	LinkedIn	Whatsapp	Viber	Telegram
CAPTCHA	Yes	Yes	Yes	Yes	No	No	No
Multi-factor authentication	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Password/PIN	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Two-factor authentication	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Biometric authentication	Yes	No	No	Yes	Yes	No	Yes
Certificate-based authentication	No	No	No	No	No	No	No

According to Table 2, we can note that CAPTCHA is used by all OSN platforms apart from the instant-messaging applications Whatsapp, Viber, and Telegram. All platforms employ password/PIN, two-factor, and multi-factor authentication. As opposed to this, only Facebook, LinkedIn, WhatsApp, and Telegram support biometric authentication. None of the aforementioned platforms use certificate-based authentication.

4.3 Privacy and security settings in OSNs

A previous study [26] has identified various privacy options that social media platforms provide for users to sign in and participate in privacy-related activities. Our study has expanded the range of privacy and security settings on OSN platforms and includes whether these platforms have that privacy setting by stating "yes" or "no".

By exploring and looking into the privacy settings that social networking platforms provide, we created Tables 3 and 4, in which the privacy and security settings are listed and compared. There are two separate tables for the networking platforms. Users of Table 3 networking platforms can post a wide range of content on their profiles, including text, information, images, videos, and other types of multimedia. The platforms in Table 3 allow users to add links to their other social media accounts and to share more personal information that might be visible to the public.

Table 3: Privacy and security settings on Online Social Networking platforms

Privacy settings	Facebook	Instagram	Twitter	LinkedIn
Set up public/private profile	Yes	Yes	Yes	Yes
Choose who can see the content you post and share	Yes	Yes	Yes	Yes
Disable/limit who can comment/reply on your post	Yes	Yes	Yes	Yes
Show/hide activity status	Yes	Yes	/	Yes
Disable seen option	No	No	Yes	Yes

Discoverability(by email/phone number)	Yes	Yes	Yes	Yes
Two-factor authentication	Yes	Yes	Yes	Yes
Login alerts	Yes	Yes	Yes	Yes
Block users	Yes	Yes	Yes	Yes
Location restriction	Yes	Yes	Yes	Yes

Table 4: Privacy and security settings on social instant-messaging applications

Privacy settings	Whatsapp	Viber	Telegram
Show/hide online status	Yes	Yes	Yes
Disable seen option	Yes	Yes	No
Limit who can see your profile photo	Yes	Yes	Yes
Block users	Yes	Yes	Yes
End-to-End Encryption	Yes	Yes	No (available only for secret chats)

Table 5, on the other hand, includes networking platforms that are instant messaging applications. Because Table 4 platforms, in contrast to Table 3, do not permit users to create public or private profiles or share information and multimedia content with the general public or their whole network of friends and followers, this led to the construction of two distinct tables.

The Table 5 platforms enable group creation and private communication between users and their friends and family. Sharing multimedia content is done discreetly on instant messaging networks, which means that you only share the desired content or information exchange with one friend/contact or to a specific group chat that is made of people you know and trust.

5 Commercial solutions for privacy and security threats on OSN platforms

To safeguard, prevent, defend, and better maintain security online against numerous and evolving security threats, many security firms have created security solutions for OSNs. These tools and software can be used by individuals as well as by businesses to protect their social network accounts and their data. Table 5 gives a brief overview of some solutions provided by commercial companies for better protection from threats on OSN platforms.

Table 5: Commercial solutions for better privacy and security protection on OSN platforms

Commercial solution	Operating System	Platform	Browser supported	Pricing
McAfee WebAdvisor	Windows		Internet Explorer 10.0 or later, Microsoft Edge, Mozilla Firefox, Google Chrome	Free
Total Defense Ultimate Internet Security	Windows, MacOS, Android	PCs, Macs, Smartphones & Tablets		Yearly subscription plans
Facebook Container			Firefox add-on	Free

LastPass	Windows, Mac, Linux, and mobile platforms	Computers, mobile devices	Offered as an add-on on Internet Explorer, Firefox, Safari, Edge, and Opera	Free version Premium version with monthly pricing plans
LogDog	iOS, Android	Devices that are supported by Android and iOS		Free (ads included), Premium version with monthly and annual pricing plans

McAfee - McAfee WebAdvisor helps in protecting online security as users browse and do searches on the Internet. WebAdvisor assists in keeping its users secure from malware act as a crypto blocker and provides security alerts. WebAdvisor offers phishing protection, URL hijacking protection, social media protection, as well as the ability to scan downloads and inform you if there is a risk, all while you browse [27]. McAfee WebAdvisor enables you to browse your social networks such as Facebook, Twitter, Instagram, LinkedIn, Youtube, and Reddit with comfort and safety. The Social Media Protection feature in McAfee WebAdvisor provides rating annotations for links on the aforementioned social networks. These annotations work by color-coding the links on these platforms to determine which links are secure to visit and which ones you should avoid [28].

Total Defense Ultimate Internet Security - A user-friendly, all-in-one Internet security suite, Total Defense Ultimate Internet Security shields your devices and you against the most recent internet threats. While you bank, shop, and interact on social networks with complete confidence, high-performance virus detection is taking place on your devices without slowing you down. Ultimate Internet Security protects you from malicious content when using social networks with social media protection features. With their anti-phishing software, this security software blocks suspicious email messages, fake posts on social media, fraudulent websites, and other frauds intended to steal your money and personal information before you even see them [29].

Facebook Container – Facebook Container add-on by Mozilla Firefox [30] prevents Facebook from being able to track your visits to other websites via third-party cookies, and Facebook Container isolates your Facebook identity into a distinct container.

LastPass - Password managers are becoming more and more popular, and both free and premium versions offer lots of convenience and security. LastPass is a password manager that stores your passwords and provides you with secure access from any computer or mobile device. LastPass gives you control over your online life by making it simple to save your sensitive data securely so you can access it from anywhere at any time. With LastPass, you can save and secure all of your usernames, passwords, credit cards, notes, and other information in your safe vault, and LastPass will automatically fill in the appropriate fields for you when you need them [31]. There are many other password-managing tools such as Enpass, Bitwarden, Dashlane, and others.

LogDog - The LogDog technology continuously checks numerous signs of unauthorized access while keeping an eye on a variety of online accounts and devices. LogDog observes how a user accesses all of their accounts and they are able to identify suspicious activity that the service providers themselves cannot. LogDog provides intrusion notifications when an attack is discovered and enables users to regain control of their accounts. By taking into account a user's activity across numerous devices and services, the LogDog system continuously

checks various signs that are linked to illicit access and keeps track of online accounts. LogDog monitors Dropbox, Gmail, Evernote, Facebook, Twitter, Yahoo, Outlook, Instagram, Stack, and LinkedIn [32].

6 Results and discussion

As a previous study [26] found, social network users are only minimally familiar with privacy settings and don't change them very often. We want to inform users about the privacy and security options available on the platforms they use. Also, inform them about solutions provided by commercial companies that can help in the better protection of their profiles and data.

Based on the privacy settings from Table 3, we can note that the four networking platforms – Facebook, Instagram, Twitter, and LinkedIn offer reliable and good privacy protection options for users' profiles. The networks have all of the aforementioned privacy and security settings, except for Facebook and Instagram, where the "seen option," also known as the "read receipt," cannot be turned off. However, we wouldn't argue that it's a crucial choice that might jeopardize someone's security and privacy or otherwise harm them. Whatsapp, Viber, and Telegram, the instant messaging apps listed in Table 4, provide good and reliable options for enhancing user privacy protection. They offer the same privacy and security settings, with the exception of Telegram, which only provides end-to-end encryption for secret chats, leaving communications vulnerable to interception by hackers as they travel through the network.

Table 5's finding shows that several software and tools can be employed to help shield consumers from dangers related to OSN platforms. These products can be completely free, like Facebook Container and McAfee WebAdvisor, or they can have free and premium versions with monthly or annual pricing options, like LastPass and LogDog, or they can only be purchased through a subscription, like Total Defense Ultimate Internet Security. These tools can be downloaded to a variety of devices, including laptops, tablets, and mobile phones, and they can run on different OS platforms. For example, McAfee is available for Windows, while Total Defense Ultimate Internet Security is available for Windows, MacOS, and Android. LastPass is available for Windows, Mac, Linux, and mobile platforms, and LogDog is an app that is available for iOS and Android. These all have the potential to enhance user security on social networks.

7 Conclusion

Online social networks in today's modern age play a significant role. In comparison to other activities, users spend the most time on social networks. Both benefits and drawbacks come with using social networks. The fact that different people can access information posted online must be recognized, and due to this fact, social networking platforms also raise privacy concerns and security issues. The information posted on OSNs can be exploited by malicious actors, therefore causing harm to the user. In this paper, we explored modern threats that surround OSN platforms and pose a risk to users' identity, privacy, and security. We also discussed the types of authentication methods that are available on well-known networking platforms, as well as the authentication factors and mechanisms they use. We also covered and outlined the different privacy and security options offered by OSN providers, which users can employ to increase their privacy and security on these platforms. Then we talked about some commercially available solutions that could help users in protecting themselves and strengthen their security on OSNs.

Users should make the most of the privacy and security options given by OSN providers to protect their online security and privacy. Since there is no solution that guarantees complete protection, users should exercise extreme caution when choosing what they share and publish online, given that everyone can view public information. Therefore, they should also keep in mind the audience they share their content and information. When using OSN platforms, users should also consider employing antivirus, anti-spyware, and other software or tools that will add additional layers of protection.

References

- [1] Jain, A.K., Sahoo, S.R. & Kaubiyal, J., 2021. Online social networks security and privacy: Comprehensive review and analysis. *Complex & Intelligent Systems*, 7(5), pp.2157–2177.
- [2] Almarabeh, H., 2019. The impact of cyber threats on social networking sites. *International Journal of Advanced Research in Computer Science*, 10(2), pp.1–9.
- [3] Kadam, Smita & Chatterjee, Madhumita. 2016. Survey on Online Social Networking Threats and Solutions. *International Journal of Computer Science and Internet Security*, 8. pp.15-24.
- [4] Fire, M., Goldschmidt, R. & Elovici, Y., 2014. Online social networks: Threats and solutions. *IEEE Communications Surveys & Tutorials*, 16(4), pp.2019–2036.
- [5] Wani, Mudasir & Jabin, Suraiya & Yazdani, Ghulam & Ahmad, Nehaluddin. (2018). Sneak into Devil's Colony- A study of Fake Profiles in Online Social Networks and the Cyber Law.
- [6] Sharma, P.K. et al., 2017. Social Network Security: Issues, challenges, threats, and solutions. *Information Sciences*, 421, pp.43–69.
- [7] A.Obiniyi, A., N. Oyelade, O. & Obiniyi, P., 2014. Social Network and security issues: Mitigating threat through reliable security model. *International Journal of Computer Applications*, 103(9), pp.1–7.
- [8] Molok, Nurul & Chang, Shanton & Ahmad, Atif., 2012. Information Leakage through Online Social Networking: Opening the Doorway for Advanced Persistence Threats. Australian Information Security Management Conference.
- [9] Kumar, Sunil & Somani, Vikas., 2018. Social Media Security Risks, Cyber Threats, And Risks Prevention And Mitigation Techniques. *International Journal of Advance Research in Computer Science and Management*, 4. pp. 125-129.
- [10] Safhi, A., Al-Zahrani, A. & Alhibbi, M., 2022. Major security issue that facing social networks with its main defense strategies. *Tehnički glasnik*, 16(2), pp.205–212.
- [11] He, X. & Lu, H., 2017. Detecting and preventing inference attacks in online social networks: A data-driven and holistic framework. *Journal of Information Privacy and Security*, 13(3), pp.104–119.
- [12] Frankenfield, J., 2022. De-anonymization definition. *Investopedia*. Available at: <https://www.investopedia.com/terms/d/deanonymization.asp>.
- [13] What is an authentication factor? Sumo Logic. (n.d.). Retrieved from <https://www.sumologic.com/glossary/authentication-factor/>
- [14] Anon, 2019. What is clickjacking: Attack example: X-frame-options Pros & Cons: Imperva. *Learning Center*. Available at: <https://www.imperva.com/learn/application-security/clickjacking/>.
- [15] Authors, R., 2021. What are the three authentication factors? *Rublon*. Available at: <https://rublon.com/blog/what-are-the-three-authentication-factors/>.
- [16] Editorial, G., 2020. Clickjacking attacks: Beware of social network identification. *Geekflare*. Available at: <https://geekflare.com/clickjacking-attacks-social-network/>.
- [17] Wagner, K. & Molla, R., 2018. Facebook has disabled almost 1.3 billion fake accounts over the past six months. *Vox*. Available at: <https://www.vox.com/2018/5/15/17349790/facebook-mark-zuckerberg-fake-accounts-content-policy-update>.
- [18] McGready, S., 2019. Scams: How spoofing, Twitter clones, fake green padlocks and gift card 'fines' could catch you out. *Live life richer with Lovemoney*. Available at: <https://www.lovemoney.com/news/71657/scam-fraud-spoofing-twitter-clone-green-padlock-gift-card-fines>.

- [19] Anon, Should you share your location on social media? *The risks of sharing your location on social media* | Equifax UK. Available at: <https://www.equifax.co.uk/resources/identity-protection/should-you-share-your-location-on-social-media.html>.
- [20] Anon, Pearson IT certification. *Understanding the Three Factors of Authentication* | Pearson IT Certification. Available at: <https://www.pearsonitcertification.com/articles/article.aspx?p=1718488>.
- [21] Farik, Mohammed & Lal, Nilesch & Prasad, Shalendra., 2016. A Review Of Authentication Methods. *International Journal of Scientific & Technology Research*. 5. pp. 246-249.
- [22] N-able, 2021. Understanding network authentication methods - N-able. N. Available at: <https://www.n-able.com/blog/network-authentication-methods>.
- [23] Anon, 2022. 5 user authentication methods that can prevent the next breach. *ID R&D*. Available at: <https://www.idrnd.ai/5-authentication-methods-that-can-prevent-the-next-breach/>.
- [24] Anon, What is Two-factor authentication (2FA)? *Authy*. Available at: <https://authy.com/what-is-2fa/>.
- [25] P, S. & Chatterjee, M., 2018. Comparative study of threats and solutions in online social networks. *International Journal of Advanced Research in Computer Science*, 9(1), pp.760–764.
- [26] Senthil Kumar N, Saravanakumar K & Deepa K, 2016. On privacy and security in Social Media – a comprehensive study. *Procedia Computer Science*, 78, pp.114–119.
- [27] McAfee, Browse safely and steer clear of online dangers: McAfee WebAdvisor. *McAfee*. Available at: <https://www.mcafee.com/en-us/safe-browser/mcafee-webadvisor.html>.
- [28] Anon, How to enable social media annotations in WebAdvisor. *Antivirus, VPN, Identity & Privacy Protection*. Available at: <https://www.mcafee.com/support/?locale=en-US&articleId=TS103074&page=shell&shell=article-view>.
- [29] Kalle, - et al., Ultimate Internet Security. *Total Defense*. Available at: <https://www.totaldefense.com/shop/ultimate-security/>.
- [30] Anon, 2018. Facebook container – get this extension for Firefox (EN-US). *Facebook Container – Get this Extension for Firefox (en-US)*. Available at: <https://addons.mozilla.org/en-US/firefox/addon/facebook-container/?src=collection>.
- [31] Anon, LastPass: Free password manager. *Google*. Available at: <https://chrome.google.com/webstore/detail/lastpass-free-password-ma/hdokiejnpimakedhajhdlcegeplioahd>.
- [32] Anon, 2021. About Us. *LogDog*. Available at: <https://getlogdog.com/aboutus-full/>.
- [33] Marija Bukalevska, Aleksandar Karadimce., 2022. Privacy Risks and Security Threats in Online Social Networks. Conference Paper. Conference: 19th International Conference on Informatics and Information Technologies - CIIT 2022.

OVERVIEW AND PERFORMANCE ANALYSIS OF LATEST SUPERCOMPUTERS

Teala Seferi ¹, Floriana Doko ¹, Atanas Hristov ²

Email(s): teala.seferi@cns.uist.edu.mk
floriana.doko@cse.uist.edu.mk
atanas.hristov@usit.edu.mk

¹ Faculty of Communication Networks and Security, University of Information Science and Technology “St. Paul the Apostle”, Ohrid, 6000, Macedonia

² Faculty of Information and Communication Sciences, University of Information Science and Technology “St. Paul the Apostle”, Ohrid, 6000, Macedonia

Abstract

Advanced distributed technologies play a pivotal role in numerous fields, including scientific research, weather forecasting, and financial modeling, by revolutionizing the way data is processed and analyzed. In scientific research, these technologies enable collaborative efforts across different institutions and countries, allowing scientists to pool their resources and expertise for groundbreaking discoveries, they allow for the processing and analysis of large amounts of data, such as genomics data or observational data from telescopes. They also enable the use of complex models and simulations that would otherwise be infeasible... By distributing the computational load across multiple systems, complex simulations and data-intensive experiments can be performed more efficiently, leading to accelerated scientific progress. Similarly, in weather forecasting, advanced distributed technologies empower meteorologists to process vast amounts of data from satellites, weather stations, and other sources in real-time. This facilitates accurate predictions, early warning systems, and improved disaster preparedness, ultimately saving lives and minimizing damages caused by severe weather events. Furthermore, in financial modeling, distributed technologies enable the analysis of vast financial datasets and the development of sophisticated algorithms for risk assessment, portfolio optimization, and market predictions. These technologies provide financial institutions with faster and more accurate insights, aiding decision-making and reducing risks. In summary, advanced distributed technologies are instrumental in unlocking the full potential of scientific research, weather forecasting, and financial modeling, driving innovation and enhancing our understanding of the world around us.

Keywords

Supercomputing, architecture, analysis, aurora supercomputer, fugaku supercomputer, processors, interconnects, memory, FLOPS, memory bandwidth, power consumption

Introduction

Supercomputing is the use of advanced computing resources to solve complex problems that require vast amounts of computational power. The field has seen significant growth in recent years, with the development of new technologies and the increasing demand for more sophisticated simulations and data analysis. In this research paper, we will analyze and compare two supercomputing systems that have emerged in the last five years.

Aurora is a supercomputer developed by Intel and Cray for the U.S. Department of Energy's Argonne National Laboratory. It is one of the fastest supercomputing systems in the world, with a processing power of over 1.5 exaflops. Aurora is designed to address a wide range of scientific and industrial applications, including simulation and modeling, artificial intelligence, and data analysis.

Fugaku is a supercomputer developed by RIKEN and Fujitsu, and it is located in Kobe, Japan. It is currently ranked as the fastest supercomputer in the world, with a processing power of over 415 petaflops. Fugaku is designed to address a wide range of scientific and industrial applications, including simulation and modeling, artificial intelligence, and high-performance data analytics.

Our focus will be on the technical specifications, performance characteristics, and applications of these systems. Through this analysis, we aim to provide insights into the state of the art in supercomputing and to highlight the key trends and innovations in this field.

1. Supercomputers

Supercomputers are among the most powerful computer systems in the world. They are designed to perform highly complex and resource-intensive tasks, such as modeling and simulating large-scale physical systems, performing complex scientific research, and analyzing large amounts of data. They are often used in fields such as weather forecasting, climate research, drug discovery, and nuclear weapon simulation.

Supercomputers are characterized by their high processing power, which is measured in floating-point operations per second (FLOPS). FLOPS are a unit of measurement that quantifies a computer's computational performance and the number of floating-point arithmetic operations that can be performed per second. (e.g., addition, subtraction, multiplication, or division). IPS is a measure of the number of instructions that a computer's processing unit can execute in one second. IPS provides a more general measure of computational performance that takes into account all types of operations performed by a computer, not just floating-point arithmetic operations. Hz is a measure of frequency that is used to quantify the number of clock cycles that a computer's processing unit can execute in one second. Clock cycles are the basic unit of time in a computer's processing unit, and they are used to synchronize the execution of instructions. The clock frequency of a computer's processing unit determines the number of clock cycles per second and, thus, the number of operations that can be executed in one second. [1]

Supercomputers also typically have a large amount of memory, storage, and specialized hardware, such as graphical processing units (GPUs), that are optimized for certain types of computations. The high-speed interconnect network is a crucial component that connects the computer processors, allowing them to share data and work together to perform complex tasks in parallel.

Supercomputers are generally maintained and operated by government agencies, research institutions, and large corporations, and they are often available for use by researchers and scientists from around the world.

In recent years, advances in computer technology have led to the development of even more powerful supercomputers, such as exascale supercomputers, which are capable of performing a billion calculations per second. These machines are expected to be used for a wide range of scientific and industrial applications and to push the boundaries of what is currently possible in terms of computational power.

Supercomputers are some of the most powerful machines on the planet, capable of performing billions

of calculations per second. These machines are used for a variety of tasks, including scientific research, weather forecasting, and even nuclear weapon simulations. In this essay, we will take a look at some of the best supercomputers in the world and the ways in which they are used.

One of the most powerful supercomputers in the world is the Summit, located at Oak Ridge National Laboratory in Tennessee. The Summit is capable of performing more than 200,000 trillion calculations per second, making it one of the fastest supercomputers in the world. The machine is used for a variety of tasks, including research in fields such as materials science, energy, and medical research. [2]

Another top supercomputer is the Sunway TaihuLight, located in Wuxi, China. This machine is capable of performing more than 93,000 trillion calculations per second, making it the fastest supercomputer in China. The Sunway TaihuLight is used for tasks such as weather forecasting and scientific research, as well as for industrial and commercial applications.

The Piz Daint, located in Switzerland, is another powerful supercomputer. This machine is capable of performing more than 25,000 trillion calculations per second and is used for a variety of tasks, including research in fields such as climate science, earthquake simulations, and drug discovery.

The Gyokou, located in Japan, is a supercomputer that is used primarily for scientific research. The Gyokou is capable of performing more than 19,000 trillion calculations per second and is used for tasks such as simulating the behavior of large-scale systems, such as the earth's atmosphere and oceans. [3]

Finally, the Tianhe-2A, located in China, is another powerful supercomputer. This machine is capable of performing more than 61,000 trillion calculations per second and is used for a variety of tasks, including scientific research, weather forecasting, and industrial and commercial applications.

In conclusion, supercomputers are incredibly powerful machines that are used for a variety of tasks. The Summit, Sunway TaihuLight, Piz Daint, Gyokou and Tianhe-2A are some of the best supercomputers in the world, each with its own unique capabilities and uses. These machines are helping to push the boundaries of science and technology and are enabling new discoveries and innovations that would not be possible without them.

2. Specifications and Architecture Of Some Of The Top Supercomputers In The World

The Summit supercomputer, located at Oak Ridge National Laboratory in Tennessee, is powered by IBM Power9 processors and NVIDIA Volta GPUs. It has a total of 4,608 nodes, with each node containing two Power9 processors and six Volta GPUs. The system has a total of 9,216 Power9 processors and 27,648 Volta GPUs, providing a total of 1.5 petaFLOPS of computational power. It also has a total of 1.6 petabytes of memory and 2 petabytes of storage. [4] [5]

The Sunway TaihuLight, located in Wuxi, China, is powered by Sunway 260-core SW26010 processors. It has a total of 10,649,600 cores, providing a total of 93.01 petaFLOPS of computational power. The system also has 1.3 petabytes of memory and 12 petabytes of storage. [6]

The Piz Daint, located in Switzerland, is powered by Intel Xeon processors and NVIDIA Tesla GPUs. It has a total of 5,320 nodes, with each node containing two Xeon processors and one Tesla GPU. The system has a total of 10,640 Xeon processors and 5,320 Tesla GPUs, providing a total of 25.3 petaFLOPS of computational power. It also has a total of 1.1 petabytes of memory and 15 petabytes of storage. [7]

The Gyokou, located in Japan, is powered by Fujitsu A64FX processors. It has a total of 7,680 nodes, with each node containing two A64FX processors. The system has a total of 15,360 A64FX processors, providing a total of 19.14 petaFLOPS of computational power. It also has a total of 1.4 petabytes of memory and 1.2 petabytes of storage. [8]

The Tianhe-2A, located in China, is powered by Intel Xeon processors and NVIDIA Tesla GPUs. It has a total of 16,000 nodes, with each node containing two Xeon processors and three Tesla GPUs. The system has a total of 32,000 Xeon processors and 48,000 Tesla GPUs, providing a total of 61.4 petaFLOPS of computational power. It also has a total of 1.4 petabytes of memory and 12 petabytes of storage. [9]

It's worth noting that these supercomputers have different architectures, and some of them use accelerators like GPUs, which are specialized processors that are optimized for certain types of computations, such as those used in machine learning, to boost the performance of the system. Also, for these supercomputers the interconnect network is crucial for their performance as well, as it connects all the nodes and allows them to communicate and share data.

3. Analysis Of Two Supercomputers Of Last 5 Years

It's worth noting that the knowledge cutoff of my training data is 2021 and the latest two supercomputers might not be the current ones.

Supercomputers are some of the most powerful machines on the planet, capable of performing billions of calculations per second. These machines are used for a variety of tasks, including scientific research, weather forecasting, and even nuclear weapon simulations. In recent years, advances in computer technology have led to the development of even more powerful supercomputers, such as exascale supercomputers, which are capable of performing a billion billion calculations per second.

The latest two supercomputers that were released in the last five years are the Aurora, located at Argonne National Laboratory in Illinois, and the Fugaku, located in Japan.

Aurora, designed by Intel and Cray, is powered by Intel Xeon processors and Intel Xe GPUs. It was first introduced in 2021 and is expected to deliver a peak performance of 1.5 exaFLOPS, making it one of the most powerful supercomputers in the world. The Aurora is designed to be used for a wide range of scientific and industrial applications, including weather forecasting, climate research, drug discovery, and nuclear weapon simulations, as well as in fields such as artificial intelligence, machine learning, and big data analytics.

The Fugaku supercomputer was developed by Riken and Fujitsu and is powered by Fujitsu A64FX processors. It was first introduced in 2020 and has delivered a peak performance of over 415 petaFLOPS, making it one of the most powerful supercomputers in the world. The Fugaku is designed for a wide range of scientific and industrial applications, including weather forecasting, climate research, drug discovery, and nuclear weapon simulations, and it is expected to be used for research in fields such as materials science, energy, and medical research.

Both supercomputers have been able to perform complex and resource-intensive tasks and have been used in various research fields to push the boundaries of current computational power. They are expected to be used by researchers and scientists from around the world to make new discoveries and innovations.

In conclusion, The Aurora and Fugaku are two of the latest and most powerful supercomputers that were released in the last five years. They have been able to perform incredibly complex and resource-intensive tasks, and have been used in various research fields to push the boundaries of what is currently possible in terms of computational power. These machines continue to be used by researchers and scientists from around the world, helping to make new discoveries and innovations that would not be possible without them.

4. 1 Aurora and Fugaku Supercomputers

The Aurora supercomputer, located at Argonne National Laboratory in Illinois, is powered by Intel Xeon processors and Intel Xe GPUs. It was first introduced in 2021 and it was expected to deliver a peak performance of 1.5 exaFLOPS, making it one of the most powerful supercomputers in the world. The Aurora is designed to be used for a wide range of scientific and industrial applications, including weather forecasting, climate research, drug discovery, and nuclear weapon simulations. It is also

expected to be used for research in fields such as artificial intelligence, machine learning, and big data analytics.

The Aurora supercomputer is a collaboration between Intel and Cray and it uses Cray's Shasta architecture, which is designed to scale to exascale levels of performance. The system is based on a high-speed interconnect network and it uses a combination of processors and accelerators to achieve its high performance. The Aurora uses the Intel Xeon Scalable processors and Intel Xe GPUs, which are specialized processors that are optimized for certain types of computations, such as those used in machine learning, to boost the performance of the system. [10]

The Fugaku supercomputer, located in Japan, is powered by Fujitsu A64FX processors. It was first introduced in 2020 and it has delivered a peak performance of over 415 petaFLOPS, making it one of the most powerful supercomputers in the world. The Fugaku is designed to be used for a wide range of scientific and industrial applications, including weather forecasting, climate research, drug discovery, and nuclear weapon simulations. It is also expected to be used for research in fields such as materials science, energy, and medical research.

The Fugaku supercomputer is a collaboration between Riken and Fujitsu. It uses a custom-designed interconnect network and it is based on the Fujitsu A64FX processor, which is specifically designed for high-performance computing applications. The A64FX processor is a 48-core Arm processor that is based on the Arm SVE (Scalable Vector Extension) instruction set and it is designed to deliver high performance for a wide range of scientific and industrial applications. The Fugaku also uses a hierarchical memory system, which allows for high bandwidth and low-latency data access. [11]

Both of these supercomputers are expected to be used for a wide range of scientific and industrial applications, and they are pushing the boundaries of what is currently possible in terms of computational power. They are expected to help researchers and scientists from around the world make new discoveries and innovations that would not be possible without them.

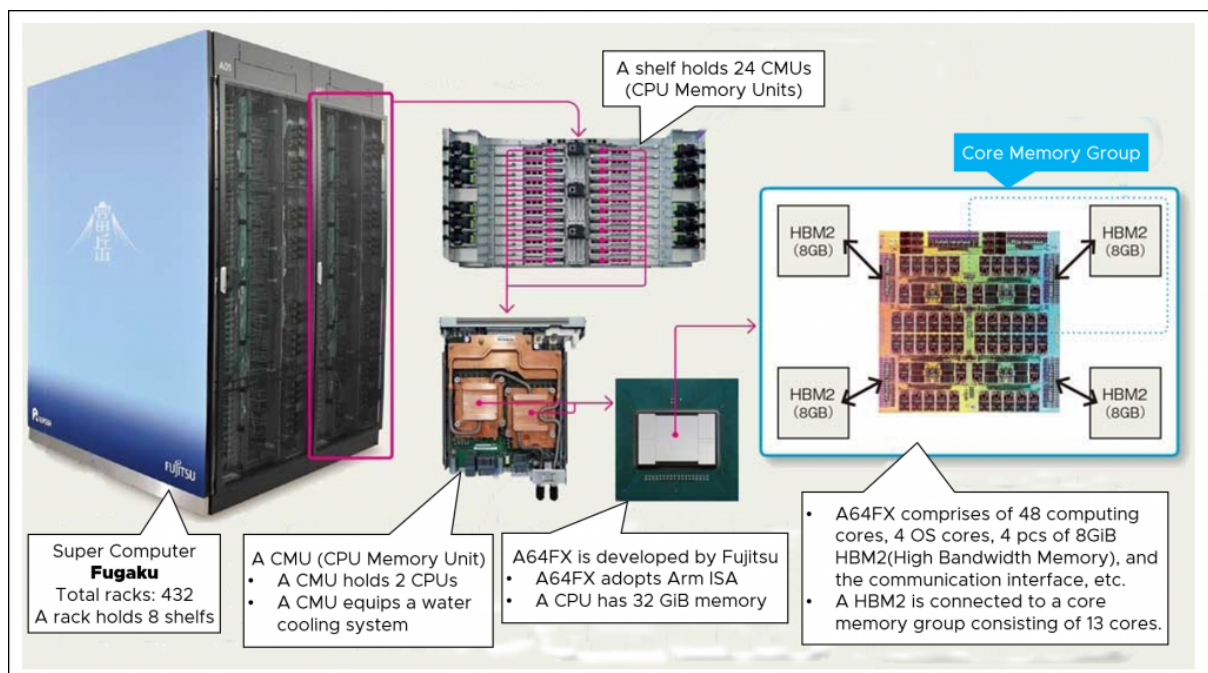


Figure 1: Overview of Fugaku supercomputer



Figure 2: High-level view of Aurora supercomputer

5. Conclusion

Supercomputers are some of the most powerful machines on the planet, capable of performing billions of calculations per second. They are designed to perform highly complex and resource-intensive tasks, such as modeling and simulating large-scale physical systems, performing complex scientific research, and analyzing large amounts of data. They are often used in fields such as weather forecasting, climate research, drug discovery, and nuclear weapon simulation.

Supercomputers are typically built using large numbers of computer processors that work together in parallel, with specialized hardware such as graphical processing units (GPUs) that are optimized for certain types of computations. They are also maintained and operated by government agencies, research institutions, and large corporations, and they are often available for use by researchers and scientists from around the world.

In recent years, advances in computer technology have led to the development of even more powerful supercomputers, such as exascale supercomputers, which are capable of performing a billion billion calculations per second. These machines are expected to be used for a wide range of scientific and industrial applications and to push the boundaries of what is currently possible in terms of computational power.

The Aurora and Fugaku are two examples of the latest and most powerful supercomputers that were released in the last five years. They have been able to perform incredibly complex and resource-intensive tasks, and have been used in various research fields to push the boundaries of what is currently possible in terms of computational power. These machines continue to be used by researchers and scientists from around the world, helping to make new discoveries and innovations that would not be possible without them.

In conclusion, supercomputers are incredibly powerful machines that are used for a variety of tasks. They are able to perform highly complex and resource-intensive tasks, and they continue to push the boundaries of what is currently possible in terms of computational power. These machines are helping to drive new discoveries and innovations in a wide range of fields, and they will continue to play an important role in scientific research and industrial applications in the future.

References

- [1] "Top 500 List," November 2022. [Online]. Available: <https://www.top500.org/>.
- [2] "National Energy Research Scientific Computing Center, Summit: A Leadership- Class Supercomputer,," 2021. [Online]. Available: <https://www.nersc.gov/users/computational-systems/summit/>.
- [3] "RIKEN Center for Computational Science,," 2021. [Online]. Available: <https://www.r-ccs.riken.jp/en/gyouku/>.
- [4] "Oak Ridge National Laboratory,," [Online]. Available: <https://www.olcf.ornl.gov/computing-resources/summit/>.
- [5] "IBM Summit: The World's Most Powerful and Intelligent Scientific Supercomputer,," [Online]. Available: <https://www.ibm.com/systems/summit>.
- [6] "National Supercomputing Center in Wuxi. (n.d.). Sunway TaihuLight,," 2021. [Online]. Available: <http://www.nscctx.cn/english/2017/0620/c3234a239079/page.htm>.
- [7] "Swiss National Supercomputing Centre,," 2021. [Online]. Available: https://www.cscs.ch/computing_resources/computer_systems/piz_daint/.
- [8] "RIKEN Center for Computational Science,," 2021. [Online]. Available: <https://www.r-ccs.riken.jp/en/gyouku/>.
- [9] "National Supercomputer Center in Guangzhou,," 2021. [Online]. Available: <http://en.nscgz.cn/systems/th-2a.html>.
- [10] "Argonne National Laboratory Aurora: A revolutionary supercomputer,," [Online]. Available: <https://www.anl.gov/research/aurora>.
- [11] "RIKEN Center for Computational Science, Fugaku supercomputer,," [Online]. Available: <https://www.r-ccs.riken.jp/en/fugaku-supercomputer>.