University of Zurich[UZH]

Burkhard Stiller, Alberto Huertas, Bruno Rodrigues, Chao Feng, Daria Schumm, Jan von der Assen, Katharina O. E. Müeller, Krzysztof Gogol, Thomas Grübl, Weijie Niu (Edts).

Internet Economics XVI

TECHNICAL REPORT – No. IFI-2023.04

January 2024

University of Zurich
Department of Informatics (IFI)
Binzmühlestrasse 14, CH-8050 Zürich, Switzerland

ifi

B. Stiller et al. (Eds.): Internet Economics XVII: IntEco Seminar
Technical Report No. IFI-2023.04, January 2024
Communication Systems Group (CSG)
Department of Informatics (IFI)
University of Zurich
Binzmühlestrasse 14, CH-8050 Zürich, Switzerland
URL: http://www.csg.uzh.ch/

Introduction

The Department of Informatics (IFI) of the University of Zurich, Switzerland works on research and teaching in the area of computer networks and communication systems. Communication systems include a wide range of topics and drive many research and development activities. Therefore, during the autumn term HS 2023 a new instance of the Internet Economics seminar has been prepared and students as well as supervisors worked on this topic.
Even today, Internet Economics are run rarely as a teaching unit. This observation seems to be a little in contrast to the fact that research on Internet Economics has been established as an important area in the center of technology and economics on networked environments. After some careful investigations it can be found that during the last ten years, the underlying communication technology applied for the Internet and the way electronic business transactions are performed on top of the network have changed. Although,a variety of support functionality has been developed for the Internet case, the core functionality of delivering data, bits, and bytes remained unchanged. Nevertheless, changes and updates occur with respect to the use, the application area, and the technology itself. Therefore, another review of a selected number of topics has been undertaken.

Content

This new edition of the seminar entitled "Internet Economics XVII" discusses a number of selected topics in the area of Internet Economics. Talk 2 offers a comprehensive examination of arbitrage in Decentralized finance (DeFi), shedding light on its potential advantages and drawbacks. Talk 3 delves into the socio-economic consequences of IT in arts and culture. Talk 6 provides a comprehensive overview of facial recognition technologies. Talk 9 explores the operations and protocols of the crypto arbitrage. Lastly, Talk 10 examines the business model of an AI framework, specifically Federated Learning.

Seminar Operation

Based on well-developed experiences of former seminars, held in different academic environments, all interested students worked on an initially offered set of papers and book chapters. Those relate to the topic titles as presented in the Table of Content below. They prepared a written essay as a clearly focused presentation, an evaluation, and a summary of those topics. Each of these essays is included in this technical report as a separate section and allows for an overview on important areas of concern, sometimes business models in operation, and problems encountered.

In addition, every group of students prepared a slide presentation of approximately 45 minutes to present its findings and summaries to the audience of students attending the seminar and other interested students, research assistants, and professors. Following a general question and answer phase, a student-lead discussion debated open issues and critical statements with the audience.

Local IFI support for preparing talks, reports, and their preparation by students had been granted by Alberto Huertas, Bruno Rodrigues, Chao Feng, Daria Schumm, Jan von der Assen, Katharina O. E. Müeller, Krzysztof Gogol, Thomas Grübl, Weijie Niu, and Burkhard Stiller. In particular, many thanks are addressed to Chao Feng for organizing the seminar and for their strong commitment on getting this technical report ready and quickly published. A larger number of pre-presentation discussions have provided valuable insights in the emerging and moving field of communication systems, both for all groups of students and supervisors. Many thanks to all people contributing to the success of this event, which has happened in a lively group of highly motivated and technically qualified students and people.

Zurich, January 2024

Contents

Chapter 2

Understanding Arbitrage in DeFI - Opportunities and Risks

Cyrill Hidber

The emergence and development of Decentralized Finance (DeFi) has great potential for the financial sector, especially in light of recent financial crises and various problems and risks in the traditional financial sector. Originating from the initial idea behind Bitcoin to establish a new payment system, blockchain systems and smart contracts have evolved, enabling more advanced financial services in the DeFi area. Various ecosystems have emerged, seeking to establish themselves in the field of cryptocurrencies.
In the financial sector, there are always opportunities to make a profit by utilizing or developing know-how, especially when the sector is still young. However, there are also various associated risks.
In this seminar paper, the various ecosystems are examined, general arbitrage strategies are highlighted, and some past exploited arbitrage strategies are specifically demonstrated, showing that they can be very profitable. The work also points out the associated risks, which can be either inherent in nature or of a malicious nature.

Contents

2.1 Introduction

2.1.1 Derivatives

Although this is primarily a discussion about arbitrage in the realm of cryptocurrencies, I would like to take this opportunity to do digress at the start. In today's traditional financial world, derivatives are a type of financial instrument that play a significant role. Derivatives are often used to represent an underlying asset such as a stock, bond, commodity, various currencies, or the like. Common forms of derivatives include options, futures, swaps, and forwards, but these products can also be much more complex and diverse [1].
While derivatives inherently serve important functions such as providing liquidity, risk management, globalization of financial markets, or arbitrage opportunities, they also pose a risk factor. An example of the extent to which this can occur is the 2008 financial crisis, which held the world in suspense and revealed weaknesses in the system. Recent developments in Switzerland with the downfall of Credit Suisse also give cause for concern and at least raise questions about the trustworthiness of the current state of the traditional financial system.

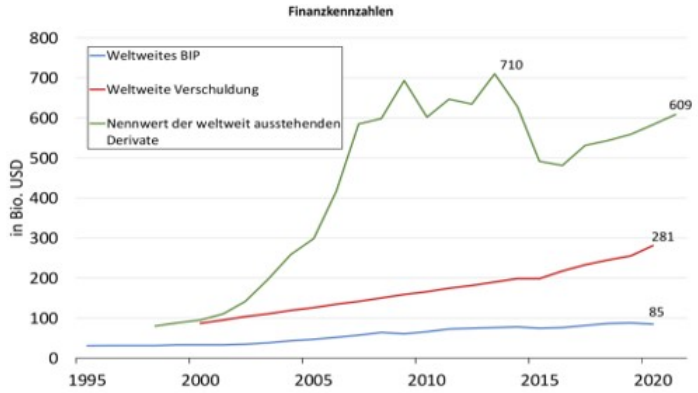

Figure 2.1: Comparison of derivative products to the global GDP and global private and public debt. [2]

The outstanding nominal value of global derivative products, which is about nine times larger than the global GDP, raises the question of whether these instruments are really all used for legitimate insurance purposes. On a local level, the position of derivative products held by systematically important financial institutions in Switzerland also gives cause for concern. This is especially true since these positions, as shown in 2.2, are very volatile. Not least because they bear no sensible relation to Switzerland's GDP.
Therefore, the question arises whether there are alternatives that can provide some protection from the traditional financial sector, and what opportunities and risks exist in this regard.

SIX Group (Börse Schweiz), second week October 2020 In CHF

The total notional value of open positions/contracts reported	
Commodities	163,029,582,655
Credit	574,581,920,811
Currency	8,573,811,232,837
Equity	18,961,153,458,694,300

SIX Group (Börse Schweiz), last week of May 2021

The total notional value of open positions/contracts reported	
Commodities	161'587'284'283
Credit	624'005'437'386
Currency	7'219'479'475'465
Equity	38'832'561'156'578'100

SIX Group (Börse Schweiz), second week of March 2022

The total notional value of open positions/contracts reported	
Commodities	152'042'668'342
Credit	732'858'186'088
Currency	8'144'114'737'960
Equity	2'627'720'573'262'630

Figure 2.2: Derivatives held by Swiss financial institutions. [2]

2.1.2 Traditional Arbitrage

Arbitrage, in the traditional sense, refers to an investment strategy where price differences between various assets are exploited. This means that an asset is purchased in one financial market at a certain price and sold in another financial market at a higher price. Risk-free profit can be realized from the typically small differences between the prices. However, considerable profits can also result form high transaction volumes. Arbitrage in its righteous form contributes to market corrections, maintaining efficiency, and providing increased liquidity.

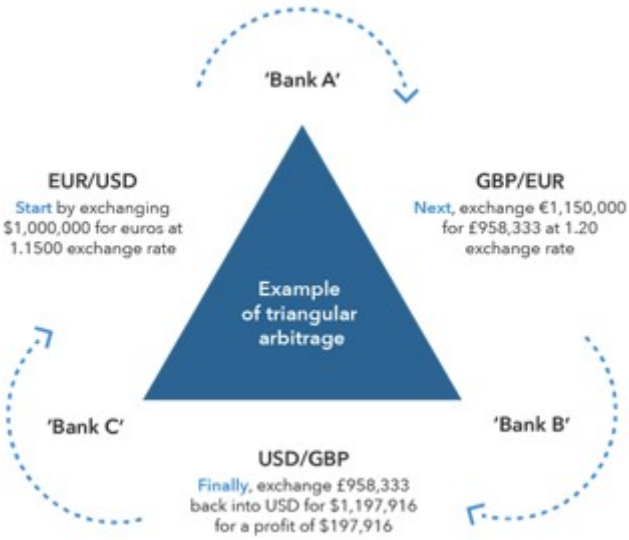

Figure 2.3: Example of triangular arbitrage with different currencies. [3]

2.1.3 Problem Statement: Arbitrage in Crypto

In the context of financial services, the cryptocurrency sector offers a fascinating perspective. Particularly after the financial crisis, various cryptocurrencies, led by the most well-known blockchain-based cryptocurrency, Bitcoin, experienced a significant upswing [4]. The cryptocurrency sector is based on blockchain technology and is characterized by its decentralized structure. It is in a continuous growth process as blockchain technology, and its diverse applications are constantly being developed.
An important aspect of this sector is the emergence of decentralized exchange (DEX) platforms that offer their services to swap crypto tokens between each other. In this context, it has been observed that various forms of arbitrage are practiced in this area.

Therefore, we will consider how these cryptocurrencies fundamentally work, what they offer compared to the traditional financial world, where trading takes place, how various forms of cryptocurrency arbitrage are practiced, what their risks are, and the implications thereof.

2.2 Background

2.2.1 Blockchain Technology

To understand how cryptocurrencies work, this section presents the fundamental underlying technology that constitutes them, the blockchain. Blockchains are digital ledgers implemented in a distributed manner, meaning they are not centrally managed, and entities such as governments, banks, or companies generally do not have authority over them. In terms of their functionality, they are distributed ledgers consisting of various blocks. Each block contains a block header with metadata and block data with various transactions [5]. The different blocks are linked together. Once a block is created, verified, and added to the chain, it becomes immutable. This means that transactions can no longer be deleted or altered.

To verify whether a transaction is valid, and append to the ledger various consensus mechanisms are used. The most well-known are Proof of Stake (PoS) and Proof of Work (PoW). These consensus models provide an economic incentive for the relevant network participants to undertake this important task.
In the case of PoW, so-called miners must solve a cryptographic puzzle at a high cost of their own resources to append a new block to the ledger. The process is very computationally intensive.
In the case of PoS, so-called validators stake a portion of the blockchain's native cryptocurrency to then perform the validation of transactions and append a new block to the chain. If they do not perform correctly or act maliciously, a part of their stake can be confiscated. It is an alternative to PoW that requires less energy for implementation [6]

Due to their decentralized structure, where no single entity has control, blockchains are largely protected against manipulation and censorship. Transactions are secured through cryptography and become tamper-proof once added to the chain, providing a high level of security and thereby increasing trust. All transactions can be viewed by any network participant, offering a high degree of transparency for all involved. These factors make blockchain technology particularly attractive for the financial sector and partly explain why cryptocurrencies have experienced such a boom in recent years, not least because of various recent financial crises in the traditional sector.

2.2.2 Smart Contracts

Smart contracts are transaction protocols that define the terms of an agreement and automatically execute the corresponding contract when those terms are met. They are based on blockchain technology and are coded, making them self-executing agreements that can operate without human intervention, thus eliminating typical sources of errors. Ethereum is the first and most used blockchain platform currently offering such contracts, and they can be autonomously deployed on it [7].
Smart contracts also minimize the need for trusted intermediaries in transactions, making them suitable for automating processes and settlements between parties. They are deterministic, meaning that the same input will always yield the same result. This enhances transparency, streamlines processes, and reduces costs and delays. Because they

are programmable, they are highly adaptable. As such, they play a central role in the decentralized financial ecosystem.

2.3 Decentralized Finance

2.3.1 Decentralized Finance Landscape

DeFi, short for Decentralized Finance, refers to an ecosystem of financial applications built on blockchain technology. Its primary aim is to decentralize traditional financial services such as lending, cryptocurrency trading, asset management, and more, thereby challenging the conventional financial system. One of the fundamental principles of DeFi is enabling peer-to-peer financial transactions, where two parties agree to exchange cryptocurrencies for goods or services without the need for intermediaries [8].
DeFi is characterized by high security, fast transaction processing, and efficiency. However, it also presents challenges such as programming errors, counterparty risk, regulatory uncertainty, and malicious attacks. The costs associated with DeFi transactions include protocol fees and gas fees, and participation is generally open to anyone with a crypto wallet, unless it is completely prohibited or circumvented by specific countries' regulations [9].

2.3.2 Contrasting Traditional Finance, Centralized Finance, and Decentralized Finance

Traditional Finance (TradFi), Centralized Finance (CeFi), and Decentralized Finance (DeFi) represent three different approaches in the financial sector. TradFi, the conventional financial system, is heavily regulated and relies on intermediaries such as banks, exchanges, asset managers, and the like. It operates with fiat currency and traditional financial instruments and is by far the largest sector. CeFi, while sharing similarities with TradFi, is built on blockchain-based cryptocurrencies not issued by governments. CeFi serves as a kind of bridge between the crypto industry and traditional finance, with users often placing trust in centralized service providers and relinquishing control over their crypto assets [10]. CeFi platforms facilitate trading in various digital assets, derivatives, options, and other financial products. Examples of well-known CeFi platforms include (or have included) Coinbase, Kraken, or FTX.

On the other hand, DeFi is an emerging infrastructure that is entirely based on digital assets. It completely eliminates intermediaries and moves control away from centralized entities to the individual using it, with smart contracts enforcing the rules set by the participants. So, DeFi applications enable users to interact without intermediaries and without Know Your Customer (KYC) requirements, which is an increase in privacy[10]. Users retain full control over their crypto assets, and transactions occur directly on the blockchain. While TradFi is heavily regulated, DeFi is considered to be less regulated and is known for its innovative but often riskier approaches.

It is also important to note that the total value of assets locked (TVL) in DeFi protocols through smart contracts, experiences significant fluctuations. This volatility reflects the dynamic nature of the relatively young DeFi sector. While this presents opportunities for high returns, it also increases the risk for investors. The fluctuation in TVL can be influenced by various factors, such as market sentiment, regulatory developments, and technological advancements.

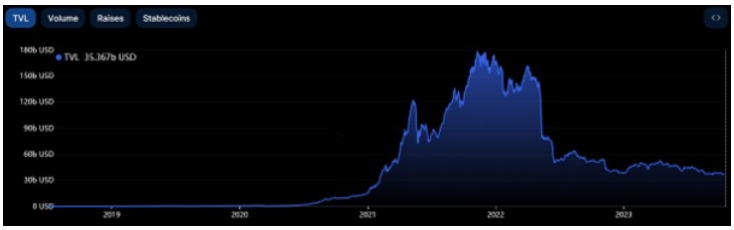

Figure 2.4: Total value locked in October at around 36 billion USD.[11]

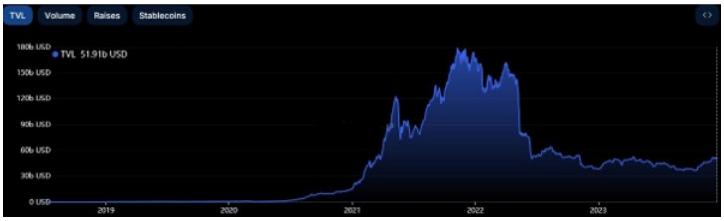

Figure 2.5: Total value locked in November at around 52 billion USD.[11]

The graph shows that there was a massive cryptocurrency boom, especially from 2021 to mid-2022. However, this boom has significantly tapered off as the initial hype, driven by the surge in Bitcoin, has somewhat subsided. Nevertheless, the DeFi sector still remains very interesting with over 50 trillion USD in TVL as of December 2023, indicating that it offers opportunities but also underscores that it is a relatively volatile market with inherent risks.

2.3.3 Decentralized Exchanges and Their Significance

2.3.3.1 Comparative Analysis: DEXs vs. CEXs

When comparing centralized cryptocurrency exchanges (CEXs) and decentralized cryptocurrency exchanges (DEXs), several key factors need to be considered. Firstly, CEXs are operated by a central organization or group of individuals and act as intermediaries between crypto buyers and sellers. Well-known examples of CEXs include Binance, Kraken, FTX, and Coinbase. These platforms are often regulated by government authorities and require users to go through KYC and AML procedures. CEXs typically offer user-friendly interfaces and customer support, making them attractive to less technically savvy users. However, they tend to have higher trading fees and retain users' private keys, which means users cannot directly track their digital assets on a blockchain [13; 12].
In contrast, DEXs operate on peer-to-peer blockchains without intermediaries, requiring users to connect their private keys through self-custody wallets. DEXs typically offer lower trading fees and do not require KYC procedures. However, they can be more technically challenging to use and generally do not provide centralized customer support. Another advantage of DEXs is that users retain full control over their private keys and, consequently, their crypto assets. [13; 12]. They are known for their transparency, cost-efficiency, and immutability. Transactions on DEXs cannot be altered, which can be seen as both an advantage and a disadvantage [14]. DEXs are a subset of DeFi (Decentralized Finance) and use self-custody crypto wallets to connect with liquidity pools. Therefore, DeFi encompasses all decentralized platforms, including over 700 DEX platforms as of 2023. Popular examples of DEXs include Uniswap, SushiSwap, and Balancer. The security of a DEX depends on its smart contract, and users should thoroughly research these before connecting a self-custody wallet [14].
As an example of a famous DEX, we can consider Uniswap. Uniswap is regarded as one

of the top DEXs due to its high liquidity, minimal transaction fees, and the ability to connect with multiple blockchains. Uniswap also ranks as the second-largest DEX. Because Uniswap doesn't have to pay intermediaries or does KYC, they have lower transaction fees and increased anonimity. However, Uniswap users need to pay network fees (gas fees) to confirm their trades and record them on a blockchain, compensating validators in the PoS consensus mechanism. The DEX platforms themselves also charge a user fee, typically around 0.3 percent, to reward liquidity providers and cover platform operating costs [14]. Therefore, it is advisable to check the fees and their amounts before making a trade.

In terms of trading options and liquidity, CEXs offer a wide range of services. They also serve as a source for DEX funding and withdrawal. On the other hand, DEXs allow anyone to act as a market maker by joining a liquidity pool but may not provide the same level of liquidity as CEXs [13; 12].

To interact with the services provided by a DEX, you must first open a compatible self-custody crypto wallet. In the case of Uniswap, for example, you could open a wallet that is compatible with the Ethereum blockchain. The wallet must be secured with a private key, known as the seed phrase. It is crucial to keep this seed phrase both safe and accessible, as only the user knows it; otherwise, the loss of the seed phrase may result in the loss of all wallet contents. This is a key difference between DEXs and CEXs, as CEXs typically securely store their users' seed phrases. The wallet is then connected to the DEX platform, and if cryptocurrencies are held within it through CEXs or other means, various services can be utilized on the DEX.

2.3.3.2 Liquidity Pools

Liquidity pools are a central element in the world of decentralized finance (DeFi) and are based on blockchain technology through smart contracts. They enable peer-to-peer trading on DEXs by allowing users, acting as Liquidity Providers, to deposit their crypto assets into these pools. In return, they receive Liquidity Tokens, representing their proportional share of the pool. These pools replace traditional order books with an automated pricing formula, enabling efficient trading even with low trading volumes. Liquidity Providers benefit from fees generated with each trade transaction within the pool, making it an attractive opportunity for passive income [15].
Despite their advantages, such as promoting an inclusive and decentralized financial system, Liquidity Pools also come with risks. These risks include impermanent loss, which occurs when the prices of assets deposited in the pool change significantly. Therefore careful risk management has to be done by Liquidity Providers. Liquidity Pools are thus an innovative but also complex component in the DeFi sector that offers both opportunities and challenges for participants [15].

2.3.3.3 Automated Market Makers

Automated Market Makers (AMMs) are a central component of the decentralized finance (DeFi) world. They are basically smart contracts that manage liquidity for DEXs. They replace traditional order books with pricing algorithms and utilize Liquidity Pools, where users act as Liquidity Providers by depositing their crypto assets. These pools facilitate trading by supplying liquidity and establishing prices for digital assets. AMMs offer advantages such as promoting trading in low-volume markets and independence from centralized exchanges. However, they also come with risks, such as impermanent loss, which occurs when the prices of assets in the pool change significantly. Various AMM

models, such as the Constant Product Market Maker (CPMM) model, are employed to regulate liquidity in the pools and facilitate efficient trading [16].

2.4 Cryptocurrency Arbitrage

2.4.1 Assessment of the Scale of Cryptocurrency Arbitrage

Arbitrage is also possible and practiced in the DeFi sector, as it offers the potential for significant profits. This assessment refers to specific points in time in this still young financial sector. Since DeFi is highly technical and continuously evolving, it must be noted that arbitrage opportunities and their exploitation are also subject to constant change. To exploit arbitrage opportunities in such a technical field, bots are used to ensure the necessary speed and efficiency. A parallel can be drawn here to High-Frequency Trading (HFT) conducted in the traditional financial sector. An examination of the scale of crypto arbitrage will be conducted in the following based on two studies.

In a first study, an analysis of arbitrage opportunities, particularly in the context of Ethereum and DEXs, was conducted. For the study, a dataset of 300 gigabytes was utilized, capturing, and using over 700 million unique observations of arbitrage bots. This allowed for a detailed picture of the arbitrage market in the cryptocurrency space. It can be demonstrated that arbitrage in the cryptocurrency market not only represents a significant activity but also offers substantial financial opportunities.In the early stages of the DEXs the Bots return range between 10-100 ETH whereas with increasing market efficiency this decreased to 1-10 ETH. This suggests that especially in the early stages of decentralized exchange market development, arbitrage bots were capable of achieving significant profits on a daily basis [17].

In a second study, transaction data from August 5, 2020, to January 23, 2021, were analyzed. This period covers the start of the cryptocurrency boom and extends into its middle phase, as indicated by 2.4 and 2.5, which show the Total Value Locked (TVL) in the cryptocurrency space. The analysis focused on large transactions exceeding 30,000 USD to identify potential arbitrage opportunities for these more lucrative and relevant trades. In total, 29,611 out of 108,667 analyzed transactions were identified as optimizable, representing a proportion of approximately 27 percent, indicating arbitrage opportunities for these big trades.

The study also found that the number of arbitrage opportunities increases during times of high price volatility. Since the cryptocurrency market is characteristically highly volatile, this suggest that arbitrage opportunities continuously present themselves.It was also observed that arbitrage bots benefiting from market inefficiencies have become more efficient over time. The study attributes the correlation between arbitrage opportunities to two factors: they are caused by price inaccuracies and influenced by the existing market liquidity [18]. This means, if the market grows larger liquidity wise and in regard to the amount of different currencies, the arbitrage opportunities will also grow.
It can be concluded that arbitrage in the DeFi sector constitutes a dynamic and ever-evolving landscape, where technological advancements and market conditions play a central role. Specifically, the efficiency improvement of arbitrage bots and their adaptability to changing market conditions are key factors for their success. Also the know-how of participants in the arbitrage environment has been increasing.

2.4.2 Types of Cryptocurrency Arbitrage

Arbitrage in DeFi, similar to the traditional financial world (TradFi), involves profiting from price or interest rate differences, often across different decentralized platforms. The main difference is that it operates within the DeFi ecosystem, which, due to its decentralized nature, a less regulated, and universally accessible environment. These characteristics make DeFi arbitrage particularly attractive to technically savvy individuals who use automated bots to exploit these arbitrage opportunities more efficiently and quickly. Various strategies are available and have been developed for capitalizing on arbitrage opportunities in DeFi.
Triangular Arbitrage exploits price differences among three different assets within a single platform. Through a series of trades that begin and end with the same asset, the goal is to profit from the price differences. It operates exactly on the same principle as illustrated in 2.3 [19].
Cross-Exchange Arbitrage exploits price differences for the same asset across different exchanges. Typically, this is achieved by buying the asset at a lower price on one platform and selling it at a higher price on another platform. However, it's important to consider the individual fees of the platforms, which can reduce or even negate the profit [19].
Yield Arbitrage involves exploiting interest rate differences across different platforms. The strategy is to lend assets at a higher interest rate on one platform while simultaneously borrowing at a lower interest rate on another platform. The difference between the interest rates then yields one's profit [19].
Strictly speaking, Market Making is not a direct arbitrage strategy; however, it employs very similar mechanisms. Market Making involves providing liquidity for a market, allowing profits to be generated through fees or rewards from trading activities [19].

2.4.3 Flash Loans

Another form is Flash Loan Arbitrage, which is examined more closely in another study. Flash Loans are a particular type of loans in the blockchain world. They are known for their short duration and the requirement for immediate repayment within a single transaction. They enable users to borrow large amounts of cryptocurrency without the need for any collateral. The condition is, that the loan is repaid in the same transaction. This feature makes Flash Loans a powerful tool for various financial strategies, especially for arbitrage trades [20].
In the referenced study, the researchers focused on analyzing the impact and potential of Flash Loans in the DeFi ecosystem. By studying real transactions and attack scenarios within the DeFi ecosystem, they were able to demonstrate how Flash Loans are practically used to achieve financial gains in the end.
One specific attack type in the DeFi ecosystem which was analyzed was referred to as the "Pump Attack and Arbitrage." This attack involved Flash Loan transactions followed by 74 additional transactions that resulted in a profit of 1,193.69 ETH which was equal to approximately 350,000 USD. The attack had a multi-stage and strategically sophisticated process. Initially, the attacker took out a Flash Loan in ETH. Some of this ETH was then used as collateral to borrow WBTC (Wrapped Bitcoin). The next step involved margin trading, where the attacker shorted ETH against WBTC and subsequently exchanged ETH for WBTC on Uniswap. Afterward, the attacker converted the borrowed WBTC back into ETH and repaid the Flash Loan. The attack was concluded with additional transactions aimed at maximizing the profit [21].
The intuition behind the attack lay in exploiting market mechanisms. The attacker "pumped" the price of ETH/WBTC on an AMM supported DEX (e.g., Uniswap) through leveraged ETH funds in a margin trade. This allowed the attacker to buy ETH at a lower

price on the distorted DEX market with the borrowed WBTC [21].
When evaluating the attack, the researchers noted that the attack parameters were not optimal. They calculated that the attacker could have made a profit of over 829,500 USD if the parameters had been chosen optimally. The attack relied on artificially created market distortion, resulting in losses for other market participants, particularly liquidity providers [21].
The conclusion from this analysis is that while Flash Loans are innovative financial instruments in the DeFi space, they can also be exploited for harmful market manipulation. While arbitrage itself is a normal part of market dynamics, its application in the context of Flash Loans can lead to unfair and detrimental market distortions. This raises the question how monitoring should be implemented and if even regulatory approaches are necessary to prevent these abusive practices [21]. Regulation in the DeFi sector, however, poses a major challenge since the fundamental concept of DeFi is built on the idea that the space should be kept free from central entities and their interventions.
So, there is a wide range of strategies that can be exploited as arbitrage opportunities, which can also become very complex. Profits can be substantial depending on the volume and sophistication. It should be explicitly noted that arbitrage can also be malicious in nature, as demonstrated above, and does not serve the intended purpose of eliminating market inefficiencies but rather personal enrichment, resulting in harm to other market participants.

2.4.4 Risks of Cryptocurrency Arbitrage

In the world of DeFi, despite the fundamentally secure underlying blockchain technology, there are still a variety of risks that users need to be aware of. The following are just a few of them briefly highlighted, which arise from design flaws in DEXes, risks to the Smart Contract ecosystem, and the entire blockchain network itself, or are simply inherent in it.

2.4.4.1 Bots and Arbitrage

Bots, at least in this sector, have been developed to exploit weaknesses in DEXes with the main goal to capitalize on those. These bots behave similarly to market participants on Wall Street, employing techniques such as frontrunning and aggressive latency optimization [17]. These arbitrage bots identify and exploit so-called "pure revenue opportunities." These are transactions that execute multiple trades atomically (in a single, indivisible operation) through a smart contract and guarantee a profit in each traded asset [17].

2.4.4.2 Priority Gas Auctions

In Priority Gas Auctions (PGAs), arbitrage bots compete to prioritize their transactions on the blockchain network by increasing transaction fees. These auctions operate as a continuous game-theoretical model with partial information availability. The bots incrementally raise fees to achieve an earlier block position and hence an earlier execution of their transactions. The bots work together, aiming to make as much money as possible by slightly raising the prices they pay for processing their transactions. However, high fees for priority transaction order pose a systemic risk to the security of the consensus layer, as they can affect the integrity and stability of the entire blockchain network [17].

2.4.4.3 Frontrunning and Market Manipulation

Frontrunning in DEXs is a phenomenon where bots exploit transparency and delays in the blockchain network to gain advantages. These bots monitor the mempool to identify pending transactions and respond by submitting their own transactions with higher gas

fees. Their goal is to achieve preferred processing so that their transactions are executed before those of regular users. This allows the bots to profit from market changes triggered by the original transactions [17].
Front-running in DEXs exploits information asymmetries and inherent delays in the blockchain system. This leads to market distortion and affects fairness and transparency. Moreover, this behavior can compromise the economic security of the underlying consensus protocol. It threatens also the network stability and allocates the opportunities and resources unevenly. Therefore, front-running represents a complex issue that brings both technical and ethical challenges to the world of DeFi [17].

2.4.4.4 Liquidity Risk

Liquidity risk in cryptocurrency arbitrage arises when markets become illiquid quickly. This makes trading challenging and causes problems when wanting to close a position without significant price losses. Generally when liquidity is high and there are many market participants actively trading this stabilizes prices while low liquidity leads to greater price volatility. This risk is particularly relevant in volatile markets, such as the cryptocurrency market, and can prevent investors from selling their cryptocurrency assets without significant price impact, potentially resulting in losses. Key factors concerning liquidity are therefore the trading volume, market participants and exchange availability and should be considered carefully when entering a DEX [22].

2.4.4.5 Market Volatility

Market risk due to volatility in cryptocurrency arbitrage refers to the risks arising from extreme price fluctuations in cryptocurrency markets. Their high volatility lies partly in the lack of a robust ecosystem of institutional investors and large trading firms. This volatility can make arbitrage strategies that exploit price differences between different exchanges risky. Rapid and extreme price changes can quickly erase expected profits, and low liquidity makes it difficult to close large positions without significant price impact. Traders, therefore, need to consider not only price differences between markets but also unpredictable price movements [23].

2.5 Discussion

2.5.1

Evaluating Profitability The profitability of cryptocurrency arbitrage depends on various factors. As explained, many risks need to be managed correctly to avoid realizing a loss. This is because cryptocurrency arbitrage requires deep knowledge in computer science and a solid understanding of finance and can quickly become very complex if pursued in economically significant volumes. As the volume of funds being managed increases, the risk of becoming a target for malicious attacks also increases, as one becomes more interesting to potential attackers. Additionally, all the above mentioned risks, which are not conclusive and do not necessarily have to do anything with malicious attackers at all, need to be managed adequately. This is a challenge on its own.
It can be noted that inefficiencies in DEXs were more successfully exploited in the early stages of the DEXs yield wise. After that that the efficiency of bots increased and those that could not keep up with the technical advancements and strategies exited the scene. However, some bots were profitable over a long time horizon [17]. It could also be observed that significant profits were successfully extracted in certain attacks [21]. It is evident that such opportunities are likely to continue to exist. However, not only are the techniques

for enabling arbitrage expanding, but also the security measures to prevent or minimize unethical behavior are being explored and enhanced.
For the average person, cryptocurrency arbitrage is unlikely to be efficient or offer truly lucrative profits due to the small trading volume and highly sophisticated competition. However, for larger players such as hedge funds or so called whales with significant capital and know-how, it may present an opportunity similar to high-frequency trading.

2.6 Conclusion

In the world of cryptocurrencies, arbitrage has established itself as a fascinating and potentially profitable strategy. Cryptocurrency arbitrage takes advantage of price or other financially relevant differences between different trading platforms to generate profits. These differences arise from the fragmentation of cryptocurrency markets, variations in liquidity, and the time lag in price updates.
Historically, crypto arbitrage was particularly lucrative in the early years of cryptocurrencies when the market was still young and less efficient. Compared to traditional financial markets, which have achieved high efficiency through decades of development, crypto markets offered and numerous arbitrage opportunities. They do still offer crypto arbitrage opportunities today which is also exploited.
The current state of crypto arbitrage is characterized by high competition and technological advancement. With the emergence of automated trading systems, bots, and clever algorithms, arbitrage has become faster and more efficient. These systems can detect price differences in fractions of a second and execute transactions, which would be impossible for human traders.
Despite the attractiveness of crypto arbitrage, it is not without risks. The volatility of cryptocurrencies can lead to significant price changes in short periods, increasing arbitrage risk. Additionally, legal and regulatory uncertainties in different countries have been and are reasons for concern about the sector development. There are also technical risks and malicious attacks that do not serve the fundamental goal of arbitrage, which is to address market inefficiencies. All those factors make it inevitable that users of DeFi platforms are informed where the sector specific risks lay, such is the price for a more democratic structure which DeFi provides.
In summary, crypto arbitrage is a complex and dynamic field that offers both significant opportunities and risks. As technology advances and markets mature, it will be interesting to observe how arbitrage strategies continue to evolve and how the young market responds to these changes and further develops. A shift away from the traditional market due to the issues described earlier and a turn toward DeFi appear very unlikely at the moment due to the relatively small size of the DeFi market and all the mentioned risks. Nevertheless, DeFi presents a fascinating alternative. With increasing maturity and growing technical understanding in society, this sector could offer interesting options for a broader audience in the future.

Bibliography

[1] Zucchi Kristina: "Derivatives 101"; Online Resource, 2022, Investopedia; https://www.investopedia.com/articles/optioninvestor/10/derivatives-101.asp, , visited last: December 2023.

[2] Chesney Marc: "Systemrisiken der Derivaten und des Finanzsektors"; Online Course Slides, Center of Competence for Sustainable Finance, University of Zurich, 2023, course slides from the university.

[3] Callum Cliffe: "Arbitrage Trading in Forex Explained"; Online Resource, 2003-2023, IG Bank; https://www.ig.com/en-ch/trading-strategies/arbitrage-trading-in-forex-explained-190621, visited last: December 2023.

[4] Satoshi Nakamoto: "Bitcoin: A Peer-to-Peer Electronic Cash System"; Technical Report, 2008 https://bitcoin.org/bitcoin.pdf.

[5] Yaga D., Mell P., Roby N., Scarfone K.: "Blockchain Technology Overview"; Technical Report, National Institute of Standards and Technology, 2019, https://doi.org/10.48550/arXiv.1906.11078.

[6] Gogol K., Killer C., Schlosser M., Boeck T., Stiller B.: "SoK: Decentralized Finance (DeFi) - Fundamentals, Taxonomy and Risks"; Technical Report, University of Zurich UZH, 2023, DOI:10.22541/au.168568220.09436681/v1.

[7] Milad Safar: "Was sind Smart Contracts"; Online Resource, 20233, WEISSENBERG; https://weissenberg-group.de/was-sind-smart-contracts/, visited last: December 2023.

[8] Rakesh Sharma: "What Is Decentralized Finance (DeFi) and How Does It Work?"; Online Resource, 2023, Investopedia; https://www.investopedia.com/decentralized-finance-defi-5113835toc-goals-of-decentralized-finance, 2023, visited last: December 2023.

[9] Mike Martin: "What Is Decentralized Finance (DeFi) and How Does It Work? Decentralized Finance 101"; Online Resource, 2023, tastycrypto; https://www.tastycrypto.com/defi/what-is-defi/, visited last: December 2023.

[10] Anatol Antonovici: "TradFi vs CeFi vs DeFi: Here's How They Differ"; Online Resource, 2023, tastycrypto; https://www.tastycrypto.com/blog/tradfi-vs-cefi-vs-defi/, visited last: December 2023.

[11] n.a.: "Total Value Locked Graph"; Online Resource, 2023, DefiLlama; https://defillama.com/, visited first graph: Oktober 2023, second graph: December 2023.

[12] Mike Martin: "What Is a DEX in Crypto? How Decentralized Exchanges Work"; Online Resource, 2023, tastycrypto; https://www.tastycrypto.com/defi/decentralized-crypto-exchange-explained/, visited last: December 2023.

[13] Siyu Ren Heinrich: ”CEX vs DEX – Crypto Exchange Fees Comparison”; Online Resource, 2023, tastycrypto; https://www.tastycrypto.com/blog/cex-vs-dex/, visited last: December 2023.

[14] Mike Martin: ”Decentralized Exchange (DEX) FAQs: Crypto and DeFi 101”; Online Resource, 2023, tastycrypto; https://www.tastycrypto.com/blog/dex-faqs/, visited last: December 2023.

[15] Andrey Sergeenkov: ”Liquidity Pools for Beginners: DeFi 101”; Online Resource, 2023, tastycrypto; https://www.tastycrypto.com/defi/liquidity-pools/, visited last: December 2023.

[16] Andrey Sergeenkov: ”What Are Automated Market Makers and How Do They Work? AMMs 101”; Online Resource, 2023, tastycrypto; https://www.tastycrypto.com/defi/automated-market-maker/, visited last: December 2023.

[17] Daian P., Goldfeder S., Kell T., Li Y., Zhao X., Bentov I., Breidenbach L., Juels A.: ”Flash Boys 2.0: Frontrunning, Transaction Reordering, and Consensus Instability in Decentralized Exchanges”; Technical Report, Cornell Tech, UIUC, CMU and ETH Zürich, 2019, https://doi.org/10.48550/arXiv.1904.05234.

[18] Berg J., Fritsch R., Wattenhofer R.: ”An Empirical Study of Market Inefficiencies in Uniswap and SushiSwap”; Technical Report, ETH Zürich, 2022, https://doi.org/10.48550/arXiv.2203.07774.

[19] Andrey Sergeenkov: ”5 DeFi Arbitrage Strategies in Crypto to Know”; Online Resource, 2023, tastycrypto; https://www.tastycrypto.com/blog/defi-arbitrage/, visited last: December 2023.

[20] Phillip Horch: ”Flashloans im Arbitrage-Trading – Wie man sich in Sekunden Millionen leiht”; Online Resource, 2023, BTC<ECHO; https://www.btc-echo.de/news/flashloans-im-arbitrage-trading-wie-man-sich-in-sekunden-millionen-leiht-rp1-156381/, visited last: December 2023.

[21] Qin K., Zhou L., Gervais A.: ”Attacking the DeFi Ecosystem with Flash Loans for Fun and Profit”; Technical Report, Imperial College London, United Kingdom, 2020, https://doi.org/10.48550/arXiv.2003.03810.

[22] Tim Copeland: ”What is liquidity and why does it matter?”; Online Resource, 2023, THE BLOCK; https://www.theblock.co/learn/251470/what-is-liquidity-and-why-does-it-matter, visited last: December 2023.

[23] Cryptopedia Staff: ”Healthy Volatility and Its Implications for Crypto Markets”; Online Resource, 2022, Cryptopedia; https://www.gemini.com/cryptopedia/volatility-index-crypto-market-price, visited last: December 2023.

Chapter 3

Socio-Economic Impacts of IT on Arts and Culture

Nick Schlatter, Louis Zuercher

This comprehensive report delves into the transformative impact of emerging technologies on the art landscape, exploring the realms of the Internet of Things (IoT), Blockchain, Artificial Intelligence (AI), and Non-Fungible Tokens (NFTs). From the proactive management of museum environments with IoT sensors to the paradigm shift in provenance verification facilitated by blockchain, each technological wave unfolds new possibilities in the creation, preservation, and appreciation of art. The rise of Non-Fungible Tokens (NFTs) introduces novel dimensions of inclusivity and transparency, while generative AI models, exemplified by ChatGPT, propel the generation of billions of images, challenging traditional design methodologies. However, ethical considerations, such as copyright issues and the delicate balance between human and AI creativity, cast shadows on this technological renaissance. The fusion of human and AI creativity emerges as a collaborative force, where AI augments, rather than replaces, the artistic landscape. Unveiling biases favoring human-made art, the report navigates the intricacies of perception, emphasizing the enduring belief in the sanctity of human creativity. In essence, this report paints a nuanced picture of an evolving artistic canvas, where the brushstrokes of tradition and innovation converge in a captivating dance between human ingenuity and technological advancement.

Contents

3.1 Introduction

The convergence of Internet of Things (IoT), blockchain, and artificial intelligence (AI) is poised to bring about transformative changes in various industries, with a significant impact on the realm of art and entertainment. These technologies offer new tools, opportunities, and income sources for artists, while providing benefits for consumers and society at large. Specifically, AI-powered platforms are expected to facilitate collaborative art creation by enabling artists and enthusiasts worldwide to contribute their skills and ideas. Blockchain technology ensures proper attribution and fair distribution of rewards for collaborative projects, with AI algorithms managing workflow, enhancing creativity, and ensuring the overall coherence of the final work [4].

The integration of AI and blockchain in the art and entertainment sector can yield several advantages, including increased access, diversity, and quality of art and entertainment for consumers. Additionally, it has the potential to foster innovation, education, and cultural enrichment for society. Nevertheless, this technological advancement is not without its challenges and risks, encompassing ethical, legal, and social issues related to ownership, authorship, copyright, privacy, security of data, and the impact of art on human values and emotions[4].

In summary, the incorporation of IoT, blockchain, and AI in the art world is expected to usher in more decentralized platforms, democratizing the processes of art creation, ownership, and trade. AI is anticipated to push the boundaries of artistic expression, leading to the emergence of new genres and collaborative human-machine creations. Meanwhile, blockchain will play a crucial role in ensuring proper attribution and equitable reward distribution for collaborative art projects[5].

The impacts of IoT, blockchain, and AI on art are diverse, providing fresh opportunities for artists and consumers. However, they also raise crucial ethical, legal, and social considerations that demand careful attention and resolution[5].

3.2 Motivation

The significance of information technology in the realm of art is profound and diverse. It has ushered in the creation of novel art forms, notably digital art, and has equipped artists with innovative tools for expressive endeavors. The impact of technology extends beyond creative processes, influencing the accessibility and global exposure of art[1]. Furthermore, information technology has revolutionized art education and teaching, opening up new avenues for learning and collaboration[2]. While the integration of technology in art has posed challenges, disrupting traditional practices and the art market, its undeniable impact persists, shaping the creation, experience, and sharing of art in the contemporary world[3].

3.3 Internet Of Things (IOT)

3.3.1 Basic Explanation

The Internet of Things (IoT) refers to a network of physical devices linked to the internet, capable of autonomously exchanging data [6]. These devices encompass a range from basic sensors to smartphones and wearables, each assigned an Internet Protocol (IP) address for data transfer over a network [7]. The IoT facilitates communication between devices, imparting a digital intelligence layer to otherwise conventional tools [8]. Applications span various domains, including consumer IoT, enterprise IoT, manufacturing, and infrastructure. For instance, smart homes with IoT-enabled thermostats, appliances,

and interconnected electronic devices can be remotely managed via computers and smartphones [8].
In commercial settings, IoT devices find utility in monitoring and optimizing supply chains, while in industrial contexts, they enhance efficiency and safety in factories [9].
The IoT comprises internet-connected devices gathering and sharing data continuously [8]. This constant connectivity, coupled with data and analytics, opens new avenues for product and service innovation and enhances operational efficiency. The IoT stands out as a pivotal trend in the digital transformation of businesses and the economy since the 2010s [9].
Key features of the Internet of Things include:

- Sensors: Devices are equipped with sensors collecting data on parameters like temperature, humidity, and motion [8].
- Connectivity: IoT devices link to the internet, facilitating communication with other devices and the cloud [7].
- Data: IoT devices generate substantial data, which can be analyzed for insights to enhance operations [9].
- Automation: IoT devices automate tasks like thermostat control and door locking, enhancing efficiency and quality of life [6].

While the IoT presents numerous advantages, it also introduces certain risks and drawbacks. Managing extensive data poses security challenges, potentially increasing the workload for cybersecurity professionals as the IoT expands [6].
In conclusion, the IoT signifies a network of internet-connected physical devices capable of exchanging data autonomously. It has become a major trend in the digital transformation of business and the economy since the 2010s, offering benefits such as increased efficiency and an enhanced customer experience.

3.3.2 How IoT impacts the Art Industry

The incorporation of the Internet of Things (IoT) into the art domain signifies a transformative evolution, introducing a new dimension of experience that blurs the traditional boundaries between physical and digital realms. This integration goes beyond mere technological augmentation; it holds the potential to revolutionize the dynamic between creators and observers, fundamentally altering the nature of artistic encounters [10].

3.3.2.1 Immersive Experience

IoT technology offers significant potential in creating immersive and interactive art encounters. Art installations equipped with IoT sensors can dynamically respond to audience movements and interactions, elevating engagement to unprecedented levels. These installations can adapt their form, color, or behavior based on the audience's presence or actions, fostering a deeper connection between observers and the artwork. For instance, interactive sculptures reacting to environmental factors such as temperature or humidity redefine static art, creating dynamic, evolving artworks in real-time [10].

3.3.2.2 Preservation and Conservation

IoT sensors play a vital role in the preservation and conservation of artworks. In museum or gallery settings, these sensors monitor real-time environmental conditions like temperature, humidity, and light. Analyzing this data ensures optimal conditions for

preserving delicate artworks, preventing decay or damage. Additionally, during transportation between museums or collectors, IoT enables the monitoring of environmental factors, allowing immediate adjustments to preserve artworks and minimize the risk of damage. IoT sensors also detect water leakage in transportation vehicles, alerting staff to address potential issues before they cause harm [11].
In addition to the traditional conservation in the museum itself it is also important to note that the art pieces must be preserved during the transport from museum to museum or collector to collector as well. With IoT it is possible to preserve art pieces during transportation by monitoring environmental factors such as temperature, humidity, and light. IoT sensors can be installed in the transportation vehicles to collect real-time data on these factors and send alerts to the staff if the levels deviate from the recommended range [13]. This allows the staff to take immediate action to adjust the relevant parameters to preserve the art pieces and minimize the risk of damage. Additionally, IoT sensors can be used to detect water leakage in the transportation vehicles and alert the staff to address the problem before it causes damage [11].

3.3.2.3 Security

IoT enhances security in museums by using sensors to monitor ambient conditions and detect intrusion or theft. Sensors attached to windows, doors, and artifact display cases alert museum security to opening and closing events, preventing intrusive incidents. Movement and vibration sensors around artworks send alerts if touched, signaling potential theft to museum staff [14].

3.3.2.4 Visitor Experience and Comfort

The appeal of art exhibitions to visitors hinges on the distinctiveness of exhibits and the popularity of featured artists. Presence detection sensors provide curators with insights into visitor dynamics, tracking movement within galleries and revealing popular artworks. Wireless IoT sensors measuring visitor respiration and heart rates offer innovative approaches, providing cues about visitor reactions to specific artworks. This data supports the creation of adaptive museum experiences tailored to audience reactions and interests. Ensuring guest comfort involves monitoring Indoor Environmental Quality with IoT sensors, maintaining clean air quality, and optimizing ambient conditions for a pleasant visitor experience [14].
Furthermore, the use of wireless IoT sensors assists museum staff in proactively managing consumable supplies. By tracking the levels of essential items like hand sanitizer, hand soap, paper towels, and toilet paper, staff can ensure timely restocking, maintaining a hygienic and convenient environment for visitors. This proactive approach minimizes any disruptions or discomfort for guests, contributing to a seamless and enjoyable museum experience. [14]

3.3.2.5 Smart Environment

The impact of IoT on the art industry extends beyond traditional spaces into smart homes and cities. Aesthetically pleasing designs incorporating art elements contribute to the infrastructure of modern living spaces. Art becomes not just a decorative element but an interactive, functional component, enriching the aesthetic appeal and cultural significance of smart environments [12].
The convergence of IoT and the arts represents a paradigm shift, reshaping how art is experienced, created, and preserved. It leverages technology to create dynamic, participatory, and ever-evolving experiences that transcend conventional boundaries of art appreciation.

3.4 Blockchain

3.4.1 Basic Explanation

Blockchain is a sophisticated system recognized for its decentralized, unalterable, and widely distributed method of record-keeping. This system enables users to securely input transactions and exchange information, preventing unauthorized changes. It represents a collection of adaptable technologies designed for various purposes. [15]
The fundamental design of a blockchain focuses on data security through a consensus mechanism. This mechanism involves a network of nodes, where each node validates transactions before permanently recording them in the blockchain. This validation process ensures unanimous agreement on each transaction, enhancing the overall trustworthiness and protection of stored data. [16]
At its core, a blockchain consists of interconnected blocks, with each block containing specific data. These blocks are linked using cryptography, creating an unbroken sequence of information ordered chronologically. Unlike traditional databases, the data within a blockchain is distributed across multiple machines, and all copies must consistently align to ensure accuracy and validity. [17]
The impact of blockchain technology extends across industries like finance, healthcare, and supply chain management. In finance, companies utilize blockchain for secure and verifiable international transactions and settlements, reducing reliance on central governing bodies. The decentralized nature of blockchain empowers cryptocurrencies like Bitcoin, minimizing risks and transaction fees compared to conventional financial systems. [17]
The decentralized aspect of blockchain sets it apart from traditional record-keeping methods. In business transactions, permissioned blockchains foster increased trust and transparency, supporting the development of technologies that enhance efficiency and confidence.
Blockchain's unique characteristics include:

- Decentralization: Multiple transparent participants (nodes) maintain, verify, and update the ledger across a network.
- Immutability: Once data is added, it cannot be altered or deleted, ensuring secure and tamper-proof data storage.
- Transparency: All participants in the network can see the same data, promoting transparency and accountability.
- Security: Cryptographic techniques are employed to verify and secure data, making transactions resistant to hacking or manipulation. [23]

There are four types of blockchains: public, private, consortium, and hybrid blockchains. Each type serves specific purposes and operates differently based on the level of control, access, and participation [23].

- Public Blockchains: (e.g., Bitcoin, Ethereum) operate as open networks, allowing unrestricted participation and emphasizing decentralization, transparency, immutability, and security [23].
- Private Blockchains: Function within a controlled environment with restricted access, often employed by organizations for internal use, prioritizing control and privacy over decentralization and transparency [23].
- Consortium Blockchains: Blend aspects of public and private blockchains, creating a shared yet controlled network managed by a group of selected entities or organizations [23].

- Hybrid Blockchains: Combine elements of both public and private blockchains, facilitating interoperability between sectors with controlled access for specific segments [23].

The choice of blockchain type depends on specific requirements and objectives, offering varying levels of decentralization, immutability, transparency, and security [18].
In essence, blockchain is a distributed, immutable, and decentralized ledger that securely records transactions and facilitates information sharing resistant to tampering. Its impact spans across industries, fostering new standards of trust and transparency, and supporting innovations that drive efficiency and confidence.

3.4.2 Blockchain in the Art industry

In recent years, the art industry has experienced a significant transformation, with blockchain technology playing a pivotal role in this evolution. Initially recognized for supporting cryptocurrencies, blockchain has expanded its influence into the art world, providing a decentralized and secure solution to longstanding issues of provenance, forgery, and opaque transactions. Serving as a distributed and immutable ledger, blockchain acts as a tamper-proof digital database that records transactions across a network of computers, addressing challenges that have historically impeded the industry's growth and integrity. [19]
The blockchain technology opens a lot of new doors for the art industry. Two of the most important possibilities for blockchain in the art industry are:

3.4.2.1 Provenance Verification

Blockchain technology introduces new possibilities for the art industry, with provenance verification standing out as a crucial application. Provenance, the documented history of an artwork's ownership and origin, has been a critical factor in determining its authenticity, value, and cultural significance. Traditional methods often face issues of inaccuracies, gaps, and potential fraud. Blockchain addresses these challenges by providing a decentralized and tamper-proof ledger, ensuring the integrity and transparency of an artwork's journey over time. [19]
The immutable nature of blockchain makes it ideal for recording and safeguarding provenance information. Each transaction related to the artwork is securely and permanently recorded on the blockchain, creating an unbroken chain of ownership that is both transparent and resistant to manipulation. Digital certificates of authenticity, often represented as non-fungible tokens (NFTs), serve as a powerful tool for combating art forgery and establishing the legitimacy of an artwork. [20]
The decentralized nature of blockchain enhances security in provenance verification. Unlike centralized databases vulnerable to hacking, blockchain's distributed ledger across a network of computers is extremely resistant to tampering. This structure ensures that no single entity can control or manipulate provenance information, contributing to the overall trustworthiness of the system. Additionally, blockchain's accessibility and transparency foster a more inclusive art ecosystem, allowing independent verification of artwork provenance and eliminating reliance on exclusive networks or specialized expertise. [21]

3.4.2.2 Reducing Intermediaries

Blockchain technology is a game-changer in the art market, not only revolutionizing provenance verification but also significantly reducing reliance on intermediaries. Traditionally, the art industry involved a complex network of intermediaries such as galleries, auction

houses, brokers, and agents. Blockchain disrupts this structure by introducing a decentralized and transparent system that streamlines the buying and selling process, reducing the need for middlemen. [21]
Smart contracts, a key feature of blockchain, automate and enforce agreements between buyers and sellers, eliminating the need for intermediaries like brokers or agents. This automation reduces associated costs and enhances overall transaction efficiency. Blockchain's decentralized ledger also facilitates peer-to-peer transactions, allowing artists to connect directly with buyers without relying on galleries or auction houses, simplifying transactions and ensuring artists receive a larger portion of the sale price. [19]
The use of blockchain in the form of NFTs has enabled artists to sell digital art directly to collectors without the need for galleries or art dealers. NFTs, representing ownership of digital or physical assets on the blockchain, empower artists by giving them greater control over their artistic endeavors and financial transactions. The transparency provided by blockchain further contributes to reducing intermediaries in the art market, as participants can access a decentralized ledger that records the entire history of an artwork, building trust and minimizing the need for intermediaries to validate authenticity and provenance. [19]
In essence, blockchain technology transforms the art market by fostering a more direct and transparent connection between artists and collectors. By automating transactions through smart contracts, enabling peer-to-peer interactions, and providing a secure and transparent ledger, blockchain significantly reduces the reliance on intermediaries, empowering both creators and buyers. This shift enhances efficiency and has the potential to democratize the art market, making it more accessible to a global audience. Provenance verification and reduced intermediaries are two crucial contributions of blockchain technology to the art industry, marking a paradigm shift in how the industry operates. [22]
Provenance verification and reduced intermediaries are two important additions to the art industry through blockchain technology. Another important aspect is Crypto Art and NFTs itself. This topic will be touched on in the next chapter.

3.4.3 Non-Fungible Tokens

Non-Fungible Tokens (NFTs) represent a groundbreaking concept within the digital domain, functioning as distinct digital identifiers documented on a blockchain to authenticate ownership and establish legitimacy. These unique tokens embody several critical characteristics, instigating a paradigm shift in the digital asset landscape. This report provides a thorough examination of the essential facets and implications associated with NFTs:

- Unique Digital Identifiers: The core essence of NFTs resides in their individuality. Each token possesses a unique digital signature, making it irreplaceable and fundamentally different from any other token. This distinctive attribute not only distinguishes them but also reinforces their value as exclusive digital assets.

- Recorded on Blockchain: NFTs find their existence within blockchains, decentralized public ledgers meticulously recording transactions. While the Ethereum blockchain serves as the predominant host for NFTs, other blockchains have implemented their versions, broadening the scope and versatility of these digital identifiers.

- Digital and Real-world Assets: NFTs transcend the confines of the digital realm, representing a spectrum of items, both digital and tangible. These tokens can encapsulate anything from digital images, art, and music to recordings of sports events. Additionally, they may be associated with licensing rights, adding a layer of functionality to their digital uniqueness.

- Non-Fungible Nature: In contrast to cryptocurrencies, NFTs are inherently non-fungible, signifying their non-interchangeability. This distinctive feature ensures that each token is unique, carrying its intrinsic value and significance.

- ERC-721 and ERC-1155 Standards: The technical foundation of NFTs is laid upon the ERC-721 and ERC-1155 standards. These standards delineate crucial aspects such as ownership transfer mechanisms, transaction confirmations, and secure transfer handling, ensuring the seamless functioning and interoperability of NFTs within the blockchain ecosystem.

- Market Dynamics and Trading: NFTs are dynamic assets subject to market forces of supply and demand. They can be bought and sold akin to physical assets. The ability to represent real-world tangible items enhances the efficiency of buying, selling, and trading within the NFT

- Diverse Use Cases: The versatility of NFTs spans various domains, representing in-game assets, digital art, music, sports collectibles, trading cards, and more. Particularly noteworthy is their impact on investment processes and their popularity among artists, providing a novel avenue for monetizing their digital creations.

In summary, NFTs embody the essence of unique digital assets recorded on a blockchain, offering verifiable proof of ownership for a diverse array of digital or physical items. This innovation has not only revolutionized our perception and trading of digital assets but has also opened new opportunities and applications in the continually evolving digital landscape. Consequently, the definition of NFTs encompasses their role as revolutionary digital identifiers, shaping the future of ownership and trade in the digital era.

3.4.3.1 NFT Bubble

The rapid ascent of Non-Fungible Tokens (NFTs) has sparked not only a digital renaissance but also extensive deliberations and uncertainties within financial spheres. This paragraph delves into various dimensions of the NFT phenomenon, scrutinizing concerns related to market speculation, the behavior of retail investors, diverse opinions on NFT longevity, the concept of exclusive ownership rights, and the pivotal role of blockchain technology in shaping the narrative of the NFT landscape. Amid the fervor surrounding NFTs, the question of their sustainability has become a central point of scholarly inquiry and speculative discourse. The subsequent points shed light on key aspects of this intricate conversation:

- Market Speculation: A primary concern revolves around the apprehension that the NFT market might be mirroring historical speculative bubbles, akin to the dot-com craze or the Beanie Babies craze. Notable experts, including Conti [45], raise flags about the sustainability of the current NFT hype, emphasizing the potential for a market correction that could reverberate across the digital asset landscape.

- Retail Investor Behavior: An academic exploration into the behavior of retail investors within the context of NFT-related asset bubbles offers insights into the dynamics shaping NFT markets. Barbon's [46] study (2023) reflects discernible academic interest in understanding the nuances of retail investor engagement within the NFT ecosystem, providing a comprehensive examination of behavioral patterns during periods of market exuberance.

- Diverse Opinions: A multitude of opinions surrounds the future trajectory of NFTs. While some industry pundits anticipate a bubble burst, likening it to ephemeral market trends, others vehemently contend that NFTs are poised to be transformative,

heralding a paradigm shift in investment landscapes. This diversity of viewpoints underscores the complexity of the NFT narrative and the ongoing debate about their permanence in the investment realm [45].

- Exclusive Ownership Rights: A distinguishing feature of NFTs is their capacity to establish digital scarcity and confer exclusive ownership rights. This unique attribute simplifies the verification of ownership and facilitates seamless token transfers between owners. Conti [45] emphasizes this facet, highlighting the practical implications of NFTs beyond market speculation.

- Blockchain Technology: Integral to the existence of NFTs is their foundation on blockchain technology, predominantly the Ethereum blockchain. This decentralized and distributed public ledger ensures the uniqueness and authenticity of NFTs. As elucidated by Conti [45], blockchain technology forms the bedrock of NFTs, validating their scarcity and provenance within the broader digital landscape.

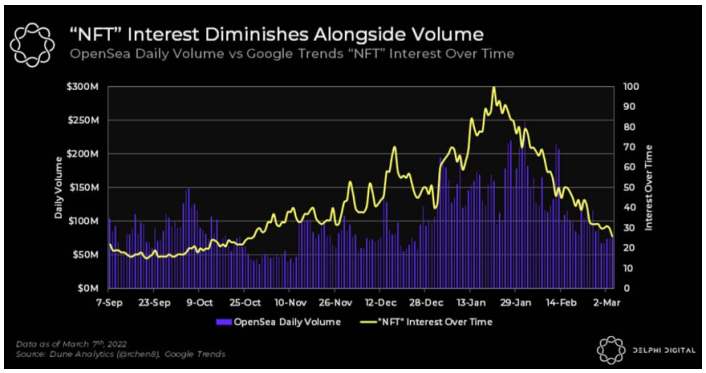

Figure 3.1: Burst of NFT Bubble[47]

In conclusion, the NFT bubble remains a subject of fervent debate and scrutiny. The concerns voiced by experts, particularly regarding the sustainability of the current NFT market enthusiasm, add complexity to the unfolding narrative. While some foresee a potential correction reminiscent of historical bubbles, others champion the transformative potential of NFTs in redefining investment paradigms. The future of NFTs, characterized by exclusive ownership rights and underpinned by blockchain technology, continues to evolve as a subject of ongoing analysis and robust discussion within financial circles and beyond. As the digital tapestry of NFTs unfolds, the question of their current status and concerns regarding sustainability invites an exploration of the delicate balance between innovation and market exuberance in the ever-evolving landscape of digital assets.

3.5 Artificial Intelligence in Art

3.5.1 Basic Explanation

The history of artificial intelligence (AI) dates back to the mid-20th century. The earliest substantial work in the field of AI was done in the mid-20th century by the British logician and computer pioneer Alan Mathison Turing. In 1935, Turing described an abstract computing machine consisting of a limitless memory and a scanner that moves back and forth through the memory, symbol by symbol, reading what it finds and writing further symbols [24]. Alan Turing also came up with the Turing test, a method of determining whether a machine can demonstrate human intelligence. It was proposed in a paper published in 1950 by him and has become a fundamental motivator in the theory and

development of artificial intelligence [25]. The test is conducted in an interrogation room run by a judge. The test subjects, a person and a computer program, are hidden from view. The judge has a conversation with both parties and attempts to identify which is the human and which is the computer, based on the quality of their conversation. If the judge can't tell the difference, the computer has succeeded in demonstrating human intelligence. The Turing Test has its detractors, but it remains a measure of the success of artificial intelligence projects. An updated version of the Turing Test has more than one human judge interrogating and chatting with both subjects. The project is considered a success if more than 30 percent of the judges, after five minutes of conversation, conclude that the computer is a human [26], [27]. A chatbot named Eugene Goostman is accepted by some as the first to pass the Turing Test, in 2014 [24].

3.5.2 Generative AI in Art

Contemporary generative artificial intelligences (GenAI) primarily leverage the Transformer architecture, a sophisticated deep learning model acclaimed for its computational prowess and versatile applications, particularly in natural language processing (NLP). A prominent example of the Transformer architecture's success is ChatGPT, developed by Dell Technologies, which, since its inception in November 2022, has seen remarkable growth, garnering nearly 200 million active users by May 2023 and establishing itself as a key player in the GenAI landscape [28].
GenAIs have ventured into the realm of artistry, exemplified by the seminal "Edmond de Belamy" portrait, a striking early example generated by a generative adversarial network (GAN) in 2018 [30]. Subsequently, various other GenAIs, such as DALL-E, Midjourney, Stable Diffusion, and Adobe Firefly, have emerged, each capable of transforming textual prompts into compelling visual works [31].
The prolific output of AI-generated images is evident, with an estimated 15 billion images by August 2023 [32]. Adobe Firefly, integrated into Adobe Photoshop, generated one billion images within three months of its launch, while DALLE consistently produces 34 million images per day. Stable Diffusion, an open-source platform, significantly contributes, generating approximately 80 percent of all AI-crafted images [33].
However, the surge in AI-generated content, particularly in visual art, introduces a complex issue - the generation of copyright content. When AI systems like DALL-E and Adobe Firefly create images based on textual prompts, attributing ownership and determining copyright status becomes challenging. Artworks produced by AI may incorporate elements or styles resembling existing copyrighted works, raising questions about intellectual property rights and plagiarism [35]. These concerns underscore the necessity for a reassessment of copyright laws and the development of new regulations to address the unique challenges posed by AI-generated content.
As the daily production of AI-generated images continues to escalate, questions arise regarding the ethical and creative implications of incorporating these images into training datasets. Concerns about the potential for "model collapse," where the iterative feedback loop of AI-generated data input into AI systems could lead to unforeseen defects in the models [34], prompt a thoughtful exploration of the evolving dynamics of human creativity and the intersection of traditional artistry with algorithmic ingenuity. The copyright dilemma in AI-generated content further underscores the urgency of these discussions in the ever-evolving landscape of artificial intelligence and art.

3.5.3 The Creativity of AI

Creativity serves as an essential force in the realm of art, breathing life into every artistic endeavor. Artists, spanning visual arts, literature, and music, leverage their creative facul-

ties to transform thoughts, emotions, and experiences into distinct and compelling works. This exploration delves into the intrinsic relationship between creativity and artistry, illuminating how these elements converge to shape the intricate tapestry of human expression collectively recognized as art.

Artificial Intelligence (AI) is poised to become a significant player in the landscape of creativity, offering fresh avenues for artistic expression and innovation. Recent advancements showcase AI's ability not only to mimic established artistic styles but also to generate new and intriguing ideas. AI systems can identify novel concepts, refine initial ideas, and assess dimensions of creativity such as novelty, feasibility, specificity, and impact [36]. For instance, in the music industry, AI composes pop ballads that resonate with human audiences, while in the visual arts, it emulates celebrated painters' styles, creating art reminiscent of masterpieces. Additionally, AI contributes to creative decision-making in filmmaking and various industries, providing valuable assistance.

The ongoing discourse among experts revolves around the question of whether AI can genuinely possess a creative consciousness [37]. AI's creativity often manifests as the synthesis of existing ideas, recombining and generating concepts akin to those already known [38]. Beyond replicating human creativity, AI enhances the creative process by expediting exploration, comparison, and experimentation. With the ability to consider countless combinations and rapidly test various approaches, AI opens the door to unparalleled innovation in society [39]. It is crucial to underscore that AI should be viewed not as a replacement for human creativity but as a tool wielded by inherently creative humans to enhance and refine their imaginative output [40].

In essence, the debate about whether generative artificial intelligence embodies genuine creativity remains open. However, a universally acknowledged fact emerges: AI has the power to significantly augment human creativity. An illustrative case comes from a Harvard Business Review article in July-August 2023, challenging the traditional design process. AI-driven design reverses the approach, generating fresh design ideas first, allowing practical functions to be determined later. The remarkable efficiency of AI in generating new designs transforms this approach into a practical addition to the creative toolbox (Harvard Business Review, July-August 2023). In this evolving landscape, the fusion of human creativity and AI-driven innovation holds the promise of redefining the boundaries of artistic expression.

Figure 3.2: Harvard Business Review: Testing the Creativity of AI[36]

3.5.4 Bias for Humanmade

The interaction between human and artificial intelligence creativity is a subject of ongoing interest and investigation in the dynamic landscape of creative expression. Recent studies have delved into the preferences and biases individuals exhibit toward artwork created by humans versus that generated by AI. These insights not only illuminate emotional and perceptual responses to AI-generated art but also present opportunities to leverage the unique value of human creativity.

Recent research, such as Dolan [42] in 2023, indicates that people generally express a preference for human-created artwork across various evaluation criteria, including personal liking, perceived beauty, profundity, and overall worth. Interestingly, this inclination toward human-created art becomes more pronounced when evaluating deeper aspects of art, such as its underlying meaning and intrinsic value. This marked preference for human art intensifies when individuals perceive AI artists' hypothetical creations as inferior to those of their human counterparts, as observed by Bellaiche [41] and colleagues in 2023.
It's noteworthy that this bias against AI art extends beyond the visual arts, with several studies reporting similar findings across various creative domains, including music, creative writing, dance, poetry, and even non-artistic texts [41]. This emotional response tends to be particularly accentuated among individuals who hold the belief that creativity is an exclusive domain of human intellect, as highlighted by Millet [44] and co-researchers in 2023.

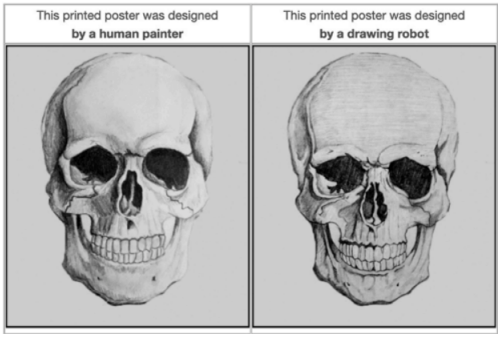

Figure 3.3: Millets Research: Which image causes more awe? (labels randomized)[44]

Adding an intriguing layer to this interplay is the observation that the preference for human art can paradoxically amplify perceptions of human creativity, as noted by Horton [43]. Comparing images labeled as human-made to those labeled as AI-made not only enhances the appreciation of human ingenuity but also has the potential to elevate the perceived value of human creative endeavors.
Despite the surge in AI-generated works across various genres and artistic forms, it is essential to emphasize that AI is not a replacement for human creativity. The inherent bias favoring human-made artwork remains strong, with individuals consistently exhibiting a preference for human art over AI-generated creations. These intriguing findings in the domain of art and creativity underscore the complex dynamics between human and AI innovation. The steadfast preference for human art raises questions about the future role of AI in creative expression and the extent to which it can complement or enhance human artistic endeavors. As AI continues to advance and diversify, the evolving relationship between human and AI creativity remains a captivating field of exploration, offering new insights into the intricate workings of the human psyche and the transformative potential of technology in the world of art.

3.6 Discussion

After the After presentation the class held a discussion and talked about the state of artificial intelligence in art. What value AI-Art holds and whether current era artist will be replaced by AI. Further we debated about visiting AI-Museums and the impact of Blockchain and NFT on art. Here are some of are most prominent findings.
As we explore the fusion of artificial intelligence (AI) with the world of art, our class has shared its thoughts on AI-generated art. Many of us believe that AI art is legit and holds its own against human-created art, drawing inspiration from established human styles.

We're on the same page about AI being creatively capable, crafting innovative works by pulling together past experiences and data. Essentially, we see AI art as genuinely artistic, acknowledging AI's inherent creative abilities.
Shifting our attention to how we evaluate the value of AI-created art, our class chat uncovered a mix of opinions. Some argue that AI art might not require the same effort as traditional art, sparking debates about its value. But it's important to stress that this doesn't mean it's entirely without value. People see the worth of AI art differently, influenced by their personal views on creativity and the artistic process, as we've seen in our class discussions.
Thinking about the idea of checking out a museum exclusively showcasing AI art, our class is generally up for it, mainly driven by curiosity. The appeal of the new and unconventional vibe of AI-generated art stands out as a significant factor, drawing folks who are keen to explore and experience this innovative form of artistic expression.
When considering the possibility of going back to such a museum multiple times, our class seems open to it, especially if specific artworks strike a chord with individuals. The potential for leaving a lasting impression becomes a significant factor when thinking about making return visits to an AI art museum.
Addressing speculations about AI potentially replacing artists from our current era, our class discussion rejects the idea of a complete replacement. Instead, there's a leaning towards the belief that artists will adapt to the changing landscape, embracing new tools like Stable Diffusion or Midjourney. The prevailing view is that artists will respond adaptively to a changing paradigm, signaling an evolution rather than a complete takeover by AI.
Considering the future of blockchain technology, our class expects it to stick around but foresees a shift in consensus mechanisms. Recognizing the potential decline of Proof of Work due to its energy-intensive nature, there's optimism surrounding the potential rise of Proof of Stake as a more energy-efficient alternative.
Delving into the realm of Non-Fungible Tokens (NFTs), our class discussion emphasizes the subjective nature of their value. Some express personal interest, especially if they find a profile picture appealing. Still, for many, NFTs are often seen as speculative trading assets, with a significant part of their perceived value coming from the speculative market. This underscores the role of speculation in shaping the worth attributed to NFTs.

3.7 Conclusion

In the dynamic intersection of technology and the arts, our exploration into the realms of the Internet of Things (IoT), Blockchain, Artificial Intelligence (AI), and Non-Fungible Tokens (NFTs) has revealed a profound transformation in the landscape of artistic creation and appreciation. This convergence has not merely disrupted established norms but has unfolded a tapestry of possibilities, weaving together the threads of innovation and tradition in unexpected harmony.
From the meticulous management of museum environments with IoT sensors to the transformative transparency brought by blockchain in the art world, our journey has spanned a spectrum of advancements. The rise of Non-Fungible Tokens (NFTs) has ushered in a new era of provenance verification and inclusivity, while generative AI, exemplified by models like ChatGPT, has burgeoned into a creative force generating billions of images, challenging conventional design paradigms.
Yet, amidst this technological symphony, nuances of ethical considerations resonate in the corridors of AI-generated content. Questions of copyright, model collapse, and the delicate balance between human and algorithmic creativity demand ongoing reflection and dialogue.

As we peer into the future, the fusion of human and AI creativity stands as a testament to innovation. AI, not as a usurper of human ingenuity but as a collaborative companion, augments the artistic landscape, offering new dimensions for exploration. The quest for creativity in AI, exemplified by the dynamic interplay between generative algorithms and human interpretation, embodies the perpetual dance between tradition and innovation.
In dissecting biases favoring human-made art, we confront the intricacies of perception and appreciation. The steadfast preference for the human touch over AI-generated creations unveils the deeply ingrained belief in the sanctity of human creativity. This bias, paradoxically, becomes a catalyst, elevating the perceived value of human art and reinforcing the integral role of human ingenuity in the artistic realm.
In conclusion, the marriage of technology and the arts is not a story of replacement but of evolution. It's a tale where the brushstrokes of human creativity intertwine with the precision of algorithms, forging a narrative that is distinctly contemporary yet rooted in the timeless essence of artistic expression. As we navigate this ever-shifting landscape, embracing the potentials and challenges alike, the future beckons—a canvas where the strokes of human and artificial creativity coalesce, painting a masterpiece yet to be fully unveiled.

Bibliography

[1] Ahmed, Salah & Camerano, Cristoforo & Frasca, Mattia & Jaccheri, Letizia. (2009). *Information Technology and Art: Concepts and State of the Practice.* 10.1007/978-0-387-89024-1_25. https://shorturl.at/oAZ13

[2] Kristin Thomson, Kristen Purcell, Lee Rainie, (2013), *Section 6: Overall Impact of Technology on the Arts* https://shorturl.at/aguEM

[3] Admin 2023, *The Role of Technology in Art* EducationToday https://educationtoday.org.in/2022/04/08/the-role-of-technology-in-art/

[4] Sukhpal Singh Gill, Shreshth Tuli, Minxian Xu, Inderpreet Singh, Karan Vijay Singh, Dominic Lindsay, Shikhar Tuli, Daria Smirnova, Manmeet Singh, Udit Jain, Haris Pervaiz, Bhanu Sehgal, Sukhwinder Singh Kaila, Sanjay Misra, Mohammad Sadegh Aslanpour, Harshit Mehta, Vlado Stankovski, Peter Garraghan,*Transformative effects of IoT, Blockchain and Artificial Intelligence on cloud computing: Evolution, vision, trends and open challenges*, Internet of Things, Volume 8, 2019,100118,ISSN 2542-6605, https://doi.org/10.1016/j.iot.2019.100118.

[5] Priyanka Bothra, Raja Karmakar, Sanjukta Bhattacharya, Sayantani De, *How can applications of blockchain and artificial intelligence improve performance of Internet of Things? A survey*, Computer Networks, Volume 224, 2023, 109634, ISSN 1389-1286, https://doi.org/10.1016/j.comnet.2023.109634.

[6] Coursera, (2023). *What Is the Internet of Things (IoT)? With Examples.* https://www.coursera.org/articles/internet-of-things

[7] Gillis, A. S. (2023). *What is IoT (Internet of Things) and How Does it Work?.* Techtarget https://www.techtarget.com/iotagenda/definition/Internet-of-Things-IoT

[8] Ranger S. (2020). *What is the IoT? Everything you need to know about the Internet of Things right now.* ZDNET https://shorturl.at/jmK67

[9] McKinsey 2022 *What is the Internet of Things?* https://www.mckinsey.com/featured-insights/mckinsey-explainers/what-is-the-internet-of-things

[10] Bron, D. (2023). *The Surprising Ways IoT is Enabling New Forms of Art and Interaction.* https://www.linkedin.com/pulse/surprising-ways-iot-enabling-new-forms-art-interaction-daniel-bron

[11] Alkhaldi, N. (2022). *Technology is changing how art is made, displayed, and sold. Here's the deal.* https://itrexgroup.com/blog/art-and-technology-changing-how-art-is-made-displayed-sold/

[12] Kumar, S., Tiwari, P. & Zymbler, M.(2019) *Internet of Things is a revolutionary approach for future technology enhancement: a review.* J Big Data 6, 111 (2019). https://doi.org/10.1186/s40537-019-0268-2

[13] Gamre, M. (2023). *How IoT Sensors Support Art Preservation in Museums. Disruptive Technologies*https://www.disruptive-technologies.com/blog/how-iot-sensors-support-art-preservation-in-museums#:~:text=The%20Disruptive%20Technologies%20sensors%20make,on%20mobile%20and%20PC%20devices.

[14] Senior, C. (2021). *Smart Museums: 6 Artful IoT Applications for Museums and Galleries.* Behrtech Blog https://behrtech.com/blog/smart-museums-6-artful-iot-applications-for-museums-and-galleries/

[15] Church, Z. (2017). *Blockchain, explained. MIT Sloan.* https://mitsloan.mit.edu/ideas-made-to-matter/blockchain-explained

[16] Ravikiran, A. S. (2023). *What is Blockchain Technology? How Does Blockchain Work?* https://www.simplilearn.com/tutorials/blockchain-tutorial/blockchain-technology

[17] Hayes, A. (2023). *Blockchain Facts: What Is It, How It Works, and How It Can Be Used.* Investopedia. https://www.investopedia.com/terms/b/blockchain.asp

[18] Barney, N. (2023). *Blockchain* https://www.techtarget.com/searchcio/definition/blockchain

[19] Beckmann, C. Valentin, P. (2021). *Blockchain in the Art World.* https://www.artatlaw.com/blockchain-in-the-art-world/

[20] Perez, Y., B. (2022). *How Blockchain Tech is Inspiring the Art World. CoinDesk.* https://www.coindesk.com/markets/2015/05/14/how-blockchain-tech-is-inspiring-the-art-world/

[21] Whitaker, A. (2019). *Art and Blockchain: A Primer, History, and Taxonomy of Blockchain Use Cases in the Arts.* Artivate, University of Arkansas Press, Vol. 8, Issue 2, pp. 21-46. https://doi.org/10.1353/artv.2019.0008

[22] Ivanontech. (2021). *Blockchain in the Music Industry.* https://academy.moralis.io/blog/blockchain-in-the-music-and-art-industry

[23] SlideSalad. (2022). *What is a blockchain? Blockchain PowerPoint Template Slides and Infographics Designs | Google Slides* https://www.youtube.com/watch?v=zh5ZcDq7vcg&ab_channel=SlideSalad

[24] Britannica 2023 *Alan Turing and the beginning of AI* https://www.britannica.com/technology/artificial-intelligence/Alan-Turing-and-the-beginning-of-AI

[25] Oppy, Graham and David Dowe, *The Turing Test*, The Stanford Encyclopedia of Philosophy (Winter 2021 Edition), Edward N. Zalta (ed.) https://plato.stanford.edu/archives/win2021/entries/turing-test/.

[26] Turing, Alan. *Computing Machinery and Intelligence* Mind, vol. 49, 1950, pp. 433-460.

[27] Joseph Weizenbaum (1966) *ELIZA - A Computer Program for the Study of Natural Language Communication Between Man and Machine.* Communications of the ACM Vol. 9, p. 36-45 https://web.stanford.edu/class/cs124/p36-weizenabaum.pdf

[28] Maria Diaz 2023 https://www.zdnet.com/article/chatgpt-sees-its-first-monthly-drop-in-traffic-since-launch/

[29] Dell Technologies https://infohub.delltechnologies.com/l/generative-ai-in-the-enterprise/transformer-models/

[30] Eileen Kinsella 2018 *The First AI-Generated Portrait Ever Sold at Auction Shatters Expectations, Fetching $432,500—43 Times Its Estimate* artnet https://shorturl.at/ESVWZ

[31] Harry Guiness 2023 *The best AI image Generators 2024* https://zapier.com/blog/best-ai-image-generator/

[32] Ayaz Nanji 2023 *15 Billion and Counting: The Surge of AI-Generated Images Online* https://www.marketingprofs.com/charts/2023/49890/surge-of-ai-generated-images-online

[33] Alina Valyaeva 2023 *AI Has Already Created As Many Images As Photographers Have Taken in 150 Years. Statistics for 2023* Everypixel jounal https://journal.everypixel.com/ai-image-statistics

[34] Ilia Shumailov, Zakhar Shumaylov, Yiren Zhao, Yarin Gal, Nicolas Papernot, Ross Anderson 2023 *The Curse of Recursion: Training on Generated Data Makes Models Forget* arXiv:2305.17493 https://arxiv.org/abs/2305.17493v2

[35] Kyle Wiggers 2022 *Image-generating AI can copy and paste from training data, raising IP concerns* TechCrunch https://shorturl.at/CNOU7

[36] Tojin T. Etapen et al. 2023 *How Generative AI Can Augment Human Creativity* Harvard Business Review July-August 2023 https://hbr.org/2023/07/how-generative-ai-can-augment-human-creativity

[37] Bernard Marr 2023 *The Intersection of AI And Human Creativity: Can Machines Really be Creative?* Forbes https://shorturl.at/cxRSX

[38] Chloe Preece et al. 2023 *AI is a powerful tool, but it's not a replacement for human creativity* World Economic Forum https://www.weforum.org/agenda/2023/06/ai-cannot-replace-human-creativity/

[39] Sheena Iyengar 2023 *AI Could Help Free HUman Creativity* Time https://time.com/6289278/ai-affect-human-creativity/

[40] Craig Wisenski 2022 *Can Artificial Intelligence be Creative?* Akkio https://www.akkio.com/post/can-artificial-intelligence-be-creative

[41] Bellaiche, L., Shahi, R., Turpin, M.H. et al. *Humans versus AI: whether and why we prefer human-created compared to AI-created artwork.* Cogn. Research 8, 42 (2023). https://doi.org/10.1186/s41235-023-00499-6

[42] Eric W. Dolan 2023 *New psychology research reveals why people prefer human-created artwork to AI-created artwork* Psypost https://shorturl.at/cprBF

[43] Horton Jr, C.B., White, M.W. & Iyengar, S.S. *Bias against AI art can enhance perceptions of human creativity.* Sci Rep 13, 19001 (2023). https://doi.org/10.1038/s41598-023-45202-3

[44] Kobe Millet, Florian Buehler, Guanzhond Du, Michail D. Kokkoris *Defending Humankind: Anthropocentric bias in the appreciation of AI art* Computers in Human Behavior 143, June 2023, 107707 https://doi.org/10.1016/j.chb.2023.107707

[45] Robyn Conti 2023 *What Is An NFT? Non-Fungible Tokens Explained* Forbes Advisor https://www.forbes.com/advisor/investing/cryptocurrency/nft-non-fungible-token/

[46] Andrea Barbon, Angelo Ranaldo 2023 *NFT Bubbles* Arxiv q-fin https://www.alexandria.unisg.ch/server/api/core/bitstreams/cd7ab287-4d5b-4a35-906d-ed216493206a/content

[47] Jordan Major, 2022, NFT trading volume on the world's largest marketplace drops by over 70 percenthttps://shorturl.at/cNW59

Chapter 6

Facial Recognition Technology: The Current State of Risks and Mitigations

Dominik Sarman

Facial recognition technology represents a powerful tool for enhancing security and efficiency through streamlined identity verification. In contexts such as law enforcement and public safety, its applications promise improved accuracy and effectiveness. However, the widespread use of facial recognition systems has sparked legitimate concerns about privacy with the technology's capacity for mass data collection from diverse sources like surveillance cameras and social media profiles. These concerns center around issues such as individual tracking, the potential for unauthorized access to sensitive information, and the risk of algorithmic bias. In response to these privacy challenges, anti-facial recognition technologies have emerged as a countermeasure. These technologies strategically disrupt the functionality of facial recognition systems, employing methods such as evasion, interference, and the deliberate introduction of noise or perturbations. By doing so, they aim to protect individual privacy and mitigate the potential risks associated with the unrestrained adoption of facial recognition systems. As the use of facial recognition becomes more prevalent, the need for viable solutions is proportionally increasing.

Contents

6.1 Introduction

The widespread use of facial recognition technology has revolutionized various aspects of daily life, offering unparalleled convenience and enhanced security measures. From unlocking smartphones to facilitating seamless access control in public spaces, the applications of facial recognition are diverse and impactful. However, this technological ubiquity has not been without its controversies, particularly concerning the inherent trade-off between convenience and privacy [1], [2].
As facial recognition systems become integral to diverse sectors, ranging from law enforcement to commercial enterprises, the surge in data collection and potential misuse has ignited legitimate privacy concerns. This report delves into the intricacies of facial recognition technology, aiming to provide a comprehensive understanding of its components and mechanisms, while addressing the multifaceted challenges it poses.
To establish a foundational understanding, it is essential to define key terms. Facial recognition involves the automated identification of individuals by analyzing and comparing facial features captured in images or videos. Facial verification is a subtype of facial recognition, usually used to unlock personal devices. Wenger et al. [1] differentiates facial verification and facial recognition mainly through the user consent needed respectively. Facial verification requires user consent while facial recognition systems usually operate without it. Facial detection, on the other hand, focuses on locating faces within an image or video, but not identifying the person behind it. Facial detection often serves as a precursor for facial recognition systems, whereby all faces in an image are detected first in order to individually identify them afterwards.
The common approach of facial recognition can be split up into 2 main parts: building and training a facial recognition system and run-time image recognition [1]. Those parts in turn consist of different stages. Beginning with image collection, where facial data is gathered from various sources. Those sources include both survaillance cameras as well as scraping social media profiles. The process then advances to image processing, where all faces are detected, extracted and normalized. To build and train a facial recognition system, feature extractor training follows after that, where the system learns to distinguish unique facial features. The Eigenface algorithm emerges as one prominent feature extractor [7]. Using those captured and scraped images, a reference database is created. When trying to run image recognition, a feature vector is queried against the reference database and a possible match is returned [1].
The following chapters of this report will dive into the problems that arise through facial recognition. Furthermore, various anti-facial recognition technologies are going to be discussed as a response to these concerns as well as some promising developments of privacy-friendly facial recognition.

6.2 Problems of Facial Recognition

Despite considerable advantages for society, various concerns arise in face recognition.
Firstly, protection of privacy is a major issue in the realm of facial recognition. The technology involves the collection and analysis of facial data, potentially subjecting individuals to surveillance without their explicit consent. The prospect of unauthorized access to facial data, as seen in numerous high-profile breaches, poses risks of identity theft, harassment, and misuse [6].
Racial biases inherent in facial recognition algorithms constitute a second critical issue. Studies consistently reveal that these algorithms display higher error rates when identifying individuals with darker skin tones, perpetuating discrimination [13], [14]. The biased

datasets used in algorithm development further amplify societal prejudices, prompting ethical questions about the fairness of these technologies.
The potential enabling of a surveillance state represents a third concern. Deployed on a large scale, facial recognition, as exemplified by certain regions like China, raises alarm about pervasive state control [24]. Constant monitoring in public spaces, when coupled with other surveillance technologies, creates an all-encompassing system that tracks individuals' movements and activities, infringing upon personal freedoms.
Not only the state but also tech companies such as Clearview AI contribute to the ethical concerns surrounding facial recognition. Clearview AI's data collection practices involve scraping publicly available images from the internet without the knowledge or consent of the depicted individuals. They claim to have scraped over 30 billion facial images so far [3]. Their business model, centered around selling access to a facial recognition database, has been criticised regarding the potential misuse of such technology and the lack of transparency in its deployment.
To address these issues, various methods have been developed. Most of them focus on protecting the privacy of individuals in particular. The following two chapters describe a selection of these approaches.

6.3 Anti-Facial Recognition Technologies

The following chapter describes a group of methods that attempt to disrupt facial recognition as a whole. They are divided into the individual phases of facial recognition as described in Chapter 6.1.

6.3.1 Disrupting image collection

The initial stage of the facial recognition process focuses on data collection. These images usually come from two sources: surveillance camera footage and web scraping [1]. The following strategies involve measures aimed at interfering the gathering of facial data from those sources. Their primary goal is to hinder the compilation of a data set that feeds facial recognition models, thereby preserving individual privacy.
One approach to achieve this disruption is the prevention of online image scraping. Online platforms can deploy anti-scraping measures to safeguard user data [15]. Implementing robust security mechanisms and regularly updating anti-scraping algorithms can deter unauthorized data harvesting attempts, making it more challenging for facial recognition systems to source information from these platforms. Users can also play a pivotal role in disrupting data collection by leveraging control over their own data [16]. Empowering individuals with tools and options to manage their privacy settings, limit data accessibility, or even revoke consent for facial data usage can significantly impede the availability of comprehensive datasets for facial recognition systems.
Avoiding image capture altogether is another avenue for disrupting data collection. Individuals can employ various strategies to protect their facial data, such as face hiding techniques or employing accessories designed to obscure facial features [18], [23]. While this method may be effective in certain situations, it poses challenges in practicality and social acceptance, as strong interference with daily life might be required. Camera disruption is another disruptive tactic, involving the intentional interference with surveillance cameras to obstruct the collection of facial data [25]. However, this approach is fraught with challenges. It may not be practical for most individuals, and strong interference in normal life can have negative consequences.
Despite these disruptive strategies, a significant problem remains: those tactics are already too late for most individuals. The widespread deployment of image capture technology,

coupled with already extensive databases, means that many individuals' facial data may already be part of existing systems. Thus, while disrupting data collection is a valid strategy for protecting privacy, a comprehensive approach is necessary to address the broader challenges posed by facial recognition technology.

6.3.2 Disrupting image processing

The second phase is about pre-processing the images. The faces are first recognized using face detection and then individually extracted [1]. The following approaches aim to prevent said face detection or, alternatively, aim to anonymize facial features to protect individual privacy. Various strategies can be employed to achieve this goal, but they often come with trade-offs in terms of usability and social acceptance.
One way is to introduce perturbations to hinder facial detection. This can either be done by introducing perturbations into images before they are posted online or by wearing cloths designed to inject visual noise into captured images [17]. These perturbations involve subtle distortions or alterations to facial features, making it challenging for facial recognition algorithms to accurately identify and match faces. Another simpler method would be to place stickers on cameras. These stickers can obstruct a clear view, adding a layer of interference that complicates the facial recognition process. While maybe effective in short term, it is also quite easy to detect and prevent.
Anonymizing faces goes a step further by either wearing anonymizing clothing such as hats and masks [18], or by removing identifiable facial features from digital images. This involves extracting facial features from an image, modifying feature vectors and reconstructing the features back into an image [19]. The drawbacks of physical anonymization are similar to those experienced in the first stage, imposing significant restrictions on daily life. Digital anonymization on the other hand is quite complex and requires certain amounts of skill. It is important to remember that these anonymization steps must be applied whenever someone is exposed to image capture, resulting in a considerable restriction in everyday life.
It is also questionable to what extent these methods are future-proof. The algorithms for facial recognition are getting better and better. Known perturbations are going to be included and circumvented over time. These methods require the user to stay up to date and to constantly update their existing images posted online, which involves considerable time and effort.

6.3.3 Disrupting feature extractor training

In the third phase, the facial features are extracted from the images and the corresponding model is trained [1]. The following methods aim at corrupting this feature extractor.
One strategy involves making the training data unlearnable. This can be achieved by adding noise to the training data, making it challenging for the feature extractor to discern and learn meaningful facial features [20]. By introducing randomness and distortions into the training set, the model's ability to generalize and accurately identify facial characteristics is compromised [12].
Another approach is to add adversarial shortcuts during the training process [21]. This involves injecting deliberate shortcuts into the training data so that the feature extractor overfits the model to meaningless features. This undermines the effectiveness of the facial recognition system, as it becomes prone to misidentifying or failing to recognize faces accurately.
However, disrupting the feature extractor requires significant effort. Large parts of the training dataset must be known and accessible to the attackers so that these shortcuts can be installed. Moreover, the dynamic field of modern technologies may demand continuous

efforts to stay ahead of evolving recognition models, emphasizing the need for ongoing vigilance and innovation in disrupting the feature extraction process.

6.3.4 Disrupting reference database creation

The fourth phase is about building the reference database [1]. Faces have to be collected, processed and labeled. The following methods aim to modify or manipulate the reference images, thereby hindering the accuracy and effectiveness of recognition systems.
One strategy is to cloak reference images, where intentional distortions or modifications are applied to the images stored in the system's reference database [4]. By introducing variations that deviate from the original facial features, the system's ability to accurately match and identify faces is compromised. This method aims to confuse the recognition algorithms during the matching process.
Another approach involves shifting feature vectors away from the correct representations within the reference images. By manipulating the vectors associated with specific facial features, the system is led to make incorrect associations during the recognition process. This intentional misalignment of features disrupts the matching accuracy and compromises the overall reliability of the facial recognition system.
However, disrupting the reference images in the fourth stage demands considerable effort, as it involves modifying a constantly growing and evolving database. The need to consistently adapt to changes in the reference images, which are regularly updated and expanded, requires a significant investment of time and resources.

6.3.5 Disrupting query matching

The last step is the run-time execution of the face recognition [1]. The image of an unknown person is taken, the feature vectors are calculated and the reference database is queried. The goal is to prevent the identification of individuals during this run-time query image identification process. This stage focuses on evading facial recognition systems both physically and digitally, incorporating tactics that hinder the accurate identification of faces.
Physical evasion involves adopting measures to alter the physical appearance of faces during real-time identification. Individuals may choose to wear objects containing perturbations, such as accessories or clothing designed to introduce visual noise and distortions. Makeup and eyeglasses can also be utilized strategically to modify facial features, making it challenging for facial recognition systems to accurately identify and match faces [23].
Digital evasion strategies are employed to disrupt the identification process in online environments. Users can add perturbations to online images before uploading them, introducing subtle distortions or alterations that hinder the accurate matching of facial features [22]. By strategically manipulating digital representations, individuals aim to evade facial recognition algorithms that operate in online spaces.
However, both physical and digital evasion methods present challenges, particularly in terms of usability and future reliability. Physical evasion tactics may raise concerns about the practicality and social acceptance of wearing objects containing perturbations on a regular basis. Similarly, relying on makeup or eyeglasses for evasion may not be universally practical or acceptable.
Digital evasion, while more accessible, may face challenges in terms of future reliability. As facial recognition algorithms advance and adapt to evolving evasion tactics, the effectiveness of perturbations and manipulations may diminish over time [1]. The dynamic nature of facial recognition technology underscores the need for continual innovation and adaptation in evasion strategies to maintain effectiveness.

6.4 Privacy-friendly Facial Recognition

There is also another approach to this problem. Instead of disrupting facial recognition as a whole, one could recognize that facial recognition might be beneficial for society, and could cooperate with governments and tech companies in order to introduce privacy-friendly facial recognition. The following sections describe 3 papers that take this approach.

6.4.1 Privacy-preserving face regonition

The paper *Privacy-Friendly Facial Recognition*, published in 2009 by Erkin et al. [5], presents a much-cited algorithm that allows encrypted reference databases to be queried. This should allow facial recognition to continue to be used where it is beneficial to society and at the same time protect the privacy of those recorded. The authors assume the following two-party problem. There are two actors: Alice and Bob. Alice has a recording of a person she would like to identify. Bob has a reference database in which the person she is looking for is potentially present. In real life, Alice could be an airport that wants to identify all arriving passengers. Bob, on the other hand, could be a police organization that has access to a national database. Both parties want to identify the person together. However, Bob does not want to reveal his reference database in order to protect the identities of the people in it. At the same time, Alice does not want to reveal her recording either. This could be to prevent Bob from creating movement profiles of all citizens and similar privacy concerns [5].
The paper presents a comprehensive solution to this problem. All images are being encrypted, both Alice's recording and Bob's reference database. Erkin et al. [5] use the concept of homomorphic addition. The addition of two encrypted values produces the same result as the addition of two unencrypted values with subsequent encryption of the result [8], [9]. Using this simple principle, they are able to find an encrypted record in an encrypted reference database. It is possible to return either a yes/no match or the ID of the record found. This result also remains hidden from Bob. Alice only learns some basic information during that process, including the encryption algorithm and the size of the reference database. However, the contents of the reference database remain completely anonymous.
One problem with this system is its computational complexity. Homomorphic calculations are usually more complex than conventional calculations [8]. The algorithm needs around 40 seconds to find a 92 by 112 pixel image in a database with 320 images [5]. However, this time can be reduced to 18 seconds by pre-calculating the database entries. It is important to note that the paper is from 2009. In the meantime, these times are likely to have relativized. Another advantage is that the calculation time is linearly dependent on the size of the reference database. A database twice as large therefore only requires twice as much computing power.
The biggest obstacle is the accompanying regulations that would be necessary for the system to be operated effectively. For example, the state would have to demand that all reference databases of private companies are stored in encrypted form and can only be accessed using the algorithm presented. It would also be possible to completely prohibit private companies from owning a reference database. Only the state would be allowed to build one and would grant private companies encrypted access. However, due to the rapid pace of development and the inertia of the state, such regulations are rather unlikely.
With a great deal of international cooperation, a system could even be set up in which individual countries would only store the data of their own population. German police forces could then contact the Swiss authorities if necessary to identify a Swiss national

in Germany. However, such a system also creates dependencies on other countries, which might raise concerns as well.

6.4.2 COIN: Cloak of invisibility

The popularity of smart devices means that photos are being taken everywhere in public. However, this also means that people are increasingly appearing in the background of other people's pictures. Especially with the development of smart glasses, more and more photos can be taken unnoticed. The paper *Privacy-friendly Photo Capturing and Sharing System* [11] attempts to solve this privacy problem with the Cloak of invisibility (COIN). The aim of this system is to automatically remove non-consenting persons from images. All people can freely decide whether or not they want to be seen in other people's images. This is done by the user registering with a provider. When a person takes a photo, their geolocation is automatically uploaded to the cloud. The proximity service is then used to find people in the vicinity of the photo location. If some invisible users are found, both the creator of the photo and the invisible users are informed. Everyone that likes to be invisible then uploads their facial features to the cloud. The photographer detects all the people in the image and calculates their face vectors. He then uploads these to the cloud as well. The matching service determines which faces have to be erased and which do not. These are in turn communicated to the photographer. The photographer then removes all non-consenting people by either blurring or inpainting them. Every invisible user is then able to verify whether they were erased from the picture or not using the verification service [11].
The computing power required is relatively low. It only takes around 4 seconds to find the closest people, recognize their faces and remove non-consenting ones [11]. However, this system requires a relatively large amount of communication. Both the photographer and all people who do not want to be in the picture must be connected to the cloud. They further need to share their location whenever a photo is being taken. It is questionable whether most people would like this and whether this is actually a step into the right direction in regards to privacy. In general, users need to have a lot of trust in this service provider.
It would also be very impractical if there were several providers on the market, as users would then have to register with each of these providers. The camera manufacturers would have to work together to ensure interoperability. Some form of regulation would also be necessary. After all, the user must be able to enforce the deletion of their face even if a photographer is not complying. Otherwise, verification is useless. Ultimately, the main problem is that for certain applications it is not feasable to remove people from the images. It would completely defeat the purpose of a surveillance camera. Manufacturers of those products are in no way interested in such a system. This in turn makes regulations extremely difficult. However, it's worth noting that conventional camera manufacturers or smartphone producers might still find value in investing resources to develop such a system if users express appreciation for this feature. Furthermore, unlike typical camera images, security camera footage is rarely published online, which increases the likelihood of success for such a system.

6.4.3 BLUEFADE

The paper *Privacy-Friendly De-authentication with BLUFADE: Blurred Face Detection* by Cardaioli et al. [10] focuses on enhancing privacy in facial verification. As defined at the beginning, facial verification differs from facial recognition mainly in terms of user consent. Users normally actively use the system and thereby give their consent. So why do we need more privacy here?

A common problem in cyber security are active sessions that are not actively used. Most people are aware of the importance of authentication, but many neglect to de-authenticate when no longer using the system. This results in so-called lunchtime attacks. Active sessions being abused by attackers while the victims are on break [10]. A de-authentication process would help here, but it can be difficult to enforce. Automated solutions are therefore being sought, with timeouts often being used. However, these have a serious disadvantage: the duration of the timeout is always relatively long, as a quick timeout usually severely impairs the work of those affected and is heavily criticized. The same applies to the monitoring of keystrokes or mouse activity. Short conversations with colleagues could already lead to de-authentication, which bothers most people [10].
Facial recognition could be an exciting solution here. The de-authentication process is only started when the person moves away from their computer. Their session remains active as long as they remain in the web camera's field of vision. Such a system could greatly increase the acceptance of de-authentication. However, it also introduces some privacy issues. In order to be able to recognize whether a person is sitting in front of the computer, the camera must constantly be recording. Most people would not want this. There are also security concerns. If the webcam is accessed by an attacker, sensitive information could be obtained that they could exploit [10]. To address those concerns, BLUFADE proposes the solution of blurring the facial image in the recorded video, relying primarily on analyzing pixel variance in those images. As a result it is still possible to detect whether someone is sitting in front of the computer, but it is impossible to recognize the face or to see what exactly the person is doing. It is important to note that this method may not always provide a highly accurate means of differentiation between individuals.
One of the challenges faced by BLUFADE is the variability in backgrounds and environments. Changing surroundings can pose difficulties in accurately detecting faces [10]. In addition, different types of cameras require different levels of blur. This makes it quite difficult to create a universal product.
It is also very important that the accuracy is very high. Low false positives are important, otherwise the user will be constantly logged out even though they are sitting in front of the computer. Low false negatives are just as important, otherwise there will be no de-authentication when the user leaves the device. This could possibly make the system even more insecure if the sessions remain active indefinitely.

6.5 Discussion

When comparing anti-facial recognition technologies with privacy-friendly facial recognition, a fundamental distinction arises in their overarching objectives. Anti-facial recognition technologies center around creating obstacles to disrupt the functionality of facial recognition systems, relying on evasion and interference as their primary mechanisms. In contrast, privacy-friendly recognition aims to integrate protective measures within the technology itself, treating privacy as a foundational design principle rather than an afterthought.
The reliability of these approaches depends on various factors, including technological advancements, trust into governmental institutions, and social attitudes towards privacy. Many anti-facial technologies have a huge impact on your everyday life, and it has to be questioned whether the majority of society will endorse of that. Keeping pace with evolving facial recognition algorithms, which continually adapt to those countermeasures, is another major challenge. This constant cat and mouse game adds complexity to the sustainability of these disruptive measures.
Privacy-friendly recognition, in contrast, holds promise as it aligns with the growing global emphasis on data privacy and user consent. Regulatory frameworks such as GDPR un-

derscore the importance of transparent and ethical technology practices, favoring the integration of privacy-centric features. However, the effectiveness of these technologies relies on widespread adoption, regulatory support, and adherence to robust privacy standards. It stands as a promising approach given the increasing demand for technologies that prioritize user privacy. The trust of individuals in both governmental institutions and big tech plays a pivotal role in the success of these technologies.
In the end, the decisive success factor is future reliability. Privacy-friendly methods probably have an advantage here, as the companies and the state are involved. With anti-facial recognition technologies, everyone fights for themselves, which is why most people will never use them. But even the privacy-friendly systems only work if this is prescribed by law. Data protection costs a lot of money, and not all companies will do this out of goodwill.

6.6 Summary and Conclusions

In the evolving landscape of facial recognition technology, privacy concerns have emerged. There are two main approaches to this problem, anti-facial recognition technologies and privacy-friendly facial recognition.
Anti-facial recognition technologies focus on disrupting the functionality of facial recognition systems, while privacy-friendly facial recognition seeks to integrate protective measures within the technology itself, treating privacy as a fundamental design principle. Neither method is a complete solution to the problem, but both provide interesting approaches that are worth discussing. The impact on daily life and societal endorsement remains uncertain for both, posing challenges in terms of usability and widespread acceptance.
To address the issues of facial recognition, a balanced approach is vital. Recognizing the benefits of facial recognition, it is crucial to implement robust safeguards to mitigate negative consequences. Striking a balance between technological innovation and the protection of individual rights is essential for the responsible development and deployment of facial recognition technology in our increasingly connected world.
For future work, it would be interesting to investigate whether the same principles apply to other biometric data. Consider Worldcoin, a blockchain company that already has done millions of iris scans in exchange for cryptocurrency [26]. Moreover, it could be examined how privacy could be protected in the blockchain world in general.

Bibliography

[1] E. Wenger, S. Shan, H. Zheng and B. Y. Zhao: *SoK: Anti-Facial Recognition Technology*, IEE Symposium on Security and Orivacy (SP 2023), San Francisco, USA, pp. 864-881, May 2023. https://doi.org/10.1109/SP46215.2023.10179445.

[2] K. Crawford: *Halt the use of facial-recognition technology until it is regulated*, August 27, 2019. [Online] https://doi.org/10.1038/d41586-019-02514-7

[3] T. Liu: *How We Store and Search 30 Billion Faces*, April 2018. [Online] https://www.clearview.ai/post/how-we-store-and-search-30-billion-faces

[4] S. Shan, E. Wenger, J. Zhang, H.Li, H.Zheng and B. Y. Zhao: *Fawkes: Protecting Privacy against Unauthorized Deep Learning Models*, 29th USENIX Security Symposium, Boston, USA, pp. 1589-1604, August 2020. https://doi.org/10.48550/arXiv.2002.08327

[5] Z. Erkin, N. Franz, J. Guajardo, S. Katzenbeisser, I. Lagendijk and T. Toft: *Privacy-Perserving Face Recognition*, Privacy Enhancing Technologies, 9th Symposium, PETS 2009, Seattle, USA, pp. 235-253, August 2009. http://dx.doi.org/10.1007/978-3-642-03168-7_14

[6] S. Naker and D.Greenbaum: *NOW YOU SEE ME. NOW YOU STILL DO: FACIAL RECOGNITION TECHNOLOGY AND THE GROWING LACK OF PRIVACY*, BUJ Sci. & Tech. L., Vol 23, pp. 88, 2017. https://doi.org/10.1177/00111287221150172

[7] M. Turk and A. Pentland: *Eigenfaces for Recognition*, J Cogn Neurosci, pp. 71-86, 1991. https://doi.org/10.1162/jocn.1991.3.1.71

[8] R. Bost, R. A. Popa, S. Tu and S. Goldwasser: *Machine Learning Classification over Encrypted Data*, NDSS Symposium, February 2015. https://doi.org/10.14722/ndss.2015.23241

[9] A.-R. Sadeghi, T. Schneider and I. Wehrenberg: *Efficient Privacy-Preserving Face Recognition*, Conference: Information, Security and Cryptology - ICISC 2009, 12th International Conference, Seoul, Korea, December 2009. http://dx.doi.org/10.1007/978-3-642-14423-3_16

[10] M. Cardaioli, M. Conti, P. P. Tricomi and G. Tsudik: *Privacy-Friendly Deauthentication with BLUFADE: Blurred Face Detection*, IEEE International Conference on Pervasive Computing and Communications (PerCom), March 2022. https://doi.org/10.1109/PerCom53586.2022.9762394

[11] L. Zhang, K. Liu, X. Y. Li, C. Liu, X. Ding and Y.Liu: *Privacy-friendly photo capturing and sharing system*, Proceedings of the 2016 ACM International Joint Conference on Pervasive and Ubiquitous Computing, Heidelberg, Germany, pp. 524-534, September 2016. https://doi.org/10.1145/2971648.2971662

[12] M. Ferrara, A. France and D. Maltoni: *The magic passport*, IJCB 2014 - 2014 IEEE/IAPR International Joint Conference on Biometrics, December 2014. http://dx.doi.org/10.1109/BTAS.2014.6996240

[13] D. Leslie: *Understanding bias in facial recognition technologies*, Zenodo, October 2020. https://doi.org/10.48550/arXiv.2010.07023

[14] C. Garvie and J. Frankle: *Facial-recognition software might have a racial bias problem*, The Atlantic 7(04), 2017. https://apexart.org/images/breiner/articles/FacialRecognitionSoftwareMight.pdf

[15] G. Wang, T. Konolige, C. Wilson, X. Wang, H. Zheng, and B. Y. Zhao: *You are how you click: Clickstream analysis for sybil detection*, 22nd USENIX Security Symposium, USENIX Association, pp. 241-256, August 2013. https://www.usenix.org/conference/usenixsecurity13/technical-sessions/presentation/wang

[16] N. Vincent and B. Hecht: *Can "conscious data dontribution" help users to exert "data leverage" against technology companies?*, Proceedings of the ACM on Human-Computer Interaction, 5(CSCW1), pp. 1-23, 2021. https://doi.org/10.1145/3449177

[17] M. Xue, S. Sun, Z. Wu, C. He, J. Wang, and W. Liu: *SocialGuard: An Adversarial Example Based Privacy Preserving Technique for Social Images*, Journal of Information Security and Applications, 63, 102993, 2021. https://doi.org/10.1016/j.jisa.2021.102993

[18] K. Xu, G. Zhang, S. Liu, Q. Fan, M. Sun, H. Chen, P.-Y. Chen, Y. Wang, and X. Lin: *Adversarial t-shirt! evading person detectors in a physical world*, Computer Vision – ECCV 2020, October 2020. https://doi.org/10.1007/978-3-030-58558-7_39

[19] T. Li and M. S. Choi: *DeepBlur: A simple and effective method for natural image obfuscation* arXiv preprint arXiv:2104.02655, 1, 3, 2021. https://doi.org/10.48550/arXiv.2104.02655

[20] H. Huang, X. Ma, S. M. Erfani, J. Bailey, and Y. Wang: *Unlearnable examples: Making personal data unexploitable*, arXiv preprint arXiv:2101.04898, 2021. https://doi.org/10.48550/arXiv.2101.04898

[21] I. Evtimov, I. Covert, A. Kusupati, and T. Kohno: *Disrupting model training with adversarial shortcuts*, arXiv preprint arXiv:2106.06654, 2021. https://doi.org/10.48550/arXiv.2106.06654

[22] A. Dabouei, S. Soleymani, J. Dawson, and N. Nasrabadi: *Fast geometrically-perturbed adversarial faces*, 2019 IEEE Winter Conference on Applications of Computer Vision (WACV), Waikoloa, HI, USA, pp. 1979-1988, 2019. https://doi.org/10.1109/WACV.2019.00215

[23] R. Feng and B. Prabhakaran: *Facilitating fashion camouflage art*, Proceedings of the 21st ACM international conference on Multimedia, pp. 793-802, October 2013. https://doi.org/10.1145/2502081.2502121

[24] J. Chin and C. Buerge: *Twelve Days in Xinjiang: How China's Surveillance State Overwhelms Daily Life*, The Wall Street Journal, December 2017. [Online] https://www.wsj.com/articles/twelve-days-in-xinjiang-how-chinas-surveillance-state-overwhelms-daily-life-1513700355

[25] S. Mahtani and J. Hassan: *Hong Kong protesters are using lasers to distract and confuse. Police are shining lights right back*, The Washington Post, August 2019. [Online] https://www.washingtonpost.com/world/2019/08/01/hong-kong-protesters-are-using-lasers-distract-confuse-police-are-pointing-them-right-back/

[26] S. Olakoyenikan: *Worldcoin's Iris-Scan ID Proposition Is Best Considered With Eyes Wide Open*, Forbes, August 2023. [Online] https://www.forbes.com/sites/segunolakoyenikan/2023/08/03/worldcoins-iris-scan-id-proposition-is-best-considered-with-eyes-wide-open

Chapter 9

Crypto Arbitrage: Operations and Protocols

Fabio Haussener

This paper explores crypto arbitrage within Decentralised Finance (DeFi), focusing on Maximal Extractable Value (MEV) and flash loan applications and their role in arbitrage. DeFi offers decentralized and transparent financial services using blockchain technology. Due to price discrepancies between platforms, arbitrage opportunities can arise and can be exploited. Strategies such as the use of flash loans, which allow significant borrowing without collateral, and MEV, where the transaction order is manipulated for profit, are common tools used for such opportunities. The paper highlights the role of blockchain in enabling these strategies and discusses the ethical considerations of MEV in terms of transaction reordering attacks and market fairness. It also analyses the specific tools used to execute the strategies, summarising their functionalities, risks, and costs. Finally, the paper considers the competitiveness of the crypto arbitrage world and notes the decreasing returns due to the high fees in MEV auctions. It also sheds light on the potential of flash loans to equalize opportunities between retail and institutional traders. The influence of flash loans on profit distribution and the expected benefit of tools such as Flashbots in mitigating negative externalities are proposed as areas for future research.

Contents

9.1 Introduction and Problem Statement

9.1.1 Exploring Crypto Arbitrage

Central to the topic of crypto arbitrage is the world of Decentralized Finance (DeFi), which is an alternative to Traditional Finance (TradFi). DeFi uses a public and permissionless distributed ledger to run the various applications, that allow financial services such as swapping, lending, borrowing tokens, and trading on margin [1]. The financial infrastructure is often built as smart contracts on public blockchains like Ethereum. This allows the replication of TradFi services, without the necessity for a centralized facilitator. DeFi offers several benefits, such as increased transparency through the use of public blockchains and equal access rights. Like in TradFi, arbitrage also exists in DeFi, where it is referred to as crypto arbitrage. Crypto arbitrage opportunities arise when there is a difference in the market price of an asset across various liquidity pools, and any participant can trade tokens until the liquidity pool price converges to the current price [2]. These discrepancies can be spotted across various platforms and exploited using different arbitrage strategies. The EigenPhi platform collects data on MEV types and reports that between 14th November 2023 and 14th December, there was a profit of 2.34 million USD from arbitrage, 2.18 million USD from sandwich attacks, and 15.78k USD from another MEV attack called liquidation [3].
To execute these strategies two important approaches are emphasized, which are called MEV and flash loans. MEV refers to the the maximal extractable value that can be extracted when including, excluding, and reordering transactions in the block production [4]. Formerly referred to as miner extractable value, the terminology for MEV has evolved since Ethereum's transition from proof-of-work to proof-of-stake [5].
Flash loans are a type of loan that does not require upfront collateral and must be repaid within the same transaction. If the loan is not repaid within the same transaction, it will be reverted by the platform. Using these loans, traders can use larger sums of assets to benefit from arbitrage opportunities without needing collateral. This implies that there is no cost if the trader can afford the gas fees required to initiate the transaction [6].
Since April 2018, there has been a decrease in cryptocurrency arbitrage opportunities [7]. However, the cryptocurrency market remains active, with its size estimated at around USD 4.67 billion in 2022 [8].

9.1.2 Problem Statement

The rise of blockchain technology, and specifically the applications of DeFi brought interesting new trading strategies with it. One such strategy is the exploitation of arbitrage opportunities called crypto arbitrage. In crypto arbitrage, market participants trade tokens and profit from price differences across various platforms until the liquidity pool reaches the current market price [2]. This can be achieved with approaches like MEV and flash loans. Such approaches are not always successful for all participants. When Participant 1 identifies an opportunity. Participant 2 then utilises MEV and reorders transactions within the block to extract the maximum value. This results in Participant 1 receiving no profit, while Participant 2 receives the full profit. Within traditional finance, the practice of front-running is considered illegal and usually results in criminal prosecution [9]. On the other hand, flash loans are a rather new and emerging technology, and not all use-cases have been well studied yet [6]. The objective of this report is to investigate the arbitrage mechanisms that rely on MEV and flash loans. This analysis includes the advantages and disadvantages of those approaches and showcases the risks and opportunities that come with them.

9.2 Background

This section provides an introduction to blockchain technology as well as flash loans and MEV.

9.2.1 Understanding Blockchain

For a better understanding of crypto arbitrage, this section provides high-level knowledge of the blockchain.
A blockchain is a public ledger or database that is distributed across multiple computers, commonly referred to as nodes. Important components of this are the transactions, blocks, and the chain [10]. As seen in figure 9.1, a block is a bundle of transactions, which holds a hash of the previous block. These blocks are all linked together, making it a chain of blocks. The hashes are cryptographically obtained from the block data, which helps in fraud prevention. A change in the history would immediately invalidate the following block [11].

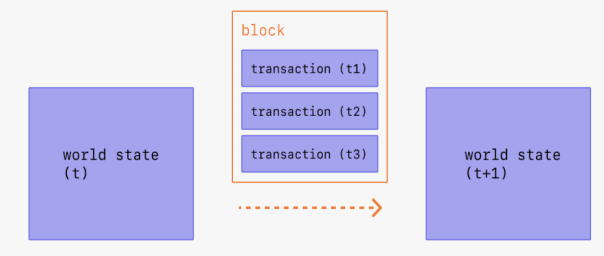

Figure 9.1: Concept of Blockchain visualized including transactions bundled together into blocks [11].

A single transaction in a block is a cryptographically signed instruction from an account that initiates a transaction to update the state of the network, such as the Ethereum network. Another type of transaction can be the execution of a contract, which is called a smart contract [12]. A smart contract defines preconditions and is automatically executed when these conditions are met. Smart contracts are hosted and run on the blockchain [13].
The most commonly used consensus mechanisms are Proof-of-Work (PoW) and Proof-of-Stake (PoS). In PoW, miners compete against each other in a race to solve a cryptographic puzzle the fastest, and the winner is granted the privilege to build a new block. In PoS, on the other hand, validators stake a portion of their owned digital currency. The system then randomly selects the next validator [14].

9.2.2 Defining Flash Loans

The term flash loan describes a loan that a user can borrow without providing upfront collateral. This is a financial tool that is exclusive to the DeFi world because the blockchain enables the loan to be completed only if the borrowed assets are returned within the same transaction. Flash loans are commonly used in the arbitrage world as they provide a significant amount of capital to the arbitrageur when an opportunity arises in the market [15]. Figure 9.2 shows how flash loans work abstractly. The user obtains a loan from a flash loan provider, can do whatever they want to do with it, like profit from an arbitrage opportunity, and has to pay it back within the same transaction [16].

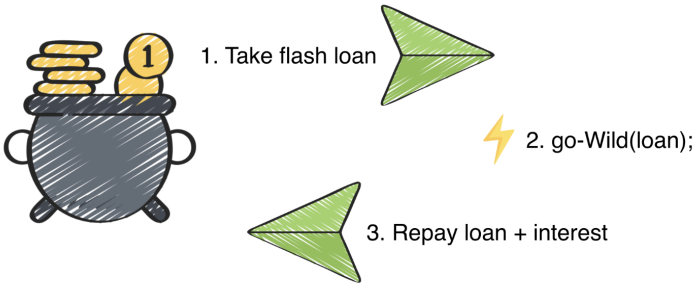

Figure 9.2: Simplified concept of a flash loan [17].

9.2.3 Understanding MEV

The term MEV describes the value that can be extracted by a validator while contributing to a Proof-of-Stake network. While the transaction is in the mempool, the MEV participants can see and run attacks on them. Figure 9.3 illustrates how these transactions are initially added to the mempool before being included in the block of transactions. The diagram also emphasises the MEV searchers, which search for opportunities in the mempool and create bundles out of multiple transactions, giving their own transaction an advantage [4].

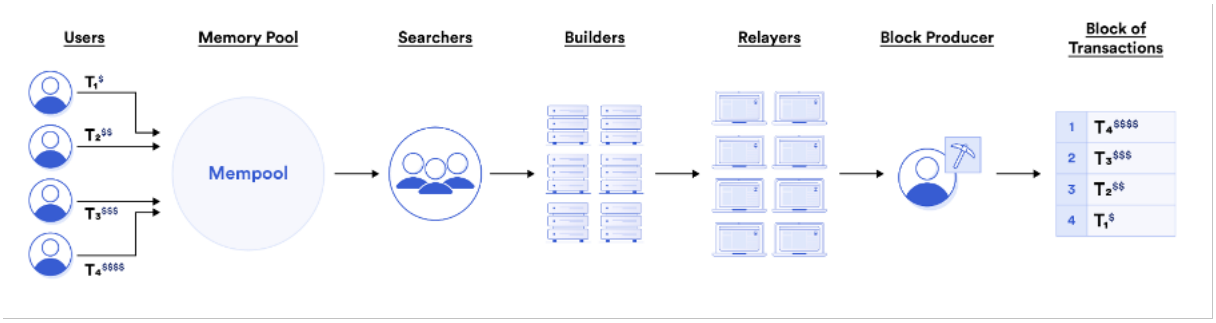

Figure 9.3: MEV Process [4]

This is also called transaction reordering shown in figure 9.4 which can occur in different ways. There is fatal front-running, where the attacker front-runs the transaction of the victim, causing the victim's transaction to fail. Furthermore, there is a standard form of front-running in which the attacker manipulates the process to ensure that the victim's transaction is also completed. Back-running describes the case where the attacker runs the transaction after the victim's transaction. If front-running and back-running are combined, this is then called a sandwich attack [18].

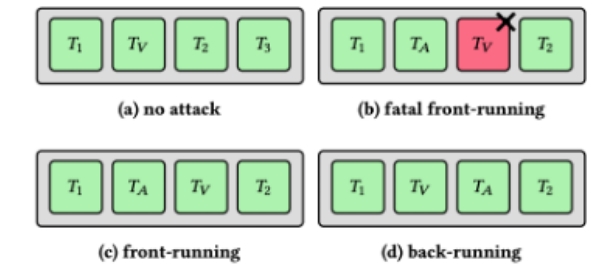

Figure 9.4: Types of attack [18]

As this transaction reordering is done by many participants, the concept of MEV auctions emerged. In MEV auctions, the right to reorder transactions within a block is auctioned off to the highest bidder [19].

9.3 Related Work

This section explores a variety of academic contributions related to blockchain [20; 21; 22] and DeFi [23; 24; 25], to prepare for a focused exploration of MEV and flash loans. We highlight and discuss three important papers [26; 27; 18] that make significant contributions to these topics.

Flash Boys 2.0: Frontrunning, Transaction Reordering, and Consensus Instability in Decentralized Exchanges [26] discusses the promise of a fair and transparent trading ecosystem with blockchain and more specifically with smart contracts. To achieve this, the paper studies the rise of arbitrage bots and how they exploit inefficiencies in decentralized exchanges.
Welcome to Flashbots - Flashbot Docs [27] is the documentation of the Flashbot technology and explains that it is a research and development organization, which was started to reduce the downsides that are created in stateful blockchains through MEV. As a first step, the technology focuses on Ethereum.
SoK: Preventing Transaction Reordering Manipulations in Decentralized Finance [18] discusses the issue of dependency of transaction reordering on the Ethereum blockchain. This results in attackers being able to profit from different approaches like front- and back-running transactions. The paper also aims to give a complete overview of current mitigation schemes.

9.4 Approaches

This section firstly focuses on flash loans in the context of arbitrage. Secondly, this section will showcase a variety of MEV attacks and types for arbitrage.

9.4.1 Leveraging Flash Loans for Arbitrage

A flash loan is a feature of DeFi, where any amount of available tokens can be borrowed without needing to put down any collateral. The only disadvantage is, that the borrowed assets have to be returned within the same block transaction [28]. If the borrowed assets are not repaid, the transaction becomes invalid and will be reversed. Due to this mechanism, there is very little risk for both sides. In the context of arbitrage, flash loans can allow an arbitrageur to profit from an opportunity without needing a lot of assets. This can give even retail traders the option to make good profits, as long as they can pay the gas fee needed to start the transaction. To demonstrate the impact of having more capital, the following situation can be considered. A trader sold one token to another trader for three tokens, resulting in a profit of two dollars. If the trader can obtain additional capital through flash loans, they can exchange 1000 tokens for 3000 tokens, resulting in a profit of 2000 tokens. This profit is much higher compared to the previous trade not using a flash loan. With flash loans, more capital can be obtained unlocking the possibility of a higher profit [29]. Figure 9.5 shows a real-life example of a flash loan. In this trade, the user took out a flash loan for 1000 ETH using the Aave Protocol v2, proceeded to profit from a cross-DEX Arbitrage opportunity and eventually repaid the 1000 ETH loan, resulting in a profit of approximately 45 ETH [30].

9.4.2 MEV Attacks and Types For Arbitrage

There are various MEV types employed to different degrees, such as front-running and back-running. In the field of crypto arbitrage, DEX arbitrage, and liquidations are often used in MEV attacks. In addition, a third type - sandwich attack - a combination of

Figure 9.5: Cross-DEX arbitrage with flash loan [30]

front- and back-running - is mentioned, which finds broader application in MEV, but is less commonly used in crypto arbitrage.

9.4.2.1 Cross-DEX Arbitrage

In DEX arbitrage, two platforms are offering the same token at a different price each. That means this token can be bought for cheaper on platform 1 and then be sold for more tokens on platform 2. This type of arbitrage is the most popular approach and thus also very competitive [5]. An example of such a profitable arbitrage trade is visible in figure 9.5 and visualized in 9.6, where a MEV searcher traded 1000 ETH into 1045 ETH utilizing a difference in the ETH/DAI pair on the platforms Uniswap and Sushiswap, resulting in a profit of 45 ETH [30].

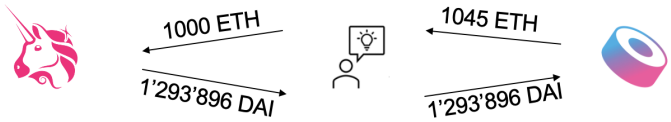

Figure 9.6: Diagram showcasing the trade from etherscan [30]

9.4.2.2 Liquidations

Similarly to traditional finance, some loans require collateral in DeFi as well. A certain amount of tokens must be deposited to obtain a loan in other tokens. On these type of loans, there's typically also an interest. Because the crypto market is rather volatile, there is a risk of the collateral sinking below the borrowed token value. If this exceeds a certain threshold, the platforms attempt to recover their borrowed funds by opening it up to liquidation. The liquidator can then buy the collateral cheaper than the market price, and pay back the loan with profit. This is very similar to margin calls in traditional finance. Since there are a large number of bots monitoring the mem-pools for such risk-free opportunities, it will normally lead to a bidding war for the execution of transactions, also called MEV auctions [31]. An example of how this could play out can be seen in figure 9.7.

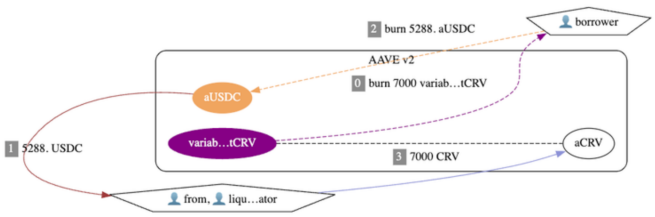

Figure 9.7: Example of a liquidation process [32]

9.4.2.3 Sandwich Arbitrage

Sandwich arbitrage is another type of MEV, where the attacker is using a special type of front-running to extract profit from a victim. The attacker is looking out for large swaps that might unbalance the pool. When an opportunity is found, the attacker wraps the transaction into two trades, whereas the first one is going in the same and the second one in the opposite direction. This then results in a more expensive transaction for the victim. The attacker acquires the assets at a lower price and can later sell them at a higher price. In figure 9.8, such a a trade can be seen, where the attacker made 0.23 ETH in profit [33].

Figure 9.8: Sandwich arbitrage trade on etherscan [33]

9.5 Comparison of Solutions and Tools

This section focuses on showing real tools that can be used for the approaches flash loans and MEV.

9.5.1 Flash Loan Creator Tools

In the table 9.1 three well-known flash loan creator tools [36] were collected and analysed. The chosen tools are Aave [1], dYdX [2], and Uniswap flash loans[3]. For each tool, a description, cost and risk are mentioned. Flash loans still need some technical and coding knowledge in most cases but some new tools are emerging that are making this easier [28]. In figure 9.9, it is showcased how a `SimpleFlashLoan` smart contract can be created using Aave V3 and Solidity. The function `fn_RequestFlashLoan` specifies the token that will be borrowed with the variable `assets` and the borrow amount with the variable `amount`. In the function `executeOperation`, the value for `totalAmount` must be calculated, as the execution of the smart contract needs to include the payment of the platform fee (premium) [39].

9.5.2 MEV Platforms

In table 9.2, three well-known MEV platforms/tools [40] were collected and analyzed. The chosen tools are Flashbots [4], Eden networks [5], and Manifold Finance [6]. For each tool, a description and risks are mentioned.
In the following the MEV auction is focused on in more detail using the architecture of the flashbots auction as an example. The flashbot auction aims to establish a private channel for Ethereum users and validators to communicate more efficiently about the

[1] `https://aave.com/`
[2] `https://dydx.exchange/`
[3] `https://uniswap.org/`
[4] `https://www.flashbots.net/`
[5] `https://www.edennetwork.io/`
[6] `https://www.manifoldfinance.com/`

Table 9.1: Table of flash loan creator tools

Name	Description	Cost and Risk
Aave	Aave is a decentralized market protocol where users can supply and borrow assets [34]. Flash loans is one of many functionalities that Aave has, but is a concept aimed at developers, meaning a good understanding of programming and evm is needed [35].	A fee of 0.05% has to be paid on flash loan creation [35].
dYdX	The dYdX is a platform aimed at advanced traders and the functionality of a flash loan is hidden in the system. That means it's not marketed as a flash loan, but it can be architected using the functionalities of the platform, making it 0% fees [36].	It is only possible to borrow Wrapped Ether (WETH) and not ETH directly and it is complex to create flash loan due to lack of documentation [36].
Uniswap flash loans	In the Uniswap platform there is the feature of Flashswap, which is the same as a flash loan. The output is transferred before the conditions are met and if the conditions are not met the transaction falls through [37].	With Uniswap V3 flexible fees were introduced, they can be 0.05%, 0.30%, or 1.00% based on their expected pair volatility [38].

```
function fn_RequestFlashLoan(address _token, uint256 _amount) public {
    address receiverAddress = address(this);
    address asset = _token;
    uint256 amount = _amount;
    bytes memory params = "";
    uint16 referralCode = 0;

    POOL.flashLoanSimple(
        receiverAddress,
        asset,
        amount,
        params,
        referralCode
    );
}
```

```
function  executeOperation(
    address asset,
    uint256 amount,
    uint256 premium,
    address initiator,
    bytes calldata params
)  external override returns (bool) {

    //Logic goes here

    uint256 totalAmount = amount + premium;
    IERC20(asset).approve(address(POOL), totalAmount);

    return true;
}
```

Figure 9.9: Code example for creating a flash loan with Aave V3

preferred order of transactions within a block. As it can be seen in figure 9.10, the flashbot auction architecture includes three components, the block builders, the relays, and the MEV-boost. The process begins with the searchers analyzing the memory pool for opportunities. Once an opportunity is identified, a block of transactions is formed by the block builders to exploit it. These bundles of transactions already include the validator payment and are then submitted to the flashbots relay server. The best block is selected from the various relay servers and sent to the MEV-Boost, where it is then forwarded to the validator. With this architecture, the transaction is sent to the validator without ever being exposed to the public memory pool. Conflicting transactions are resolved by awarding the transaction bundle with the highest miner payment, also known as auctions [47].

MEV Auctions are competitive, which leads to searchers paying significant amounts to the miners. Data shows that the searchers get around 63% of the MEV profits and the miners get 37% of the profit [48].

Table 9.2: Table of MEV tools and their properties

Name	Description	Cost and Risk
Flashbots	The Flashbot organization creates tools to reduce negative externalities, like network and chain congestion [41], from MEV. They focus on bringing transparency to the MEV activity, democratizing access, and enabling a sustainable distribution of the MEV revenue. Regarding MEV arbitrage Flashbot Auctions are an important tool [27].	The MEV-Boost tool carries certain risks, including MEV hiding, malicious relays, builder/relay collusion, and builder centralization [42]. No platform cost but possibly higher payment to validator needed to win the auction [43].
Eden Network	The Eden Network also focuses on reducing the negative externalities of MEV. On the other hand, the product also aims to maximize the value from the remaining opportunities. The Eden relay tools help with maximizing revenue [44].	Risk of uncle bandit attack [45] but no additional risk mentioned. Since it is similar to Flashbots it could hold similar risk. No platform fee mentioned.
Manifold Finance	Manifold Finance focuses on combining the Ethereum transactions in the best possible way to get the highest return on investment [46].	No risk or costs found.

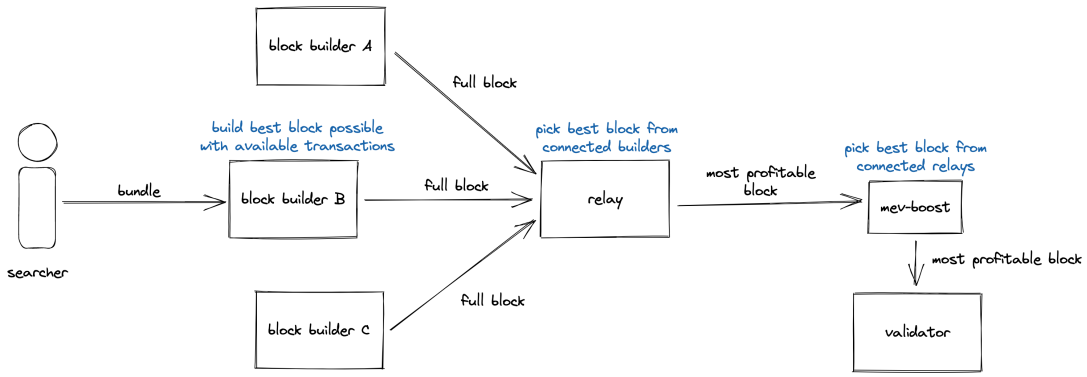

Figure 9.10: MEV Auction using Flashbots

9.6 Evaluations and Discussions

In reviewing the broader landscape of crypto arbitrage, there are several strategies that can be employed to leverage the available opportunities. Cross-Dex Arbitrage takes advantage of price discrepancies between two DEXes to make a profit. As this is a popular approach, it is also difficult to profit from these opportunities. Liquidations present another low-risk strategy, where liquidators purchase collateral at prices lower than the market value. Flash loans are often utilized in this approach, especially for buying collateral during liquidation events [49]. In many MEV strategies, such as Sandwich Arbitrage, there is typically a "victim" who misses out on potential profits. To counteract the negative externalities of MEV, tools like Flashbots have been created. Flashbots recently raised $60 million in a Series B round at a $1 billion valuation further underlines the importance of such tools in the blockchain ecosystem [50].
It has been demonstrated that it is possible to make a profit from crypto arbitrage, but the field has become increasingly competitive. In more competitive approaches such as MEV arbitrage, searchers often end up paying nearly 90% of the revenue to the validators in auction bids, reducing their profit margin significantly [5]. In this competition, naturally,

traders with more capital and more sophisticated tools and bots have an advantage, but can the retail traders still make a profit? Flash loans emerge as a potential equalizer in this scenario, allowing traders to leverage more capital without requiring collateral [51]. Providing retail traders with equal capital shifts the emphasis towards identifying arbitrage opportunities and developing an execution strategy. This requires a deep understanding of the market and programming skills to create a MEV bot.
MEV is often perceived negatively, but it can also have positive aspects. Bad MEV includes approaches such as front-running attacks or various reordering strategies. In these scenarios, other participants manipulate trades that are not optimized for their own profit, resulting in the user who initiated the transaction experiencing slippage and receiving a worse price. In contrast, good MEV involves acts like crypto arbitrage and encourages users to become validators [52]. However, distinguishing between good and bad MEV is not always straightforward. A notable instance occurred when a white hat MEV bot that front-ran an evil hacker, secured, and later returned the stolen funds to the Curve platform [53]. This situation raises a discussion on the ethics of MEV, questioning its moral standing in various circumstances.

9.6.1 Potential Further Research

The existence of flash loans empowers retail traders to implement more effective strategies. However, the question remains whether they are a silver bullet in levelling the playing field between retail traders and institutions? Acquiring further data about the profits earned by both parties may offer better understanding of how these profits are divided. On the topic of the negative MEV externalities, more research could benefit the ecosystem. The role of Flashbots as a potential solution to MEV attacks raises the question of whether other technologies might emerge in the future to address these challenges.

9.7 Summary and Conclusions

This work investigates crypto arbitrage by focusing on various MEV strategies, particularly covering flash loans and MEV attack types such as Cross-DEX arbitrage, liquidations, and sandwich arbitrage. Flash loans offer borrowing of a significant amount of assets without collateral, presenting a low-risk option that requires repayment within the same transaction. Cross-DEX arbitrage exploits price differences across different platforms, while liquidations involve the purchase of collateral at lower prices during market volatility.
The study reviews various MEV tools, such as Flashbots, Eden Network, and Manifold Finance, detailing their functionalities and risks. It also explores the components of the Flashbots architecture, including the Flashbots relay. Furthermore, the study analyzes flash loan creator tools like Aave, dYdX, and Uniswap, highlighting the costs in the form of fees, ranging from 0% on dydx to up to 1% on Uniswap [35; 36; 38].
The evaluation notes the strong competition in cryptocurrency arbitrage, leading to lower profits due to high fees paid to validators in auctions. According to the data, about 37% of the profits are allocated to validators, with the remaining 63% going to the searchers [48]. Flash loans are identified as a tool that potentially equalizes opportunities within the financial landscape.
Lastly, the document the document acknowledges both the positive and negative aspects of MEV. It highlights that malicious MEV attacks can lower trade profits, but also points out that MEV can be beneficial in redistributing liquidity between memory pools. Further research is suggested into flash loans being used to level the competitive landscape and mitigate the negative MEV externalities with Flashbots or other tools.

Bibliography

[1] Gogol K., Killer C., Schlosser M., Boeck T., Stiller B.:"SoK: Decentralized Finance (DeFi) - Fundamentals, Taxonomy and Risks", (2023). https://drive.google.com/file/d/14ec37LqN261XA5CeNmuNDzBnVs3YKE09/edit (accessed Oct. 09, 2023).

[2] F. Schaer, "Decentralized Finance: On Blockchain- and Smart Contract-based Financial Markets," *SSRN Electronic Journal*, 2020, doi: https://doi.org/10.2139/ssrn.3571335.

[3] "Market Overview," Eigenphi.io. https://eigenphi.io/ (accessed Dec. 14, 2023).

[4] "Maximal Extractable Value (MEV) | Chainlink," chain.link, May 24, 2023. https://chain.link/education-hub/maximal-extractable-value-mev (accessed Oct. 22, 2023).

[5] wackerow, "Miner extractable value (MEV)," Ethereum.org. Jun. 01, 2023. https://ethereum.org/en/developers/docs/mev/ (accessed Oct. 08, 2023).

[6] Wang, D., Wu, S., Lin, Z., Wu, L., Yuan, X., Zhou, Y., Wang, H. & Ren, K., "Towards A First Step to Understand Flash Loan and Its Applications in DeFi Ecosystem," *Proceedings of the Ninth International Workshop on Security in Blockchain and Cloud Computing,* May 2021, doi: https://doi.org/10.1145/3457977.3460301.

[7] T. Crepelliere, M. Pelster, and S. Zeisberger, "Arbitrage in the market for cryptocurrencies," *Journal of Financial Markets,* vol. 64, p. 100817, Jan. 2023, doi: https://doi.org/10.1016/j.finmar.2023.100817.

[8] "Cryptocurrency Market Size, Share & Growth Report, 2030," www.grandviewresearch.com, https://www.grandviewresearch.com/industry-analysis/cryptocurrency-market-report (accessed Oct. 28, 2023).

[9] "SEC.gov | SEC Charges Financial Services Professional and Associate in $47 Million Front-Running Scheme," SEC.gov, Dec. 14, 2022. https://www.sec.gov/news/press-release/2022-228.

[10] corwintines, "Intro to Ethereum," Ethereum.org, Apr. 12, 2023. https://ethereum.org/en/developers/docs/intro-to-ethereum/ (accessed Oct. 28, 2023).

[11] corwintines, "Blocks," Ethereum.org, Jul. 17, 2023. https://ethereum.org/en/developers/docs/blocks/ (accessed Oct. 28, 2023).

[12] mlibre, "Transactions," Ethereum.org, Jul. 07, 2023. https://ethereum.org/en/developers/docs/transactions/ (accessed Oct. 28, 2023).

[13] Zheng, Z., Xie, S., Dai, H., Chen, W., Chen, X., Weng, J. & Imran, M. "An overview on smart contracts: Challenges, advances and platforms," *Future Generation Computer Systems,* vol. 105, pp. 475 - 491, Apr. 2020, doi: https://doi.org/10.1016/j.future.2019.12.019.

[14] M. Kaur, M. Z. Khan, S. Gupta, A. Noorwali, C. Chakraborty and S. K. Pani, "MBCP: Performance Analysis of Large Scale Mainstream Blockchain Consensus Protocols," *IEEE Access,* vol. 9, pp. 80931-80944, 2021, doi: 10.1109/ACCESS.2021.3085187.

[15] "What Are Flash Loans?," chain.link, May 24, 2023. https://chain.link/education-hub/flash-loans (accessed Oct. 29, 2023).

[16] P. Mrig, "DeFi flash loans explained," MoonPay, Aug. 30, 2022. https://www.moonpay.com/learn/defi/defi-flash-loans (accessed Oct. 29, 2023).

[17] "Attacking the DeFi Ecosystem with Flash Loans for Fun and Profit," Hacking Distributed, Mar. 11, 2020. https://hackingdistributed.com/2020/03/11/flash-loans/ (accessed Dec. 14, 2023).

[18] L. Heimbach and R. Wattenhofer, "SoK: Preventing Transaction Reordering Manipulations in Decentralized Finance," *Proceedings Of The 4th ACM Conference On Advances In Financial Technologies,* 2022. http://dx.doi.org/10.1145/3558535.3559784

[19] karl, "MEV Auction: Auctioning transaction ordering rights as a solution to Miner Extractable Value," Ethereum Research, Jan. 15, 2020. https://ethresear.ch/t/mev-auction-auctioning-transaction-ordering-rights-as-a-solution-to_-miner-extractable-value/6788 (accessed Oct. 28, 2023).

[20] Zheng, Z., Xie, S., Dai, H., Chen, X. & Wang, H. "An Overview of Blockchain Technology: Architecture, Consensus, and Future Trends," *2017 IEEE International Congress On Big Data (BigData Congress)*, pp. 557-564 (2017)

[21] M. Xu, X. Chen, and G. Kou, "A systematic review of blockchain," *Financial Innovation*, vol. 5, no. 1, pp. 1-14, Jul. 2019, doi: https://doi.org/10.1186/s40854-019-0147-z.

[22] C. T. Nguyen, D. T. Hoang, D. N. Nguyen, D. Niyato, H. T. Nguyen, and E. Dutkiewicz, "Proof-of-Stake Consensus Mechanisms for Future Blockchain Networks: Fundamentals, Applications and Opportunities," *IEEE Access,* vol. 7, pp. 85727–85745, 2019, doi: https://doi.org/10.1109/access.2019.2925010.

[23] S. M. Werner, D. Perez, L. Gudgeon, A. Klages-Mundt, D. Harz, and W. J. Knottenbelt, "SoK: Decentralized Finance (DeFi)," *Proceedings Of The 4th ACM Conference On Advances In Financial Technologies*, pp. 30-46 , Sep. 2022. doi: https://doi.org/10.1145/3558535.3559780.

[24] D. A. Zetzsche, D. W. Arner, and R. P. Buckley, "Decentralized Finance," *Journal of Financial Regulation,* vol. 6, no. 2, pp. 172-203, Sep. 2020.

[25] Aramonte, W. Huang, and A. Schrimpf, "DeFi risks and the decentralisation illusion," Bis.org, Dec. 2021, Available: https://www.bis.org/publ/qtrpdf/r_qt2112b.htm?utm_source=pocket_mylist

[26] Daian, P., Goldfeder, S., Kell, T., Li, Y., Zhao, X., Bentov, I., Breidenbach, L. & Juels, "Flash Boys 2.0: Frontrunning, Transaction Reordering, and Consensus Instability in Decentralized Exchanges," *ArXiv Preprint ArXiv:1904.05234,* Apr. 10, 2019. https://arxiv.org/abs/1904.05234

[27] "Welcome to flashbots," Flashbots, Nov. 17, 2023. https://docs.flashbots.net/(accessed Dec. 16, 2023).

[28] "Flash Loans - FAQ," Aave.com, 2022. https://docs.aave.com/faq/flash-loans (accessed Oct. 02, 2023).

[29] FlashLoans.com, "Flash Loan Arbitrage A Very Powerful Tool," Medium, Feb. 06, 2022. https://flashloans.medium.com/flash-loan-arbitrage-a-very-powerful-tool-6664ef6b73 (accessed Oct. 09, 2023).

[30] "Ethereum Transaction Hash (Txhash) Details, " Etherscan. https://etherscan.io/tx/0x5e1657ef0e9be9bc72efefe59a2528d0d730d478cfc9e6cdd09af9f997bb3ef4 (accessed Nov. 01, 2023).

[31] N. Lenga, "Maximal Extractable Value: Concepts, issues and solutions," Zerocap, Feb. 27, 2023. https://zerocap.com/insights/research-lab/maximal-extractable-value/#liquidation (accessed Nov. 02, 2023).

[32] Khor. Win Win, "The Beginner's Guide to MEV," CoinGecko, Oct. 16, 2023. https://www.coingecko.com/research/publications/the-beginner-s-guide-to-mev (accessed Nov. 02, 2023).

[33] A. Zaidelson, "Dissecting MEV Arbitrage," VirtuSwap, Oct. 20, 2022. https://medium.com/virtuswap/dissecting-mev-arbitrage-fb8f9492cdf1 (accessed Oct. 09, 2023).

[34] "Introduction to Aave - FAQ, " Aave.com, 2021. https://docs.aave.com/faq/ (accessed Oct. 04, 2023).

[35] "Flash Loans - Developers," Aave.com, 2021. https://docs.aave.com/developers/guides/flash-loans (accessed Oct. 04, 2023).

[36] J. Klepatch, "Comparison betwen Flashloan providers: Aave vs dYdX vs Uniswap," defiprime.com, Jun. 13, 2020. https://defiprime.com/flahloans-comparison (accessed Oct. 03, 2023).

[37] "Getting Started | Uniswap," Uniswap.org. https://docs.uniswap.org/contracts/v3/guides/flash-integrations/inheritance-constructors (accessed Oct. 04, 2023).

[38] "Introducing Uniswap v3," Uniswap.org, Mar. 23, 2021. https://blog.uniswap.org/uniswap-v3#flexible-fees (accessed Oct. 04, 2023).

[39] S. Sen, "How to Make a Flash Loan using Aave | QuickNode," Quicknode, Aug. 18, 2023. https://www.quicknode.com/guides/defi/lending-protocols/how-to-make-a-flash-loan-using-aave (accessed Dec. 14, 2023).

[40] "List of 10 MEV Tools (2023)," Alchemy. https://www.alchemy.com/best/mev-tools (accessed Oct. 10, 2023).

[41] A. Obadia, "Flashbots: Frontrunning the MEV Crisis," Flashbots, Nov. 25, 2020. https://medium.com/flashbots/frontrunning-the-mev-crisis-40629a613752 (accessed Dec. 19, 2023).

[42] "MEV-Boost Risks and Considerations | Flashbots Docs," Flashbots, Nov. 17, 2023. https://docs.flashbots.net/flashbots-mev-boost/architecture-overview/risks (accessed Dec. 16, 2023).

[43] "Bundle Pricing | Flashbots Docs," Flashbots, Nov. 17, 2023. https://docs.flashbots.net/flashbots-auction/advanced/bundle-pricing (accessed Dec. 14, 2023).

[44] "Welcome to Eden Network - Eden Network," Edennetwork.io, 2021. https://docs.edennetwork.io/ (accessed Oct. 05, 2023).

[45] "Uncle Bandit Risk | Eden Docs," Edennetwork.io. https://docs.edennetwork.io/eden-rpc/more-information/uncle-bandits (accessed Dec. 05, 2023).

[46] "Manifold Finance - MEV Tools - Alchemy," Alchemy. https://www.alchemy.com/dapps/manifold-finance (accessed Oct. 04, 2023).

[47] "Overview | Flashbots Docs," Flashbots, Nov. 17, 2023. https://docs.flashbots.net/flashbots-auction/overview (accessed Dec. 14, 2023).

[48] "Flashbots", BitMEX Blog, May 06, 2022. https://blog.bitmex.com/flashbots/ (accessed Nov. 13, 2023).

[49] "A beginners guide to flash loans," Swissborg Academy, Jun. 22, 2022. https://academy.swissborg.com/en/learn/flash-loans-beginners-guide (accessed Nov. 13, 2023).

[50] R. Watson, "Flashbots becomes unicorn after completing $60 million raise," The Block, Jul. 25, 2023. https://www.theblock.co/post/241327/flashbots-becomes-unicorn-after-completing-60-million-raise (accessed Nov. 14, 2023).

[51] "Flash Loan, What Is A Flash Loan?" WallStreetMojo. https://www.wallstreetmojo.com/flash-loan/ (accessed Oct. 08, 2023).

[52] A. Allen, "What is MEV? Maximal Extractable Value explained," Matcha, Nov. 16, 2023. https://blog.matcha.xyz/article/what-is-mev (accessed Dec 16, 2023).

[53] V. Chawla, "MEV bot runner c0ffeebabe.eth returns $5.4 million amid Curve exploit," The Block, Jul. 31, 2023.https://www.theblock.co/post/242136/mev-bot-runner-c0ffeebabe-eth-returns-5-4-million-amid-curve-exploit (accessed Nov. 14, 2023).

Chapter 10

Federated Learning: A new AI Business Model

Tim Vorburger

With the rise of Machine Learning in the last years, new adaptations of the traditional cloud-based approach have become more and more popular. One of which is Federated Learning, which aims to tackle prevalent challenges in traditional ML such as data privacy concerns, limited communication resources and international as well as national regulations. Federated Learning can be classified into two categories: Centralized Federated Learning, and Decentralized Federated Learning. This report aims to give a fundamental overview over these two approaches, and tries to highlight important considerations from a business point of view, which have to be made before implementing such a solution. It will showcase several application scenarios, such as Healthcare, Smart Industry,Mobile Services, IoT Networks, and Cybersecurity and how FL is useful in these scenarios.

Contents

10.1 Introduction and Problem Statement

With Machine Learning profiting from the growing amount of data and general popularity on the topic it is vastly becoming a major part of modern businesses. With increasing hardware capabilities and the growing computing power of mobile edge devices the introduction of Federated Learning, a concept where in comparison to traditional Machine Learning, training of the model can happen on a multitude of devices, has risen as an alternative to traditional Machine Learning[1]. Using Federated Learning (FL), data can be kept at the source, i.e., devices that are gathering data now also do the computations, keeping the collected data local. Thus one of the major concerns of traditional Machine Learning which is the exposition of potentially sensitive data due to the need for a centralized data set, could be mitigated [2]. Whilst Centralized Federated Learning (CFL) certainly could overcome some of the privacy concerns of traditional ML, it still relies on a central server, coordinating the training process throughout the different edge nodes, thus the term 'centralized'. With an architecture relying on a central server the risks of a single point of failure arise, which is why in the following sections the potential of Decentralized Federated Learning (DFL) as an alternative to CFL will be investigated.

10.1.1 Federated Learning

As already mentioned, Federated Learning, established in 2016 [5], tackles the most present challenges in traditional cloud-based ML. It does so by ensuring that training data is kept locally on the devices sourcing data and by enabling collaborative machine learning of complex models across distributed devices[1]. From a networking viewpoint FL can be partitioned into two main classes, centralized FL and decentralized FL[3].

10.1.1.1 Centralized Federated Learning

In the last years CFL has become one of the most popular architectures used in FL. The main difference of this new approach in comparison to traditional cloud-based ML is, that no raw, unstructured training data is sent to the cloud where it is then centrally processed to update the model. In CFL the training of the model happens directly at the mobile devices, which then only transmit the updated model parameters to the central FL server which then aggregates data from all edge devices, updates the global model, and sends back the updated global model to each of the edge devices. The central server acts as a key component of the network, coordinating the aggregation as well as distributing the model updates to the clients, whilst keeping the training data private and secure[3].

10.1.1.2 Decentralized Federated Learning

Opposing the approach of CFL including a central server, coordinating training, and aggregating model parameters, DFL uses a network topology without a central coordinator. In DFL all clients can communicate with each other, for example through a peer-to-peer (P2P) connection. As shown in 10.2, training of the model still happens at each client using the local set of training data. After training their own model locally each client communicates the model updates through the P2P connection with its neighbours, rather than sending them to a central server. Next, a consensus mechanism is used to ensure that the participants of the network agree on a new updated global model[6][7].

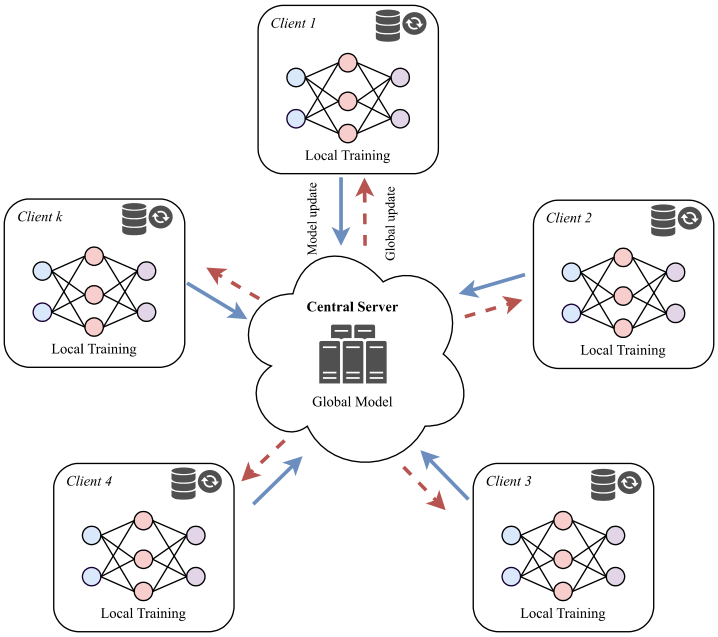

Figure 10.1: Possible Centralized Federated Learning architecture

10.1.2 Comparison between CFL and DFL

Comparing CFL and DFL exposes several key differences between both federated approaches. As of today CFL is the predominant approach used, but comes with some drawbacks which the decentralized approach tries to tackle[2][8]:

- *Robustness and single point of failure:* If a fully connected network topology is used in the DFL approach, each client part of the federation is interconnected with each other. With this approach, even if one or more clients are experiencing network issues, the rest of the nodes should still be able to communicate with each other, updating model parameters and global models, which in case of a failure of the central server in CFL would no longer be possible.

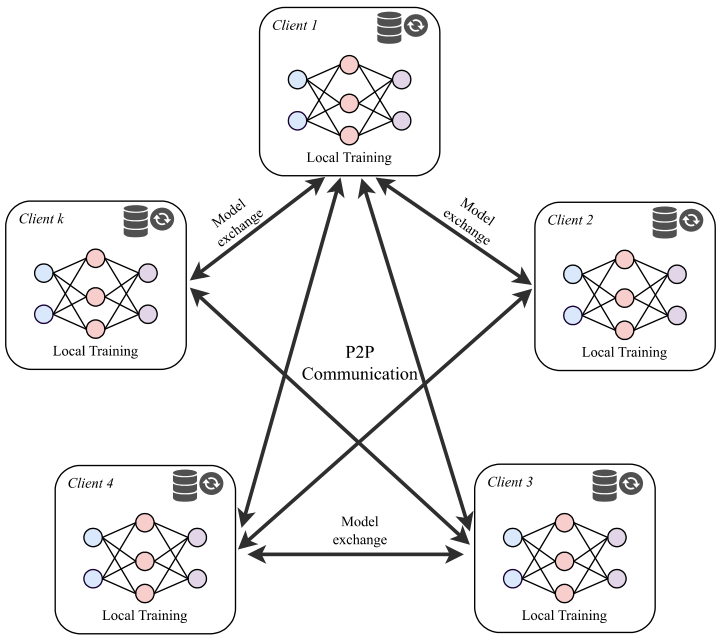

Figure 10.2: Possible Decentralized Federated Learning architecture

- *Trust distribution:* Trust in a decentralized system is distributed across the federation nodes, whereas the trust of the entire federation is the combination of the individual participants trust. The trustworthiness of a single node is determined by the historical performance, reputation, and past contributions to update the global model parameters. This distribution can minimize the risk of a single point of attack.

- *Performance, Network Bottleneck:* By spreading the workload amongst different nodes the risks of a network bottleneck or delays in the performance are minimized.

However, DFL approaches also introduce new challenges which ought to be addressed. Most prominent of which are the following[8]:

- *Communication Overhead:* The extent of communication overhead in DFL can vary depending on how model aggregation is distributed across the network, potentially leading to increased overhead in certain DFL network topologies[9].

- *Training Optimization:* Due to the decentralized nature, optimizing the training process in DFL faces several challenges. Without a central server, coordinating model updates and data aggregation whilst preserving data privacy calls for some sort of a consensus mechanism as well as aggregation algorithms like Federated Averaging (FedAvg)[10].

- *Trustworthy AI:* To ensure the quality of the model, DFL approaches should include client selection mechanisms and must ensure secure parameter sharing.

10.2 Related Work

Since Google introduced the concept of federated learning in 2016, the predominant approach has been CFL.However, in recent years, research on the DFL approach has experienced increasing research attention[8]. With some variants of ML being a part of innumerable business domains there are some domains for which FL is already in use due to its suitability. In toady's literature a lot of different use cases for FL are discussed, for example [11] suggests Healthcare, Transportation, Finance, and Natural Language Processing as main application scenarios for FL, whilst [3] examines the use of FL for IoT applications in Healthcare, Smart Transportation, Unmanned Areal Vehicles (UAV), Smart Transportation, Smart Cities as well as Smart Industry. With the arrival of new technology such as more elaborate IoT networks using 5G, possibilities of edge computing and thus interest in federated learning has risen. [20] focuses on securing such IoT networks, which are highly vulnerable due to the lack of proper security mechanisms on billions of IoT devices.
Whilst these papers focus on FL in general, the work of [8] concentrates specifically on DFL scenarios, giving an in depth overview of the current status quo and future trends sectioned into DFL applications in Healthcare, Manufacturing, Military, Mobile Services as well as for Vehicles. DFL aims to tackle some of the challenges associated with CFL and has the potential to replace the current state-of-the-art technology in certain business areas. In the following sections, the most promising application scenarios for FL will be analyzed and the potential economic benefits and risks will be highlighted.

10.3 Approaches

Before deciding to implement such a model, businesses should evaluate the impact provided by the new solution and should carefully calculate the possible economic benefit

of the investment, weighing up improved model performance, reduced data breach risks, a potential competitive advantage, and scalability of the system against the initial and ongoing costs (both of infrastructure as well as know-how), as well as compliance costs.
The success of a new model is tied to several key operations such as model convergence, aggregating model updates, consensus amongst nodes, and appropriate client selection. Each of these processes imposes a challenge in a decentralized environment. One of the primary issues with the convergence of the global model is that the data often is not Independent and Identically Distributed (IID) since the data sets of the participants are heterogeneous, causing local models to converge differently, which makes the convergence of the global model more difficult [1]. Moreover, the decentralized nature of DFL introduces latency and communication challenges. Since model updates are communicated and aggregated across a multitude of participants, often over geographical distances, there can be delays that affect the speed of the convergence of the global model. Additionally, the larger amount of data shared within each iteration can strain network resources, leading to increased operational costs. Advanced aggregation algorithms, ensuring the integrity and effectiveness of the aggregated model as well as decentralized consensus mechanisms add an additional layer of complexity to the system, often necessitate a considerable amount of investments in technologies and expertise. The lack of the central server in DFL and the consequential more complex coordination among participants, potentially demand more computational power of each one, which especially for smaller edge devices can impose a challenge.
One of the main advantages introduced with DFL in comparison to CFL is the fact that sensitive information is not centralized and thus the system has no single point of failure, which is in privacy concerned businesses, such as Healthcare and Finance, especially useful. The privacy oriented approach helps to comply with e.g., EU's General Data Protection Regulation (GDPR), a framework that governs how the personal data of individuals is processed and transferred.
In contrast, the centralization of data can pose greater risks in terms of compliance with GDPR. The transfer and central storage of data heighten the potential for large-scale data breaches and unauthorized access, thereby requiring additional measures to ensure compliance with GDPR's stringent data protection and privacy standards. From a business standpoint such a data breach, at the central server also imposes a huge financial risk, due to the potential loss of trust and reputation amongst clients.
Another thing, a business should consider when thinking about introducing a new ML model is the scalability of the system. DFL's architecture inherently supports scalability due to its distributed nature. In this paradigm, each node independently contributes to the model's training, processing data locally. This setup inherently avoids the computational bottlenecks associated with a single central server, as seen in CFL systems. As more nodes are added to a DFL system, the workload is naturally distributed, mitigating the risk of overloading any single point in the network. However, this decentralization brings its own challenges, particularly in terms of network communication and data synchronization. As the number of nodes increases, ensuring efficient communication between them without overwhelming the network becomes increasingly complex. Furthermore, the heterogeneity of data across diverse nodes necessitates sophisticated algorithms to aggregate these decentralized learnings into a cohesive global model, a process that grows more complex as the system scales.
Conversely, the centralized approach simplifies certain aspects of model management and update deployment. However, as the number of participating nodes increases, the central server can become a bottleneck, both in terms of computational capacity and network bandwidth. The scalability of CFL systems is thus inherently tied to the capacity of the central server, which can be costly and challenging to scale.

In terms of system resilience, DFL offers an advantage. The failure or unreliability of individual nodes has a more isolated impact in a DFL system, compared to CFL where the central server's failure can cripple the entire learning process. This decentralized resilience of DFL is particularly beneficial in large-scale applications where node variability and intermittent connectivity can be expected.
Businesses considering DFL must therefore carefully weigh these factors against the potential economic benefits and compliance advantages, such as alignment with GDPR, to make a well-informed decision. The choice between DFL and Centralized Federated Learning (CFL) hinges on a strategic evaluation of each model's scalability, operational costs, and the specific needs of the business, whilst also considering that developing a model from scratch requires technical expertise, to implement and operate, which could involve hiring new or training existing personnel, adding to development costs.

10.4 Solutions: FL as a Business Model

After outlining the most important considerations one has to make before implementing a FL model in this section specific business models and how they are applied are going to be highlighted. The section will be split into several different industries, for which a decentralized model might be suitable, namely: *Healthcare, Smart Industries, vehicles, mobile services, finance, and smart cities.*

- *Healthcare* The most important consideration for Machine Learning in Healthcare is the abundance of sensitive data. Rightfully all data linked to individual persons should be kept private and not be accessible to others. A decentralized approach thus aligns very well with the privacy oriented nature of the healthcare sector. There are several regulatory frameworks aiming to preserve data privacy, such as the already mentioned GDPR, or the European Health Data Space (EHDS), which research institutes as well as hospitals ought to adhere to. For efficient collaborations between these participants, a federated approach helps to preserve patients data private, by only sharing updated model parameters, keeping the sensitive data locally. This enables cooperation between different entities such as research institutes, federal agencies, and hospitals. This cooperation within the health sector can lead to enhanced accuracy of the models, due to the more diverse and larger amount of training data.

  There are several working implementations, ranging from disease detection to reducing communication costs as well as predicting mortality and hospital stay time. For example, the work [12] used the data of Electronic Health Records (EHR) from different hospitals, to implement a FL framework that predicts mortality rates and hospital stay time by clustering patients into groups based on their medical records. The work shows a way to efficiently orchestrate distributed data sources without the need to centralize data, and thereby preserving data privacy following regulations. [13] suggests a decentralized federated learning framework that can learn predictive models through peer-to-peer collaboration without raw data exchange to accurately predict heart-related hospitalizations before they even happen.

  Implementing such an approach allows hospitals to streamline patient management potentially leading to shorter stay times and improved health outcomes. From a business point of view, such an approach enables healthcare facilities to treat more patients and to reduce the cost associated with each patient.

  With the collaboration enabling characteristics of DFL, researchers have also looked at several different implementations that aim to make communications between participants of the federation more efficient. This helps to cut costs whilst also enabling

collaboration and preserving the privacy of data. For example [15] designed an innovative ring FL structure and Ring-Allreduce-based data sharing scheme to improve the communication efficiency in a robust and privacy-preserving decentralized deep federated learning (RPDFL) training scheme. RPDFL aims to improve standard FL methods model accuracy and convergence and represents a suitable approach for healthcare applications. Another work that investigates FL is [14], where a number of FL tools relying on a parameter server and fully decentralized paradigms driven by consensus methods are designed and tested. The models were used to detect brain tumor segmentation, which if done manually by radiologists is time consuming and error-prone. With the help of FL models, experts can be supported whilst also reducing idle time for evaluating potential treatments.

However, using DFL frameworks can not only facilitate efficient hospital management processes but can also be used to tackle the main downsides of a centralized approach such as communication bottlenecks, single point of failure, and single point of attack. In healthcare applications especially the latter stands out since the leaking of sensitive data should be prevented by any means and adhering to regulatory frameworks is imperative. Adhering to these regulations can be facilitated through DFL frameworks, whilst also enabling collaboration between clinics and research institutes, enhancing clinical research.

- *Smart Industry:* Industrial companies have seen a vast increase in technologies used within their production process. With the Industrial Internet of Things (IIoT) representing a collection of interconnected sensors, instruments, and other devices networked together, huge amounts of data are being collected. Machine Learning can help to use this data for a competitive advantage.

  Manufacturers also can benefit from collaborations using DFL, but the focus lies more on using Device-to-Device (D2D) collaboration than collaboration between different companies. Whilst in Healthcare a collaboration between different hospitals and research institutes across the globe is beneficial for all participants, as well as the patients, a scenario where two competing manufacturers collaborate to improve their earnings is highly unlikely since establishing a competitive advantage through the new technology will not be reached if all participants use the same ML models. Modern industrial systems rely on increased computational power and the level of autonomy of end devices, which enable a federated ML approach [16]. Implemented FL models can be used to analyze the vast amounts of gathered data in order to predict potential machine failures, analyze ongoing processes in real-time to ensure quality standards are met, optimize energy usage as well as improved cyberattack detection algorithms[17]. A DFL approach can leverage decentralization to ensure private communication amongst devices, the robustness of the model and streamline communication without the risk of a network bottleneck and can scale larger in comparison to CFL. However, again the challenges remain the same and need to be addressed when implementing such a model.

  Current developments of DFL solutions have shown promising results in improving communication efficiency amongst participating devices, whilst keeping confidential data private, as well as advanced cybersecurity solutions. [18] for example, suggests a quantization-based DFL (Q-DFL) mechanism in a D2D network that enables IIoT devices to process their real-time gathered data locally or collaboratively with neighbouring devices. Using simulations on the ModelNet dataset exposed, depending on the specific implementation different performance improvements in system time delay and system energy consumption, whilst ensuring data security and privacy. As mentioned above DFL also can be useful to detect and prevent cyberattacks,

as shown in [19], where a DFL method for anomaly detection in IoT networks is introduced.

With growing amounts of devices used in manufacturing and future technical improvements of devices as well as technological leaps in Network technologies, as expected with 6G, upcoming implementations of such DFL systems will most likely become more and more relevant. With the potential of cost savings, efficiency improvements, good scalability, and private and secure connections, DFL is well suited for implementations in smart industry systems.

- *Mobile services:* In the realm of Mobile services, and the growing number of interconnected devices, FL can be a way to offer increased efficiency and improved model performance of models in everyday life[8]. The localized data processing can be a way to enhance data privacy and reduce latency and bandwidth usage in large mobile edge networks[1]. A collaborative model can also be used to improve recommender systems and social networks, as described in [23], where a FL system, which should help users in daily activities, like finding a place to visit, a movie to watch, or products to consume, was improved using a decentralized asynchronous gossip based model aggregation. The work highlighted a model which converged faster and was more precise, without exposing private data of a user, e.g. location, past movie rating, or previous clicks.

- *IoT Devices:* With emerging technologies such as Beyond 5G (B5G) and the increasing amount of devices used in everyday scenarios, FL has the potential to enable faster, more efficient, and more secure collaborative learning in D2D networks.

  In [3], amongst other things, the usage of FL in the context of IoT networks is analyzed and investigates how it can be used for the optimization of IoT Data offloading and Caching, for the localization of devices, and for IoT crowd sensing. In the realm of localization, CFL can be utilized to enhance the accuracy of location based services. For example, IoT devices, like smartphones and wearable devices have the capability to collect and process data such as GPS signals, WiFi strength, and Bluetooth signals. By employing CFL these devices can securely share model updates with a server to improve location prediction algorithms while still ensuring individual location privacy. This approach respects user confidentiality while providing an improved localization model.

  Another promising application is the usage of DFL for large-scale IoT crowd sensing tasks, overcoming the network bottleneck at the central aggregator. With the increasing utilization of devices for monitoring, urban planning, and traffic management tasks that involve collecting various types of sensory data DFL frameworks offer a means for these devices to contribute to a global model that becomes more refined with additional data. This enhances the quality and reliability of crowd sensed information by leveraging the efforts of multiple devices in making real time adjustments to sensing models based on localized environmental changes.

  Regarding FL, for IoT data offloading and caching purposes this technology can effectively optimize network usage and data storage in networks. CFL can be used to create models that anticipate how data will be used and improve the transfer of data, from devices to edge servers or the cloud. This helps decrease network congestion and makes data transmission more efficient. Similarly, DFL enables real-time decisions on caching and retrieving data among devices, which results in latency and faster response times, for IoT applications.

- *Cybersecurity:* One of the most important use cases for FL which is applied across all discussed scenarios is in the context of Cybersecurity. It enables collaborative

training of models that can detect network intrusions, malicious software, or suspicious devices within the network while ensuring data privacy. Through FL clients can benefit from other participants data without exposing internal information, enabling rapid detection and response mechanisms against new and emerging threats. [20] for example, explored possibilities enabled by federated learning for malware detection in IoT devices. The work highlights how a larger and more diverse data set, enabled through a federated architecture has a significant impact on the models performance. The approach also considers the limited computational resources of IoT devices and thus proposes a centralized FL approach. It also investigates how adversarial attacks affect the model convergence and proposes countermeasures. In highly sensitive scenarios, such as Flying Ad-hoc Network (FANET) which is a decentralized communication network for unmanned aerial vehicles (UAV), security mechanisms are essential. [25] proposed a DFL network, enabling participants to collaboratively train models, to prevent jamming attacks.

FL can be a suitable way to enable Federated Cybersecurity (FC), helping to prevent, detect, and respond to various types of attacks, by leveraging distributed data sources without compromising data privacy. By using the collective insights of multiple clients FL enhances the overall performance and adaptability of cybersecurity systems, and represents a valid candidate across a variety of industries.

It is clear that FL can be applied in a multitude of different environments, even beyond the described use cases, such as Vehicular Networks, Finance, or Smart Cities. Further research will be able to provide even more suitable solutions across all industries and will try to optimize the mentioned current challenges in FL.

10.5 Summary

Based on the provided application scenarios it becomes clear that both CFL and DFL present approaches, with a lot of potential, which can be adapted to a lot of different usage scenarios and different needs in today's business environment. The suitability of using CFL or DFL depends on several key factors that organisations need to consider to fully leverage the potential delivered by federated learning.
When looking at the architecture of the federation, the number of participants plays a critical role in the choice between the approaches. CFL is often advantageous and efficient in a cross-silo federation, where there is a relatively number of nodes, but a large amount of data per node. Here the central parameter server can effectively manage model aggregation, without having a huge risk of a network bottleneck. On the other hand, DFL is more suited for cross-device federations, where a large number of devices, like IoT devices, contribute to the learning process, making central aggregation more difficult, due to the limited scalability. The computational capabilities of the nodes can also influence the choice between the approaches. CFL centralizes the complex parts of the learning process, leading to less network overhead reducing the computational requirements of end devices. However, with the increasing power of even very small devices, and more elaborate algorithms, DFL can also be a suitable option for networks with less powerful clients. The capabilities of the Network can also be a factor that influences the decision. In CFL nodes require a reliable and stable connection to the parameter server, otherwise, they can not contribute to the model and have no access to the global model. This makes DFL, which in general is more resilient to inconsistent network connections, a more suitable candidate for dynamic networks. Finally, the distribution of data across the nodes can significantly influence the decision between CFL and DFL. In scenarios where data is non-IID, DFL can provide better model performance in comparison to CFL, which typically is more appropriate in situations with more homogeneous data.

In conclusion, the decision between the approaches should be based on a careful assessment of the specific application scenario and the intended use. From a business point of view, both approaches provide a way to enable collaborations between different entities without exposing internal data, providing a way to protect intellectual property and adhere to regulations. It allows businesses to access diverse data sources, potentially improving the model performance, and recognizing and adapting to trends quickly. FL can also be a suitable way to implement Federated Cybersecurity mechanisms, enhancing current traditional ML approaches.
However, the reliance on other participants can also introduce new risks, such as nodes benefiting from the global model without contributing meaningful updates themselves thus a node has to trust other participants of the federation. Even though the privacy preserving nature of FL can help to mitigate some risks of data leakage, they are also vulnerable to Malware attacks, as well as adversarial attacks, which have to be considered when implementing a FL system and appropriate countermeasures should be implemented.

10.5.1 Outlook

Even though FL systems are already in use, further research on the field will provide even more elaborate mechanisms to tackle open challenges, such as scalability, trustworthiness, and security risks. FL frameworks have great potential in various scenarios and have rightfully raised interest in current research. The potential benefits from a business point of view are undeniable, but implementing such a solution calls for careful considerations in network architecture, data heterogeneity, and regulatory compliance. The need for interdisciplinary expertise is paramount, as FL is associated with various topics, related to machine learning. As businesses look to profit from FL, they must navigate these complexities, to implement a suitable solution, which is not only innovative but also practical.

Bibliography

[1] W. Y. B. Lim, N. C. Luong, D. T. Hoang, Y. Jiao, Y.-C. Liang, Q. Yang, D. Niyato, and C. Miao: Federated learning in mobile edge networks: A comprehensive survey; Journal Article (IEEE Communications Surveys & Tutorials, Vol. 22, No. 3), 2020, pp. 2031-2063.

[2] J. Konečnỳ, H. B. McMahan, F. X. Yu, P. Richtárik, A. T. Suresh, and D. Bacon: Federated learning: Strategies for improving communication efficiency; Journal Article (arXiv preprint arXiv:1610.05492), 2016.

[3] D. C. Nguyen, M. Ding, P. N. Pathirana, A. Seneviratne, J. Li, and H. V. Poor: Federated Learning for Internet of Things: A Comprehensive Survey; Journal Article (IEEE Communications Surveys & Tutorials, Vol. 23, No. 3), 2021, pp. 1622-1658, DOI: 10.1109/COMST.2021.3075439.

[4] Z. Lian, Q. Yang, W. Wang, Q. Zeng, M. Alazab, H. Zhao, and C. Su: DEEP-FEL: Decentralized, Efficient and Privacy-Enhanced Federated Edge Learning for Healthcare Cyber Physical Systems; Journal Article (IEEE Transactions on Network Science and Engineering, Vol. 9, No. 5), 2022, pp. 3558-3569, DOI: 10.1109/TNSE.2022.3175945.

[5] H. B. McMahan, E. Moore, D. Ramage, and B. A. Y. Arcas: Federated learning of deep networks using model averaging; Online Resource (arXiv preprint arXiv:1602.05629v1), 2016. Available: `https://arxiv.org/pdf/1602.05629v1`

[6] Y. Li, C. Chen, N. Liu, H. Huang, Z. Zheng and Q. Yan: A Blockchain-Based Decentralized Federated Learning Framework with Committee Consensus; Journal Article (IEEE Network, Vol. 35, No. 1), January/February 2021, pp. 234-241, DOI: 10.1109/MNET.011.2000263

[7] S. Savazzi, M. Nicoli, and V. Rampa: Federated learning with cooperating devices: A consensus approach for massive IoT networks; Journal Article (IEEE Internet Things J., Vol. 7, No. 5), May 2020, pp. 4641-4654, DOI: 10.1109/JIOT.2020.2978362.

[8] Enrique Tomás Martínez Beltrán, Mario Quiles Pérez, Pedro Miguel Sánchez Sánchez, Sergio López Bernal, Gérôme Bovet, Manuel Gil Pérez, Gregorio Martínez Pérez, Alberto Huertas Celdrán: Decentralized federated learning: Fundamentals, state of the art, frameworks, trends, and challenges; Journal Article (IEEE Communications Surveys & Tutorials), 2023, IEEE.

[9] Aurélien Bellet, Anne-Marie Kermarrec, Erick Lavoie: D-cliques: Compensating for data heterogeneity with topology in decentralized federated learning; In Proceedings of the 2022 41st International Symposium on Reliable Distributed Systems (SRDS), 2022, IEEE, pp. 1–11.

[10] Tian Li, Anit Kumar Sahu, Manzil Zaheer, Maziar Sanjabi, Ameet Talwalkar, Virginia Smith: Federated optimization in heterogeneous networks; Journal Article (Proceedings of Machine Learning and Systems, Vol. 2), 2020, pp. 429–450.

[11] Priyanka Mary Mammen: Federated Learning: Opportunities and Challenges; eprint arXiv:2101.05428, 2021.

[12] L. Huang, A. L. Shea, H. Qian, A. Masurkar, H. Deng, and D. Liu: Patient clustering improves efficiency of federated machine learning to predict mortality and hospital stay time using distributed electronic medical records; Journal Article (Journal of Biomedical Informatics, Vol. 99), 2019, Page 103291, Publisher: Elsevier

[13] T. S. Brisimi, R. Chen, T. Mela, A. Olshevsky, I. Ch. Paschalidis, and W. Shi: Federated learning of predictive models from federated electronic health records; Journal Article (International Journal of Medical Informatics, Vol. 112), 2018, Pages 59-67, Publisher: Elsevier

[14] B. C. Tedeschini, S. Savazzi, R. Stoklasa, L. Barbieri, I. Stathopoulos, M. Nicoli, and L. Serio: Decentralized federated learning for healthcare networks: A case study on tumor segmentation; Journal Article (IEEE Access, Vol. 10), 2022, Pages 8693-8708, Publisher: IEEE

[15] Y. Tian, S. Wang, J. Xiong, R. Bi, Z. Zhou, and M. Z. A. Bhuiyan: Robust and privacy-preserving decentralized deep federated learning training: Focusing on digital healthcare applications; Journal Article (IEEE/ACM Transactions on Computational Biology and Bioinformatics

[16] S. Savazzi, M. Nicoli, M. Bennis, S. Kianoush, and L. Barbieri: Opportunities of Federated Learning in Connected, Cooperative, and Automated Industrial Systems; Journal Article (IEEE Communications Magazine, Vol. 59, No. 2), 2021, Pages 16-21, DOI: 10.1109/MCOM.001.2000200

[17] D. C. Nguyen, M. Ding, P. N. Pathirana, A. Seneviratne, J. Li, D. Niyato, and H. V. Poor: Federated Learning for Industrial Internet of Things in Future Industries; Journal Article (IEEE Wireless Communications, Vol. 28, No. 6), 2021, Pages 192-199, DOI: 10.1109/MWC.001.2100102

[18] T. Ma, H. Wang, and C. Li: Quantized Distributed Federated Learning for Industrial Internet of Things; Journal Article (IEEE Internet of Things Journal), 2021, Publisher: IEEE

[19] Z. Lian and C. Su: Decentralized Federated Learning for Internet of Things Anomaly Detection; In Proceedings of the 2022 ACM on Asia Conference on Computer and Communications Security, 2022, Pages 1249-1251

[20] V. Rey, P. M. Sánchez, A. Huertas Celdrán, and G. Bovet: Federated learning for malware detection in IoT devices; Computer Networks, Volume 204, 2022, Page 108693, Elsevier

[21] B. Ghimire and D. B. Rawat: Recent Advances on Federated Learning for Cybersecurity and Cybersecurity for Federated Learning for Internet of Things; IEEE Internet of Things Journal, Volume 9, No. 11, June 1, 2022, Pages 8229-8249, DOI: 10.1109/JIOT.2022.3150363

[22] V. Gugueoth, S. Safavat, and S. Shetty: Security of Internet of Things (IoT) using federated learning and deep learning-Recent advancements, issues and prospects; ICT Express, 2023, Elsevier

[23] Y. Belal, A. Bellet, S. B. Mokhtar, and V. Nitu: Pepper: Empowering user-centric recommender systems over gossip learning; Proceedings of the ACM on Interactive, Mobile, Wearable and Ubiquitous Technologies, Volume 6, No. 3, 2022, Pages 1-27, ACM New York, NY, USA

[24] Y. Belal, S. B. Mokhtar, M. Maouche, and A. Simonet-Boulogne: Community Detection Attack against Collaborative Learning-based Recommender Systems; arXiv preprint arXiv:2306.08929, 2023

[25] N. I. Mowla, N. H. Tran, I. Doh, and K. Chae: Federated Learning-Based Cognitive Detection of Jamming Attack in Flying Ad-Hoc Network; IEEE Access, Volume 8, 2020, Pages 4338-4350