The Emerging World of Decentralized Finance

Silviu OJOG
Bucharest University of Economic Studies, Romania
silviu.ojog@csie.ase.ro

Decentralized finance (DeFi) is the term used to describe financial applications and services built on blockchain, the technology behind cryptocurrencies. DeFi uses blockchain as a trust mechanism, enabling unknown parties to transact with each other, removing unnecessary intermediaries, and lowering transaction costs. In order to seize the potential of blockchain technology in this particular industry and how it can be translated into other niches, it is necessary to understand its mechanics, implications, and particularities. This paper aims to present the operating principles, technologies, and security implications related to blockchain-based decentralized finance.

***Keywords**: Blockchain, Security, Decentralized Finance, DeFi, Smart Contracts, Fungible/Non-Fungible Token, Protocol, Exchange, Loan*
DOI: 10.24818/issn14531305/25.4.2021.05

Introduction

Traditional finance as it is known today has considerable drawbacks. The most noticeable is the lack of transparency, interoperability, customer access restrictions, and centralized control. The centralized control pitfalls have become more obvious for the general public, with the rise of tech giants, who have been accused of tampering with user data. Centralized control in countries with authoritarian regimes is seen as the economic burden is imposed on the citizens.

The banking system is generally inefficient in regards to high transfer fees for wire transfer, card purchases, and long processing time frames. The bank often imposes access restrictions to lines of credit for entrepreneurs.

Financial technologies or FinTech in short was the first major wave of disruption on traditional financial services. PayPal was one of the pioneers in the space, founded in the 2000s. Upon its creation, its purpose was to speed up transactions. Other banking initiatives have followed. Nevertheless, the banking system is built around profits from high transaction fees, which made it counterintuitive to invest in FinTech projects.

The first window of opportunity for financial technologies came after the 2008 financial crash. Governments started putting in place mechanisms for securing the economy. In 2015, the EU Commission put in place a new direction for Payment service. It involves opening up the bank APIs for smaller market players. Companies such as Revolut or TransferWise created complex services for regular people, services that were available only for high-end customers.

The Cryptocurrencies

Blockchain has emerged as a peer-to-peer way of transacting value over the internet. The most common form of value is money, in the form of fiat currencies. Fiat currencies are issued and controlled by the government. The government can choose to “create” more money, by printing more, which may cause inflation problems. Bitcoin the first blockchain-based cryptocurrency has emerged as an alternative to transacting money.

Cryptocurrencies are tokenized assets that represent value. Nevertheless, not all assets are created equal. In terms of how they are built, cryptocurrencies can have their own blockchain, as is the case of Bitcoin, they can be built on other blockchains, or they may live and be used on different blockchains. Every cryptocurrency has a purpose and value.

Tokenomics represents token economics. Tokenomics is defined by a series of indicators, the most important being the value of the token, the total market capitalization, and the total token supply.

The total supply is important for long-term investment. Some of them have a limited supply, for example, Bitcoin with 21 million tokens, and some of them have an unlimited supply, Ethereum. Bitcoin does not have all his 21 million in circulation. Bitcoins are minted and given as rewards to miners when they manage to create a block. The total supply is set to expire in 2140 [2]. For Ethereum, a lack of maximum supply, means that new tokens can be minted and can still be minted indefinitely, similarly to fiat currencies. Nevertheless, the circulating supply is always limited, at any given moment. The circulating supply represents the number of tokens available at the moment. The total supply of a cryptocurrency can be adjusted by creating new coins or deleting new coins. The processes are called minting and respectively burning coins.

In terms of its creation purpose, some of the cryptocurrencies are focused on being purely a currency. Such currencies are Bitcoin, Dash, Litecoin, or Stablecoins. These currencies use blockchain as an immutable ledger of transactions. They were created purely for transacting. With time, the transaction utility has changed gradually, especially for Bitcoin. The maximum number of transactions that can take place on Bitcoin is significantly lower than in traditional financial industries, with card processors such as Visa or Mastercard. Due to its economics, Bitcoin is seen as a store of value, or, in other words, a successor for gold. People and institutions invest in Bitcoin the same way they invest in gold because their value is set to increase over time.

Stablecoins are a special kind of cryptocurrency that aims to mimic a real-life fiat currency. Their values are derived from that of a specific fiat, most commonly USD. Stablecoins are backed up by other assets and they too can be created differently. The most used are fiat-backed stable coins, in a 1 to 1 ratio. The most used stable coin is Tether, USDT. A new USDT is minted after a traditional FIAT USD has been stored in the vault. Every time a Fiat USD leaves the vault, a corresponding USDT is burnt. DAI is another popular stablecoin with a different form of backup, using crypto-collateralization. For every DAI minted, high-value crypto such as Ether is stored. Due to the high volatility of cryptocurrencies, a larger portion of Ether must be supplied to create an overcollateralized ratio. The ratio should protect the minter from drops in the price of the collateralized asset.

Every major trading platform has its own stablecoin such BUSD for Binance, USDC for crypto.com, or TUSD. Stablecoins are usually the “gateway” into the crypto market.

Currencies have evolved from pure currency tokens to protocol tokens, exchange tokens, DeFi Tokens, utility tokens, privacy tokens, stock tokens or NFTs.

Exchange tokens are tokens created by big centralized exchanges such as Binance, Crypto.com, Kucoin. They use their tokens as an incentive for the token holders in order to get better trading fees, rewards. Binance is the biggest exchange in the world. Apart from the crypto exchange, they built their own blockchain, a fork of Ethereum, it is called the Binance Smart Chain.

Stock tokens are used to trade real stock using cryptocurrencies. The value of a stock token is bound to the value of real stock. Their values rise and drop whenever the real stock rises or drops. It is important to note that stock tokens are derivatives instruments and they do not represent a real share in the company as a stock would.

Utility tokens. One of the most known utility projects is the Basic Attention Token. BAT in short, is used by the creators of the Brave browser to encourage users to watch paid advertising and to pay content creators that are willing to serve users advertising on their content.

DeFi tokens are tokens of decentralized finance projects. They can be used for governance. The community of token holders can vote on development proposals. The elected proposals are then further developed and maintained by the Foundation company. Unlike traditional companies, the foundations are companies in charge with development of the product, but they cannot choose what they are building. The thinking behind this decision is to remove any conflict of interest. Otherwise the company in charge could influence the direction of the product and thus they can easily influence the price of the crypto asset.

Privacy tokens are a special kind of currency tokens. They are used for private trading, in the sense that they obfuscate transactions, namely the sender, receiver and the amount sent in the transaction. Some of them have built in privacy features like Monero or ZCash. Other cryptocurrencies such as Dash or Bitcoin can provide privacy features, but only integrated with a different service.

NFTs or non-fungible tokens are used to represent and certify the ownership of a digital asset.

The blockchain ecosystem, like any other, is still loaded with scam coins that do not have much usefulness behind them. They are highly volatile, that is why they are attractive to trades, especially entry level traders and day traders.

As the blockchain technology matures, more and more utility will be incorporated. New categories of tokens may emerge to serve different needs. While tokens can have different use purposes, they can be used for trading.

DeFi Foundation

DeFi is the acronym for Decentralized Finance and it represents a new paradigm for the financial industry. Traditionally, financial transactions took place through an intermediary, such as a bank, broker, exchange, or other financial institution.

The rise of blockchains as decentralized ledger technologies has enabled people to transact in a decentralized manner. Blockchains use cryptography, a shared distributed append-only ledger, and a consensus mechanism to verify and validate transactions. Transactions are validated in order to cope with a problem with double-spending problem. In real life, a person cannot spend the same amount of money twice, unless it is involved in criminal activities. On the internet, copying an asset and distributing it multiple times is fairly easy. Since transactions are assets, they must fall under a procedure of recording and verifying them.

In blockchains, cryptography is used to sign transactions, and verify the identity of the traders. The transactions are stored in a shared ledger distributed across multiple nodes over the internet. The ledger is composed of blocks of transactions that are linked between each in a continuous manner. The distributed nature of the ledger and the linkage between its blocks makes the changes of its content extremely hard to implement. The process of altering is rather unfeasible than impossible. Immutability over time enables traceability and transparency of transactions. The blockchain consensus mechanism assures no one is able to shortcut the system and take undue benefits.

Additionally, some blockchains implement smart contracts. A digital smart contract is an immutable software deployed on the blockchain. Smart contracts enable sharing of assets in a peer-to-peer, fully-transparent way, without the need for a central authority or a middleman.

Blockchains can and do act as an arbitrator between individuals, thus replacing banks as trusted central authorities. Since blockchains are not run nor controlled by a single, the incentives of

The most used platform for smart contracts is Ethereum, the second-largest blockchain by market capitalization, after Bitcoin. Ethereum has emerged in the footsteps of Bitcoin, as a way of providing business logic on blockchain. Ethereum deployment systems allow Turing-complete code deployment.

In 2020, the blockchain scene saw massive growth from projects such as Uniswap, Compound, Aave, or 1Inch. So far, the most prominent problems for DeFi are the transaction fees and possible exploitation of the smart contracts.

Decentralized Finance represents a small fraction of the traditional centralized finance market, but the premise has a high probability of changing in the future, linked to the blockchain adoption growth. The user experience of DeFi is needy.

Custody

Blockchains use private-key public-key infrastructure to prove ownership over stored assets. A private key is a long random number, used to sign transactions. A public key is also a number derived mathematically from the private key.

Traditions business models are built on

centralized entities which act as central authorities with mediating power. The decentralization paradigm of blockchain shifts the business focus from a central entity to numerous participating entities. The security risks shift themselves.

In a blockchain, the person who controls the keys controls the funds. He can initiate transactions, move funds and drain accounts. Therefore, for the average user, blockchain introduces a new burden: private keys management. Losing custody of private keys is equal to losing control over the assets. The risk is equally high for private companies transacting on the blockchain as for retail users.

In order to mitigate some of the risks, and improve the user experience, 3rd party centralized exchanges offer their customers custodial wallets. The keys to these custodial wallets are held and managed by these 3rd party entities. Users can access and move their funds after being subject to standard financial authentication procedures. While user experience-wise, the approach saves people from the overhead of managing their own keys, it may impose custodial risks. Exchanges are subject to attacks and theft of private keys. Exchanges keep the majority of funds in cold storage, while the rest is used for active daily trading.

Risk mitigation in custodial exchanges is approached from different. Crypto.com and Coinbase two of the leading crypto exchanges are insured and thus sharing the risk with the insuring company.

The risk of key management can be spread between an owner of the funds and a 3rd party provider using a shared custody approach. BitGo offers a multi-part key solution. For every user, 3 keys are generated. The user generates, holds, and stores 2 out of 3 keys. The first is used for active transactions and the other is generated and stored only offline as a backup. The key BitGo company holds the 3rd key to co-sign all the transactions. 2 out of the 3 keys are needed to sign transactions and move funds. In case any of the 3 keys are lost, the other two can be used to access funds.

Delegating custody in DeFi can come with less obvious financial losses. Protocols often offer financial incentives to their token holders. They may choose to reward them with parts of the profit, similar to dividend distribution in public listed companies. The funds come in the form of airdrops. The custodian may not support a certain airdrop or may impose restrictions on receiving funds for certain users based on their geographical location.

In short, decentralized finance uses the same instruments as traditional finance, and replaces the middlemen and central authorities with smart contracts.

In reality, DeFi products and services are not totally decentralized. The companies that build them are not decentralized and other components of the service are not centralized. The front end of a DeFi application is not decentralized as internet access requires a Domain Name Service (DNS). For the moment, no decentralized DNS service exists.

The Mechanism

The enabler of the DeFi is the smart contract. A digital smart contract is a piece of code that leaves on the blockchain and enables you to share anything of value in a peer-to-peer, fully-transparent way, without the need of a central authority or a middleman. In traditional finance, banks, brokers, or other financial institutions act as an escrow. All these 3rd parties inquire about operational costs which translate into high transaction fees.

A smart contract can be programmed to act as an escrow. Smart contracts can receive funds and can redistribute funds, namely digital assets. They also have the possibility to reverse a transaction if a certain deadline is not met or a certain threshold is not achieved. Every transaction based on a smart contract is recorded in the blockchain. The immutable character eliminates any possible disputes.

Smart contracts are not an entirely new concept. The term has been coined by Nick Szabo, in the ‘90s [6]. Nick Szabo is a known figure in the blockchain space. Prior to the existence of Bitcoin, he designed the “bit gold”, another digital currency.

Smart contracts can be used to create new tokens on the blockchain. 2021 has brought another major use case for the blockchain industry: storying NFTs on the blockchain. NFTs stand for non-fungible tokens and represent a particular class of tokens, especially used in the arts and collectibles industry. Non-fungible items cannot be interchanged or divided into smaller units, unlike a more traditional cryptocurrency. Consider a piece of art, such as a painting or a sculpture. Its value increases with scarcity. Neither can one break a piece of art into smaller pieces nor can one replace its parts without decreasing its value. NFTs exist to symbolize ownership or usage rights over something of value. NFTs can be sold and bought. NFTs are particular important for the DeFi space as the NFT owners can use them as collateral for DeFi operations. NFTs can take the form of any other digital file. The ownership representation can be extended from digital art to real world assets such as property title, bonds or any other physical asset.

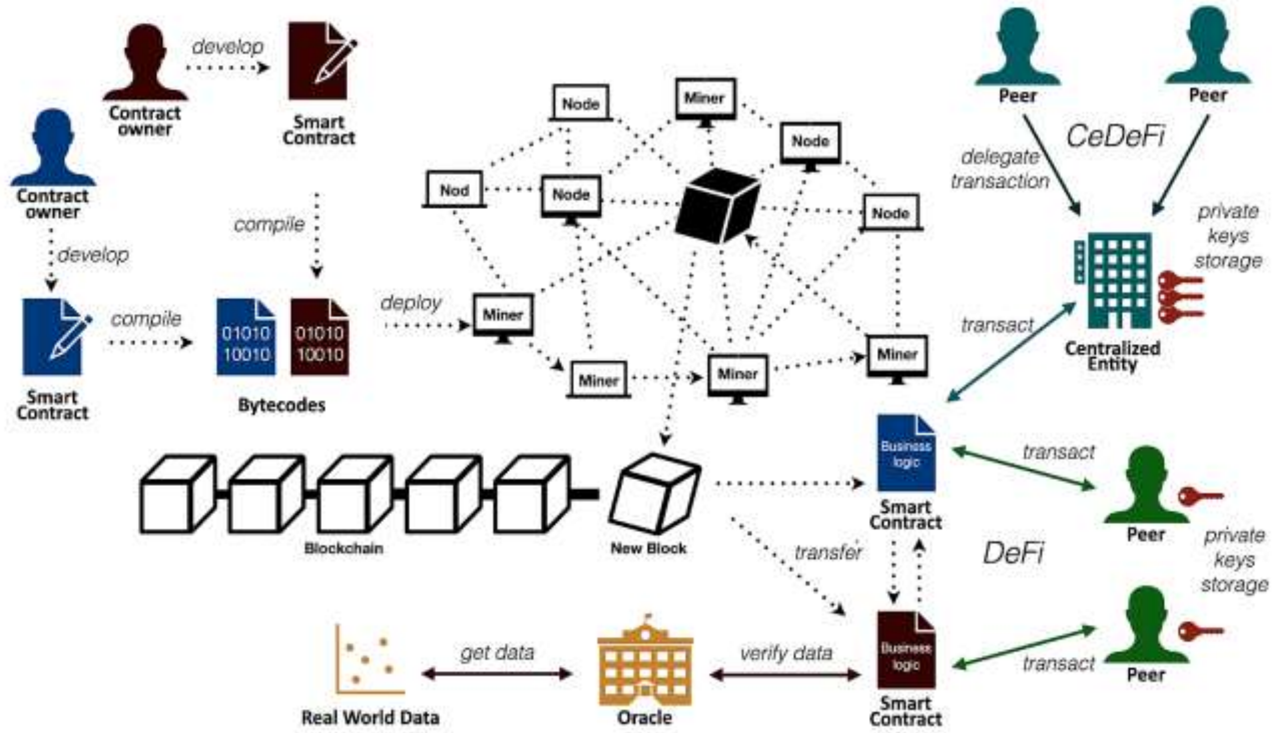

Fig. 1. Decentralized Finance Architecture

Ethereum has issued ERC standards for the creation and interaction of the tokens. The ERC stands for Ethereum Request for Comments. Every token is created through a smart contract. Standards are a set of common rules the smart contracts have to follow in order to be traded. The ERC20 - is used for fungible tokens like Uniswap. The ERC-721 standard is used for non-fungible tokens, such as digital art, gaming or tickets. The ERC1155 is used for non-fungible, fungible, semi-fungible, and tokens all in one contract. The latter was created to solve the problem of many similar tokens, slightly similar, which need to be transacted in bulk.

On blockchains with smart contract capabilities such as Ethereum or Cardano, there are two types of addresses: a standard user address and a smart contract address. A user address is also known as an externally owned address can only receive tokens while a smart contract address can receive both tokens and data.

Smart contracts reside permanently on the blockchain. They are deployed on the blockchain by a smart contract owner. The owner handles the development of its business logic, compiles the smart contract into bytecode and deploys it on the blockchain. After the contract is being registered into the blockchain, the smart contract can be used for transactions.

A blockchain transaction occurs when tokens or data is moved any two addresses. When a transaction is sent to a particular smart contract, it can be forwarded to multiple other accounts.

Users can interact directly with a smart contract through an externally owned account in a truly decentralized manner or they can delegate the interaction to a centralized entity such as an exchange which will interact with the blockchain on their behave. The latter approach is also known as Centralized Decentralized Finance or CeDeFi, namely working in the decentralized ecosystem in a centralized manner.

Smart contracts act very much like escrow contracts. In real life contracts are enforced by authorities. In a similar way, a smart contract is enforced by 3rd party oracles. Oracles are specialized 3rd party entities that provide accurate data to the contract. The smart contract participants trust oracles for their data accuracy.

DeFi Advantages

A large portion of the world population does not have access to the banking system and services. Moreover, in theory, a larger pool of people is set to have access to DeFi services than to traditional ones.

DeFi is positioned as the next-generation FinTech. Nevertheless, there are key differences between DeFi and FinTech. Firstly, the DeFi implementation is a piece of software, namely a smart contract, that runs on the blockchain. There is no censorship. DeFi does not require KYC (know your customer) processes, credit score, geographical location, or special approval to participate. Secondly, in DeFi, the users are in total control of their assets. The users own their private keys.

The leading platform for DeFi projects is Ethereum. There are four main categories of DeFi [2]: crypto loans, decentralized exchanges (dexes), derivatives, and payments.

Derivatives are complex financial assets, whose value is derived from a different asset. In traditional finance, the access to buying different assets is limited by factors such as: geographical location, available funds. The most common derivatives are options and futures.

DeFi Loans

The most common use case revolves around peer-to-peer loans [11]. In traditional finance, credit loans are the most important financial mechanism. It is one of the building blocks of the economy. Nevertheless, DeFi loans differ from traditional loans, due to the parties involved. They are rather similar to pawn loans. DeFi loans need to be paid sooner than bank loans. People are incentivized to lend if they receive high-interest rates and if they receive sooner the payout.

People are incentivized to borrow if they have access easier than with a traditional banking system, without a credit score. If those criteria are met, the borrowers are willing to pay high-interest rates. Considering those aspects, the DeFi loans are more similar to a pawn transaction. Such a transaction is achieved between a borrower and lender. The borrower must supply collateral, usually in the form of an expensive good. The input of collateral prevents the borrower from failing to fulfill its obligation to repay the loan. The borrower is given a deadline to repay the debt, otherwise, he loses the collateral. The collateral of a DeFi loan is another cryptocurrency. The value of the collateral should be larger than the borrowed amount, namely 115% from the borrowed amount [11].

While counterintuitive, the reason is simple: the borrower can use the money without having to sell his portfolio.

The prices of crypto-currencies are notoriously volatile, thus selling and rebuying it later may result in huge price differences and losses for the buyer. In the pawn loan case, usually, the borrowed amount is less than the price of the collateral. In a 1:1 ratio between collateral the borrowed amount, the lender bears the risk of collateral dropping below the amount of the credit and the borrower not having an incentive to repay debt. The loan must be overcollateralized in a ratio that both protects the borrower and the lender. On the other hand, if the price of the collateral drops before repaying the loan, his position can be liquidated.

Unlike traditional finance, anyone can liquidate the position. The liquidator will send 100% of the borrowed asset and the lender fee, in exchange he will get the rest of the collateral. The more volatile the collateral is, the bigger ratio is required to mitigate the borrower risk. The liquidators act as protocol guardians.

The biggest lending and borrowing platforms are Aave, Maker, Compound, dYdX, and Uniswap.

Decentralized Exchanges

A centralized exchange like Binance or Crypto.com is a traditional company providing exchange services and liquidity for users to trade. Centralized crypto exchanges work slightly differently from traditional currency exchanges, in the sense that they match buyer and seller orders, while traditional fiat exchanges are trading directly on a per-user basis.

A decentralized exchange, with the acronym dex, is a smart contract on the blockchain. It is not run by a centralized operator. Generally, decentralized exchanges have lower trading fees.

On dexes, users are in full control of their crypto assets, while in traditional exchanges, the assets are "held" in custody by the exchange, until withdrawal. Centralized exchanges usually provide better user experiences, as they lower the friction between the user and the technology. Nevertheless, centralized exchanges may impose withdrawal limits.

Dexes are created on a per blockchain basis. For example, Uniswap is a decentralized exchange for Ethereum, and it is only used to swap Ethereum based tokens. Each blockchain can have more than one dex. Dexes are open source projects, their code being available for auditing and forking on Github. Ethereum [3] has Uniswap, 1Inch, SushiSwap, Binance Smart Chain [4] has PancakeSwap, BurgerSwap, Cardano has Cardax and Polkadot [5] has Polkadex.

In a dex, crypto assets are "swapped", not "traded". Swapping means using an existing liquidity pool, to change a certain token for another one. The liquidity pool is a pool of assets, and it must contain the two tokens that need to be swapped. In a traditional exchange, the exchanges match together the buyer asking for a certain asset and the seller offering that asset. Liquidity pools are created with the sole purpose of collecting trading fees. Anyone can provide assets, namely cryptocurrencies, to certain trading pools, in order to collect transaction fees.

Decentralized exchanges are harder to work with from a UX perspective. It requires working directly with crypto assets. For dexes, users need to set up a wallet, in order to perform swap operations. Dexes do not offer customer services or advanced charts and analytics.

The low trading fees and access to small coins, unavailable to large crypto trading platforms are the main advantages of dex. Moreover, they can offer staking options for certain coins, in order to earn rewards.

On the other hand, dexes pose security risks. So far, they are not regulated, and potential hacks on the system can lead to permanent loss of money. They offer less insurance.

DeFi Risks

The story of the MAKER DAO hack (Decentralized Autonomous Organization) teaches the blockchain community an important lesson. Effective blockchain governance requires both on chain and off chain governance mechanisms. The DAO was in essence a decentralized investment fund built on the Ethereum network by a startup called Slock.it. Token holders would get a share of the DAO's holdings. Anyone who disagreed with the funding decision could trigger a split function, moving their funds into a new child DAO. There turned out to be an even more serious flaw in the DAO code, and ultimately, it would lead to the DAO's demise. An attacker used the flaw to drain funds by calling on the split function available to token holders. The attacker was able to, in essence, withdraw funds over and over without updating the account balance held in the DAO. It took a combination of on-chain and off-chain governance efforts to create the DAO attack.

The first risk is related to the governance of the protocol. In this case, the developers of the protocol may behave negatively towards the stakeholders. There are mechanisms to cope, with the situation, such that a new protocol can emerge by forking the initial protocol.

Before the launch of a new protocol, developers do have full control over the business logic, and they act in a centralized manner. After the launch, the project has to become fully decentralized, in order to gain the trust of users. Decentralization is achieved with a governance token. Its whole purpose is to bring democracy to the direction of the protocol. The protocol token holders can vote on the new features' implementation and funds allocation. Decisions can be made by a quorum or a majority of voting members. Any governance attack is usually counterbalanced by the financial incentives of the community. In Bitcoin, if an entity can control 51% of the mining pool, it has the ability to rewrite "history", by rewriting the past blocks of transactions. As a consequence, the underlying value proposition of the Bitcoin changes, namely its decentralization nature, and its market value is likely to plummet. Therefore, it is financially unfeasible for an entity to invest resources in order to gain control of the cryptocurrency, only to collapse the potential gains. Nevertheless, the attacker can make gains during a small window of time between being gaining control over the protocol and the time attacked is identified. An attacker can obtain capital gains by selling the protocol token. Any large dump of a cryptocurrency in the market is followed by a decrease in price.

Blockchain uses the infrastructure of the internet. DeFi protocols are hosted on different internet addresses. A DNS attack is an attack that is subject to any entity surfing the internet. The DNS attack is linked to the social engineering formula. Attackers can ask for private keys of the blockchain account or the seed phrase used to generate the private keys. By exposing private keys or seed phrases people are subject to losing their funds.

Oracles are mechanisms to input real-world events information on the blockchain. The oracle input is independent of the blockchain and it can take many forms such as the price of an outside asset, the result of a sports event. The oracles are therefore trusted parties allowed to input outside data. Oracles are in their nature centralized and they need to be reliable. If the potential profit of manipulating an oracle data source exceeds the potential gains, the oracle becomes vulnerable to attacks.

Conclusions and Future Work

The expansion of the Internet enabled the creation of new business models, unmet before, such as crowdfunding, software as a service or dropshipping. Many sub-branches of existing markets were created in social media, content creation. The mobile devices enabled access to the internet from everywhere, which accelerated the usage.

In Blockchain Revolution [1], Dan Tascot describes 4 types of blockchain business organizations and 7 types of new business models. The four types are simple Smart Contracts with low automation and low complexity, autonomous agents with high automation and low complexity, open network enterprise (ONE) - with low automation and high complexity, and distributed autonomous enterprise: the distributed application or DApp. The 7 mentioned business models by are: blockchain cooperatives, creators of intellectual property, peer-to-peer production, the metering economy, platform builders, physical worlds animators and enterprise collaboration. In the current economy, the middle man, namely the platform, captures a big part of the value. The blockchain technology is set to lower the cost of maintaining the platform, reducing risk and thus enabling the participants to capture more of the value created. DeFI is a blockchain niche very like to complement any of the upcoming business models, in a similar way traditional finance is doing with the present internet business models.

The blockchain and its decentralized finance vertical will follow the same footprint because technologies generally unfold in layers. Many of the use cases or business models are not yet clear or yet to be discovered. Nevertheless, it is safe to state that technology is here to stay.

When a new technology emerges, it is usually positioned around a use case. It does not replace completely the existing technology, but it rather complements its. In the same manner, mobile technologies did not replace the web technologies, but rather they completed them.

In the same way blockchain and DeFi will most probably continue to enhance existing economies.

The growth of the crypto and its financial industry as a whole will be a consequence of multiple actors involved such as the business sector assessing use cases, investments funds providing market stability, governments providing support and regulatory frameworks and academia offering support in complex tech problems. Regulations are laws designed to control behavior. Governance when it's done right, is really about stewardship, collaboration, and incentivizing work on common interests to achieve common goals.

The regulation process is a matter of choosing what parts should be regulated, unregulated and which parts can regulate themselves. It is similar to the regulation of the Internet, in the sense that it is a mix between the three approaches.

Pioneers of the technology insisted that it couldn't be regulated because of its openness and its international/global reach. Both Internet pioneers and blockchain pioneers shared this view.

References

[1] Don Tapscott and Alex Tapscott, *Blockchain Revolution: How the Technology Behind: Bitcoin Is Changing Money, Business, and the World*, Portfolio, 2018

[2] Campbell R. Harvey, Ashwin Ramachandran, Joey Santoro, *DeFi and the Future of Finance*, Wiley, 2021"

[3] Satoshi Nakamoto, Bitcoin: A Peer-to-Peer Electronic Cash System, 2008, Available at: https://bitcoin.org/bitcoin.pdf

[4] Ethereum Whitepaper: A Next-Generation Smart Contract and Decentralized Application Platform. Available at: https://ethereum.org/en/whitepaper/

[5] Binance Smart Chain - A Parallel Binance Chain to Enable Smart Contracts. https://github.com/binance-chain/whitepaper/blob/master/WHITEPAPER.md

[6] Nick Szabo, Smart Contracts: Building Blocks for Digital Markets, 1996, Available at: http://www.truevaluemetrics.org/DBpdfs/BlockChain/Nick-Szabo-Smart-Contracts-Bui lding-Blocks-for-Digital-Markets-1996-14591.pdf

[7] Michael Casey, Jonah Crane, Gary Gensler, Simon Johnson, Neha Narula, The Impact of Blockchain Technology on Finance: A Catalyst for Change, International Center for Monetary and Banking Studies (ICMB), 2018

[8] Nathan Williams, Protocol for Due Diligence in the Raw Material Supply Chain

[9] Dabao Wang, Siwei Wu, Ziling Lin, Lei Wu, Xingliang Yuan, Yajin Zhou, Haoyu Wang, Kui Ren, "Towards A First Step to Understand Flash Loan and Its Applications in DeFi Ecosystem," in Proceedings of the Ninth International Workshop on Security in Blockchain and Cloud Computing. editor / Jian Liu; Shweta Shinde. New York NY USA: Association for Computing Machinery (ACM), 2021. pp. 23-28

[10] Smart Contracts: 12 Use Cases for Business & Beyond (2016) - Chamber of Digital Commerce. Available at: https://digitalchamber.org/wp-content/uploads/2018/02/Smart-Contracts-12-Use-Cas es-for-Business-and-Beyond_Chamber-of-Digital-Commerce.pdf

[11] Manuel Araoz, Demian Brener, Francisco Giordano, Santiago Palladino, Teemu Paivinen, Alberto Gozzi, Franco Zeoli, "Zeppelin Os: An open-source, decentralized platform of tools and services on top of the EVM to develop and manage smart contract applications securely," 2017, Available at: https://openzeppelin.com/assets/zeppelin_os_whitepaper.pdf

Silviu OJOG has graduated the "Gh. Asachi" Technical University, in 2013, in Iasi Romania BSc in Applied Electronics. He graduated University of Bucharest, Romania MSc in Software Engineering, 2016. He is currently enrolled as a PhD Student Economic Informatics, Bucharest University of Economic Studies.