The Impact of Blockchain in FinTech

Robie Gonzales, Alessandro Luis So

ABSTRACT: Since the 1990s, mathematicians have long researched the underlying foundations of blockchain technology. It was only in 2008 with the revolutionary proposal of Bitcoin where the protocol was finally put to the test. Since then, it has been hailed as a radical, disruptive development in money and currency being the first example of a digital asset which has no central controller. However, an arguably more important aspect of the Bitcoin experiment is the underlying blockchain technology as a tool for distributed consensus, tamper-proof construction and information transparency. This paper will explore the evolution of blockchain, the recent major developments in the ecosystem and the innovative, socioeconomic impacts in the financial services industry.

I. INTRODUCTION

The creation of Bitcoin in 2008 was a radical, disruptive innovation and clearly made its mark in the history of FinTech. What is more interesting though, is the technology behind the cryptocurrency, providing properties that enable for a plethora of complex use cases. Blockchains were initially created to solve problems pertaining to cash and money, but have quickly been realized to solve problems in other traditional financial services. This has resulted in a vision for a financial system that is decentralized and accessible to anyone.

II. HISTORY OF BLOCKCHAIN

Blockchain technology is not anything inherently novel, but rather a culmination of different areas of research in computer science and mathematics. At its core, blockchains are a problem solving technique, particularly problems revolving around the idea of *distributed consensus* and how multiple, independent computers in a network can reliably agree on conflicting information [1]. In other words, how can an independent party decide the current state of data given potentially unreliable information. Blockchains solve this problem by dividing data into **blocks** and use a distributed consensus algorithm to determine the order of blocks.

A. BLOCKCHAIN TECHNOLOGY

Each block in a blockchain contains a **hash**, a cryptographically generated unique identifier. Hashes are generated based on the data within the block are created by **hash functions**, which are designed to be one-way. This means that the smallest change in data will result in a completely different hash. Hashes are also designed to be collision resistant, meaning it is computationally infeasible to find two or more inputs that produce the same output [1]. Each block also contains a **data** field as well as the hash of the previous block. This hash of the previous block links blocks together forming a *blockchain*. If a previous block's data were to change, it would have a different hash resulting in all subsequent blocks also having different hashes. This allows the detection and rejection of any changes to previously published blocks.

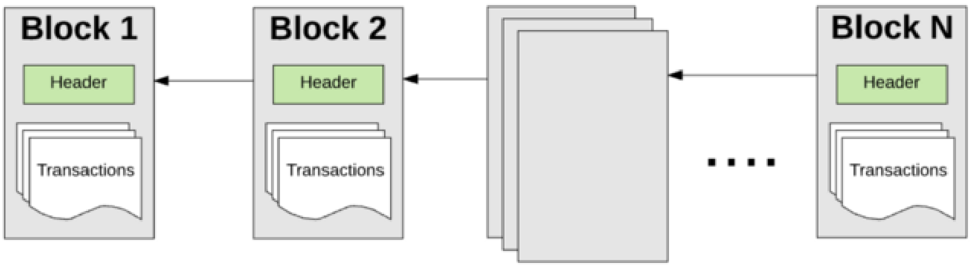

Figure 1. A simplified blockchain [1]

Blockchains are maintained by a peer-to-peer network of computers performing consensus on blocks to be added. The process of adding a new block to the blockchain is called *mining*, and requires large amounts of computational power. Consensus models allow the network to operate in a decentralized manner, as there is no need for a trusted centralized third party to determine the state of the system. Copies of the blockchain are replicated throughout the network allowing every user to verify the blockchain's integrity resulting in an immutable database.

The essential elements of a blockchain are that it is a consensus protocol used to create an append-only log that can be used to form a public auditable database [2]. This provides us with many beneficial features such as immutability, security and decentralization. Combining methods from computer science, mathematics and finance, a *digital ledger* can be built with a blockchain, removing the need for a trusted central authority and resulting in a system with complete transparency and trust.

B. A BRIEF HISTORY OF LEDGERS

Throughout history, people have utilized systems to track their transactions. In ancient civilization times, the Mesopotamiams would record quantities of items on clay tablets [3]. These tablets would also include other entries such as pictographic descriptions, signatures of officials, timestamps and other various features. These clay tablets created a system that enabled large communities to develop trust and stability. This allowed parties within the community to settle into a specialization and perform transactions with others as the administrative clay tablets made the system seem trustworthy, systematic and fair.

Centuries later, a new system of ledgers emerged among the merchants and money lenders of Italy. This ledger defined logical relations between its entries where every entry was entered twice, once as a credit and once as a debit. This double-entry system was essentially an algorithm that organized the transactions of a party into the formula: *Assets = Liabilities + Capital.* This system gave individuals, investors and lenders a common language. Financial statements derived from this system and became a standard way for parties to demonstrate their creditworthiness.

A key note of ledger systems prior to the invention of fiat money is that their entries always measured a quantity of something tangible owned or owed. This poses the question of how to make a ledger asset valuable unless it's redeemable for something valuable. This brings us to a fundamental idea of economics in that things are valuable based on the benefits derived from an economic good [3]. In other words, things are valuable because they are a means of obtaining an economic good or a means of avoiding an economic bad.

Governments realized this scheme and implemented it through a central banking system in which a central bank is given special legal authority. This central bank issues bank notes which are redeemable in credit and does not redeem its liabilities. The government then accepts payments of taxes by crediting its account at the central bank. This system constructs a new ledger technology where entries on the central bank's ledgers have value despite not being redeemable. This innovative system caused a fundamental shift in how humanity viewed money and wealth. The central banking system redirected the money of humanity from commodities and real goods to ledger numbers on paper and electronic databases [3].

C. BITCOIN

In 2008, a person under the pseudonym "Satoshi Nakamoto" released *Bitcoin: A Peer-to-Peer Electronic Cash System* [4], a paper proposal for a new system of ledgers. The paper revealed how to leverage blockchain technology to build a purely peer-to-peer system of electronic cash without suffering from the inherent weaknesses of the traditional trust based central model. Similar to how a central bank functions, the Bitcoin blockchain can create and consume coins during a **transaction** which it then stores in its data field. Similar to fiat currencies and the central bank, the entries on this transactional-based digital ledger represent value.

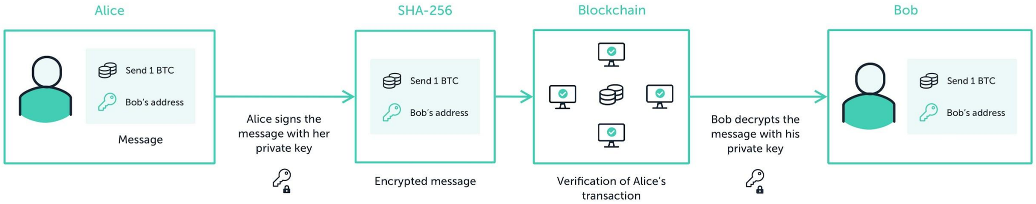
Alice
Send 1 BTC
Bob's address
Message
Alice signs the message with her private key
SHA-256
Send 1 BTC
Bob's address
Encrypted message
Blockchain
Verification of Alice's transaction
Bob decrypts the message with his private key
Bob
Send 1 BTC
Bob's address

Figure 2. Overview of a Bitcoin transaction [5]

Users on the Bitcoin network have a **public key** and a **private key**. The public key acts as an **address**, only able to receive transactions while only the private key can send and sign transactions, verifying its validity [5]. Leveraging methods from cryptography, public and private keys can be made such that transactions are guaranteed to be verifiable and secure. Double spending of coins is rendered impossible and provides pseudonymity to users. The genius of Satoshi Nakamoto's Bitcoin cannot be understated. Despite that, there are major concerns surrounding the sustainability and scalability of the network as well as its limitations.

III. BLOCKCHAIN 2.0

Blockchains are best known for its first implementation, Bitcoin and cryptocurrency. However, Bitcoin's limitations have caused a shift of attention to other aspects behind the technology powering it. Instead of just storing *data* on the blockchain, we can also store *computation*. The ideas of performing computations backed with all the benefits of a blockchain allow for unprecedented systems of innovative applications and has signalled the start of a new era for blockchains.

A. ETHEREUM

Ethereum is a blockchain created in 2015 that intends to provide a protocol for building decentralized applications (dapp) [6]. While Bitcoin was designed to support a singular application; a decentralized version of electronic cash, Ethereum aims to extend use cases of blockchain technology by providing a platform for applications. They accomplish this by providing a blockchain with built-in capabilities that enable the creation of *smart contracts*, self-executing pieces of code that can perform arbitrary state transition functions.

Ethereum has also standardized protocols for creating *tokens*, allowing for anyone to tokenize virtually anything resulting in lower barriers of entry. Ethereum can be seen as akin to the Open Banking movement in that it aims to be an interoperable network, able to service a variety of applications. In general, there are three types of applications built on top of Ethereum [6]. They include financial applications; providing users with powerful ways of managing and entering into contracts with their money, semi-financial applications; where money is involved but there is a heavier non-monetary side to what is being done and non-financial applications.

Ethereum has been the leader in the blockchain community for striving for a more sustainable, scalable and secure ecosystem [6]. They have made great technical strides in novel consensus mechanisms, scalable architectures and secure systems. Since their inception in 2015, they have grown to be the second largest blockchain with over 1 million daily transactions and over 480 billion USD market cap [7].

B. SMART CONTRACTS

The contract, a set of promises agreed to between parties, has been the traditional way of formalizing relationships. Throughout history it has been an essential building block of a free market economy. The digital revolution has allowed for the creation of new types of parties and thus, new ways of formalizing these relationships have been made possible. These new types of contracts have been dubbed *smart contracts.* A smart contract extends the idea of storing data on the blockchain and extends it to computation.

Smart contracts are a set of agreements specified in computer program form that are stored on the blockchain [6]. Smart contracts are very logical, following an “if this then that” structure. This means that they behave exactly as programmed and since they live on the blockchain, they cannot be changed. One of the biggest problems with traditional contracts is the need for trusted parties to follow through with the contract’s outcomes. Even if the conditions of the agreement are met, you still have to trust the other party to fulfill the agreement.

Smart contracts solve this by turning the terms of an agreement into computer code that automatically executes when the contract’s conditions are met. This is one of the most significant benefits of smart contracts as they remove the need for trust. A smart contract's outcome will always be automatically executed when the conditions are realized. Another benefit is predictability. The human factor is one of the biggest points of failure with traditional contracts and can often lead to misinterpretations of the same scenario. Smart contracts remove the possibility of different interpretations and guarantee the same result in equivalent conditions.

C. ORACLES

One limitation of blockchains is that they cannot pull in data from or push data out to any external system. This simple limitation, dubbed the *Oracle Problem*, is the precise property that makes blockchains extremely secure and reliable [8]. A blockchain network only needs to form consensus using data already stored on the block. However, for smart contracts to realize the majority of their potential use cases, they must connect to the outside world. Bridging the connection between blockchains (on-chain) and the outside world (off-chain) requires another piece of infrastructure known as an *oracle*.

A blockchain oracle is a secure piece of middleware that facilitates communication between blockchains and any off-chain system. Oracles are an essential aspect of smart contracts and allow for a wide range of complex use cases. Key functions of oracles include listening for user or smart contract requests for off-chain data, validating proofs of oracle services, performing secure off-chain computations and more.

Oracles operate as separate networks and are not integrated into the base layer of a blockchain for several reasons. Blockchains are highly secure and reliable due to specific design principles, namely its use of decentralization and data validation methods. Introducing subjectivity at the base layer of a blockchain poses security, reliability and governance concerns putting at risk the very value proposition blockchains aim to provide. Ultimately, the more complexity there is at the base layer of a blockchain, the more attack surface and risk to all applications that run on it. Having oracles operate as separate networks ensures blockchains have a lover attack surface and retain their determinism by maintaining a singular focus on consensus, while oracles have the required flexibility to generate determinism from a complex and subjective off-chain system without creating dependencies and limitations.

A key note of oracles is that similar to blockchains, they should be decentralized. Recall that the goal of a smart contract is to achieve determinism through technological enforcement of the contract's terms as opposed to probabilistic execution by human enforcement. To achieve this, there must be no single point of failure within the blockchain, a feature that must be extended to the oracle. Centralized oracles pose great risks as they can manipulate the inputs that determine a contract's outcome.

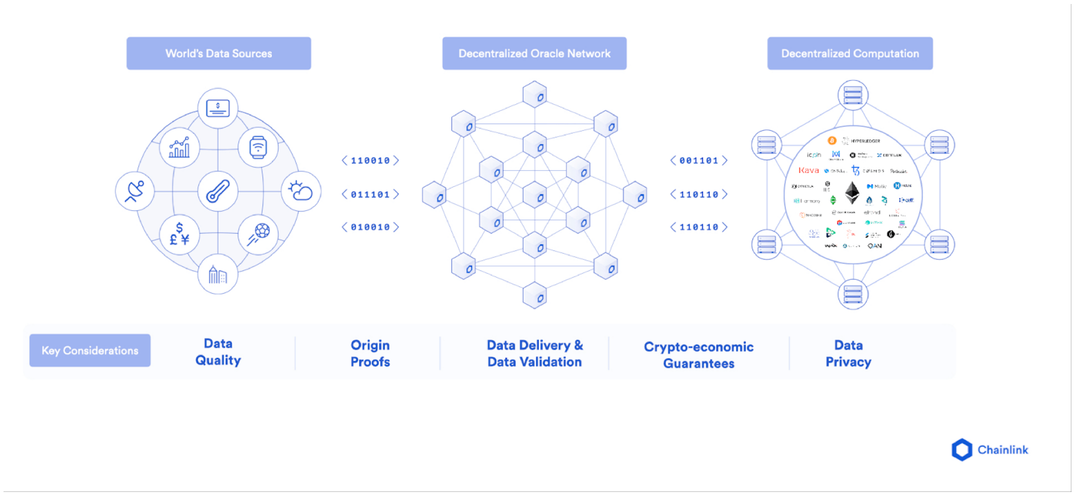

Figure 3. Chainlink's vision for decentralized oracles [8]

Chainlink has been the leader in developing decentralized oracle networks [8]. Decentralized oracle networks allow smart contracts to securely connect with external data systems without sacrificing its core value of determinism. Many financial dapps rely on Chainlink oracles to deliver financial data that is then used by a smart contract. These oracles ensure any off-chain resource is delivered securely, maintaining a core value of blockchains.

IV. DECENTRALIZED FINANCE

Decentralized finance (DeFi) is a movement that aims to build a new financial system that is open to everyone and does not require trusting intermediaries. Traditionally, the heart of market-based finance is a series of intermediaries that bring together disparate participants. These intermediaries bring together a range of financial market participants such as those with financial resources and those seeking financial resources. Thus, traditional finance is characterized by major intermediaries who centralize services and financial resources.

As a result, financial centres have emerged around the world. In order to function, these centralized financial centres fundamentally depend on trust and confidence which is underpinned by laws and regulations. Over time the state has taken an increasing role of regulation in almost all aspects of finance, in particular amidst the aftermath of the 2008 financial crisis [9]. Thus, market-based financial systems can be seen as fundamentally unstable as instability and other forms of market failure attempt to be addressed by regulation, albeit never entirely successfully.

It is this weakness that underlies the value propositions of DeFi and its vision of a financial system without the dominance of concentrated intermediaries. Traditional financial intermediaries suffer from opaque, tightly controlled environments with aging infrastructure resulting in massive inefficiencies [9]. DeFi presents a vision where technology can potentially eliminate the inherent risks of concentrated systems central to traditional finance. Scale can be achieved with blockchains and modern day technology allowing for a global range of market participants.

Ethereum has been the leader of dapp development in the DeFi space. Ethereum's smart contract compatible programming language, Solidity, is very powerful and allows for a wide range of use cases. Furthermore, DeFi is based upon open-source technologies which greatly lowers the barrier of entry for both developers and participants. As of November 2021, the total market cap of all DeFi products exceeds 2.7 trillion USD with monthly trading volume averages of 100 billion USD [7]. The DeFi ecosystem is growing everyday as new dapps and ideas are being implemented allowing for unprecedented financial products.

A. DECENTRALIZED EXCHANGES

Cryptocurrency exchanges provide a crucial source of liquidity to the global cryptocurrency market. As this market and DeFi continue to expand, exchange platforms must scale in response to the demand for new financial products. With disintermediation as a core value of the blockchain community, decentralized exchanges (DEXs) are growing in popularity alongside centralized exchanges (CEXs).

Centralized cryptocurrency exchanges have been the traditional way of interacting with cryptocurrencies and play a vital role in the acceptance of the asset by governments, businesses and institutions around the world. Similar to the traditional world of finance, CEXs function as trusted intermediaries; facilitating the buying and selling of cryptocurrencies for fiat, as well as custodians; storing and protecting your funds. Decentralized exchanges take a different approach by operating without intermediaries and instead, rely on self-executing smart contracts to facilitate trading. An exchange is built out of three main components: a price discovery mechanism, a trade matching engine and a trade clearing system [10]. By leveraging blockchain technology, all of these components can be encoded into smart contracts resulting in a completely decentralized exchange. This enables instantaneous trades often with lower costs than on CEXs. Furthermore, the absence of intermediaries creates a non-custodial framework allowing users to retain custody of their cryptocurrencies as well as giving them management of their wallets and private keys.

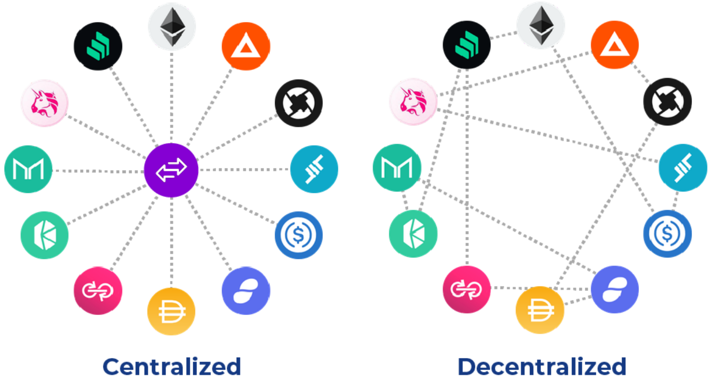

Figure 4. Architectures of centralized and decentralized exchanges [29]

In traditional order book models, the exchange relies on a market maker to provide liquidity and depth to the markets [10]. Market makers function as entities that are always willing to buy or sell an asset, allowing trades to be executed seamlessly. Instead, DEXs leverage an *automated market maker* (AMM), an algorithm for determining asset pricing in a *liquidity pool*. This AMM facilitates all components of an exchange through smart contracts, resulting in a completely decentralized, self-executing exchange.

1. AUTOMATED MARKET MAKERS

Automated market makers are predefined pricing algorithms that automatically perform price discovery and market making using assets within a liquidity pool [11]. This removes the need for **liquidity providers** to constantly monitor the market and adjust bid and ask prices while allowing **liquidity takers** to directly trade against the liquidity pool. This revolutionary mechanism provides many trading benefits such as instantaneous settlement, immediate access to liquidity and lower barriers of entry.

The core idea behind AMM algorithms revolve around **bonding curves**, which define a relationship between the price and the total token supply [12]. In other words, the ratios of each token in a pool dictate a price. The tokens in a liquidity pool are **continuous tokens** due to special properties enabled by a bonding curve. Continuous tokens have a *limitless supply, deterministic price*; where the buy and sell prices increase and decrease with number of tokens created, *continuous price*; where the price of token *n* is greater than token *n-1* and less than token *n+1*, and provide *instant liquidity*; where tokens can be bought or sold instantaneously at any time [12].

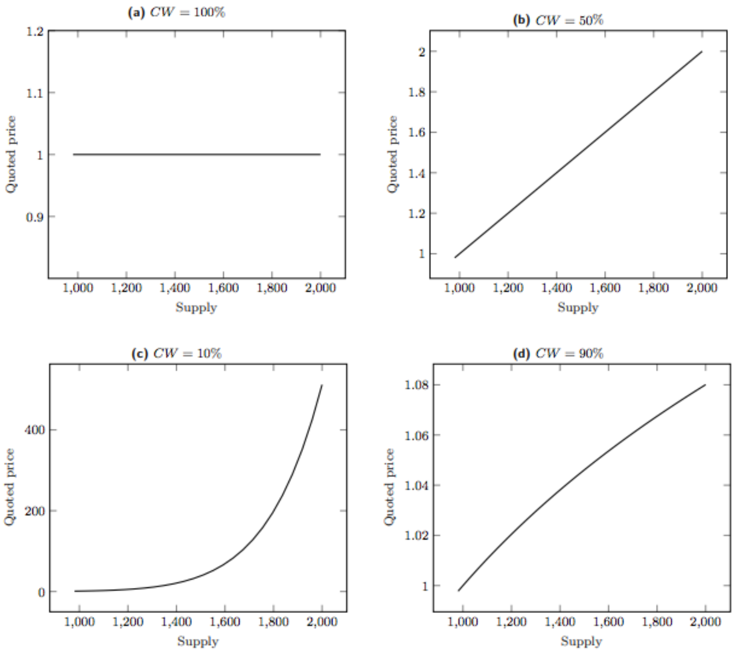

Figure 5. Ratio of supplied tokens in a pool can be optimized for different scenarios [12]

Bonding curves are mathematical formulas and thus can be optimized for different use cases. The most popular AMM algorithm is the **Constant Product** formula where the product of the supply reserves for each token equals some constant. For example in a pool of two tokens (*X/Y*), taking token *X* will decrease the supply ratio of *X* resulting in an increase of price while increasing the supply ratio of *Y* and thus decreasing the price. The core actions of an AMM can be summarized into the following functions: *AddLiquidity(X, Y), RemoveLiquidity(X, Y)* and *TransactXforY(X)* [10].

AMMs have been a revolutionary innovation in the DeFi space and have allowed for the creation of new innovative technologies. However, they do suffer from some weaknesses such as **impermanent loss**, which occurs when the price of the liquidity you provided changes compared to when you initially deposited them [11]. Similar to traditional exchanges, AMMs also suffer from **slippage**, where the price of an asset changes during a trade, albeit not as significant.

2. LIQUIDITY POOLS

Liquidity pools are smart contracts that lock in a particular combination of tokens [10]. AMMs and liquidity pools go hand in hand, constantly interacting with each other to determine asset pricing. As we've seen, changes in the pool's token supply results in changes of token prices. The extent of these price changes depends on the size of the trade in comparison to the pool. Since larger liquidity pools can facilitate larger trades resulting in less slippage and overall better experience, various liquidity pool protocols provide incentives to liquidity providers in the form of native tokens. These native tokens earn a fractional fee every time the liquidity pool facilitates a trade and can be **burned** (destroyed) to return the liquidity. The idea of offering incentives to liquidity providers is called *liquidity mining*, and is a core aspect of many DeFi protocols [11].

Uniswap, Curve and Balancer have been three dominant DEX liquidity pool protocols that have emerged in recent years. Uniswap accounts for over 60% of all daily DEX activity with over 9.5 billion USD total value locked into the protocol [13]. Uniswap users pool two tokens together that are then traded against with the price being determined by an AMM. The AMM algorithm used by Uniswap is the **Constant Product** formula where the reserves of each token must always equal some constant [14]. This allows liquidity providers to withdraw or deposit funds simply by supplying the proportional value of each token. Furthermore, when providing liquidity, users receive a liquidity pool token which can be redeemable for the underlying assets as well as fees, which are evenly distributed amongst the providers in the pool. This results in trades always being able to execute as there is constant liquidity. Other protocols such as Curve and Balancer have extended their AMM algorithms to cater to stablecoins as well as pools of multiple tokens [15].

Liquidity pool protocols and AMM algorithms have been a disruptive innovation in the DeFi space. However, they do suffer from problems experienced in traditional exchanges. Even without any information asymmetry, if the token exchange rate fluctuates liquidity providers face

arbitrage problems, which is the simultaneous purchase and sale of an asset in different markets [10]. While market makers in a centralized order book exchange can alleviate the problems of adverse selection through bid-ask spreads, liquidity providers in an AMM can neither charge a bid-ask spread nor front-run due to the order execution structure [11]. Liquidity mining, which are incentives given to liquidity providers, aim to alleviate these problems. Decentralized exchanges were the first type of platform to utilize AMMs and liquidity pools but they have quickly grown to become pillars in other areas of DeFi such as crowdfunding, lending & borrowing and governance.

B. LENDING & BORROWING

Lending & borrowing have always been important services in traditional finance. The simple idea of lenders providing funds in return for interest allows willing borrowers to pay interest in exchange for having a lump sum of money available immediately. Traditionally, lending & borrowing have been heavily facilitated by intermediaries, often with high barriers of entry. DeFi lending & borrowing protocols allow users to become lenders or borrowers in a completely decentralized and permissionless way while still retaining full custody of their tokens.

Compound [16] and Aave [17] are leading algorithmic money market protocols with over 23 billion USD combined total value locked [13]. Both of the protocols function by creating **money markets** for particular tokens. Lenders supply funds into a money market and are issued native protocol tokens, cTokens in Compound and aTokens in Aave. These native tokens earn interest and are necessary for redeeming the underlying funds. Borrowers looking to take a loan must supply collateral greater than the amount they wish to borrow. As long as the borrowed amount is less than the collateral amount times some **collateral factor**, there is no limit to the amount one wishes to borrow. If the value of the collateral falls below this threshold, the smart contract will automatically liquidate the collateral to repay the borrowed amount [18].

The interest lenders receive and borrowers pay is determined by the ratio between supplied and borrowed tokens in a particular money market. Furthermore, the interest APYs are calculated per block resulting in variable interest rates depending on latest supply and demand for particular money markets. Native protocol tokens continue earning interest which allows for varied passive income strategies.

Over-collateralization may seem counterintuitive at first but it is this precise property that makes DeFi lending & borrowing so unique. DeFi users can lend capital and unlock liquidity without trading, resulting in a plethora of possibilities such as margin trading, liquidity mining or *yield farming*. Traditionally, lending & borrowing have been dominated by institutions with high barriers of entry such as credit scores or bank data. DeFi lending & borrowing protocols leverage blockchain technology, smart contracts and over-collateralization to create a more equitable financial market.

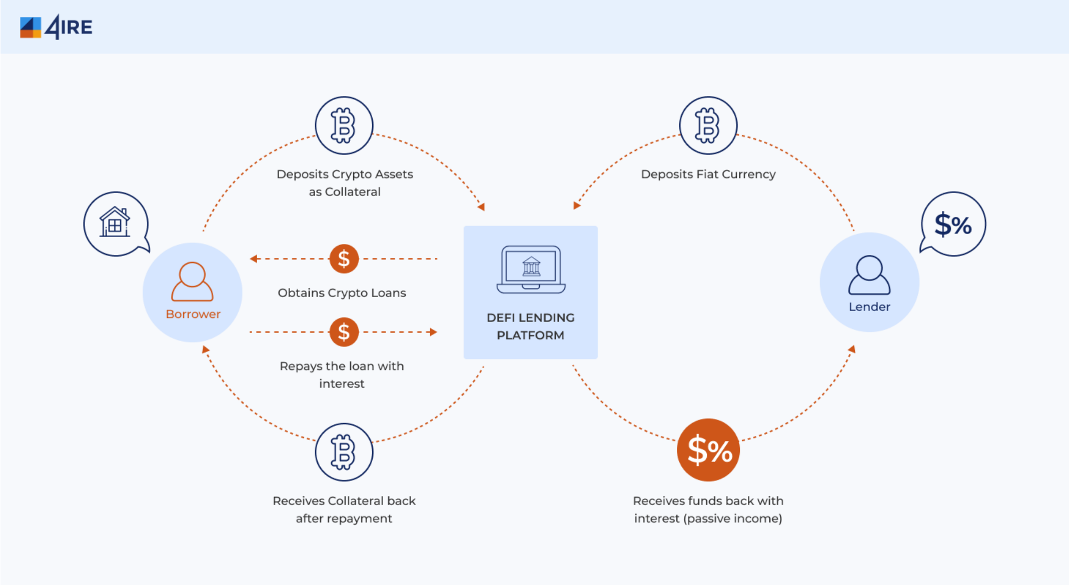
4IRE
Deposits Crypto Assets as Collateral
Deposits Fiat Currency
Borrower
Obtains Crypto Loans
Repays the loan with interest
DEFI LENDING PLATFORM
Lender
$%
Receives Collateral back after repayment
Receives funds back with interest (passive income)

Figure 6. Overview of lending & borrowing [30]

C. DERIVATIVES

Derivatives are contracts that derive its value from the characteristics of an underlying entity. This means that the buying and selling of a derivative contract does not involve the actual exchange of the underlying entity itself [19]. Smart contracts combined with oracles allow for the creation of an unprecedented set of derivative contracts. In other words, blockchain synthetic assets can mirror the performance of any real word entity resulting in a wide range of potential products.

Popular traditional derivative contracts include futures, options, swaps and forwards. The most commonly used use cases of derivatives are hedging; a risk management strategy to offset losses by taking an opposite position, and speculation; as they offer easy exposure to particular assets that may be hard to access otherwise as well as easy leverage [19]. Smart contracts and decentralized oracles radically change what DeFi derivative contracts can offer. These new types of contracts are quickly becoming pillars in other realms of DeFi such as insurance and margin trading. Popular innovative DeFi derivatives that have emerged recently include *weather derivatives,* where decentralized oracles feed valid weather data into a smart contract which then determines a price, and *perpetual contracts* [19].

Perpetual contracts are similar to a futures contract, which allows the buying or selling of an asset at a predetermined date for a specified price, with a few key differences. The biggest difference is that perpetual contracts have no expiration date or settlement, allowing them to be held or traded for an indefinite amount of time [20]. These contracts are native to a particular exchange and compose of a **mark price**; which is the trading price of the contract on its exchange, an **index price**; the price of the underlying asset, as well as **funding rates** and **margin**. Perpetual contracts mimic a margin-based spot market by utilizing funding rates to provide price stability and hence, trade close to the underlying reference index price. Perpetual funding rates incentivizes traders to buy perpetual contracts when the price is low relative to the index and sell when the price is high relative to the index. Traders must also provide collateral, known as margin. When the mark price moves against the trader, the resulting losses are deducted from this margin and if the margin balance goes too low, it will be liquidated resulting in the position automatically closing out [20].

Synthetix [21] and dYdX [22] have been leading DeFi derivatives protocols with over 1.6 billion USD combined total value locked [13]. Synthetix utilizes a highly over-collateralized shared debt pool to issue synthetic assets that track the value of real world assets. Combined with algorithmic liquidity smart contracts, traders can receive optimal price execution with little slippage. On the other hand, dYdX operates as a non-custodial perpetuals exchange that uses a centralized order book while ensuring trades and liquidations are settled in a trustless manner. This provides traders with minimal gas and trading fees with up to 25x leverage.

Derivatives are key elements of any mature financial system. The derivatives market plays a crucial role in providing market liquidity, creating investment optionality and providing other ways to manage risk. Traditionally, derivative trading has been limited to hedge funds, commercial banks and other institutional players due to high fees from contract creation and enforcement [19]. By leveraging blockchain technology, innovative decentralized derivative protocols continue to emerge. Paradigm, a leading investment firm focused on cryptocurrencies and decentralized protocols, has a dedicated research team exploring new types of derivatives such as power perpetuals, floor perpetuals and everlasting options [23].

D. DECENTRALIZED AUTONOMOUS ORGANIZATIONS

Decentralized autonomous organizations (DAOs) are communities where members can vote on decisions regarding the protocol [24]. Members of a DAO are issued governance tokens which can then be used to vote on the usage of resources owned by the protocol such as a liquidity pool. In other words, DAOs provide an infrastructure for deciding and enforcing a set of shared rules which allows groups of people with common goals to join together. This allows for unprecedented opportunities of global collaboration and coordination. Since smart contracts live on the blockchain, all activity is transparent and governance is flat. The ideas of a DAO have lots of potential in contexts of crowdfunding such as charitable funds or venture capital funds.

MakerDAO was one of the first protocols in the DeFi movement and the first protocol to introduce the idea of a *stablecoin* [25]. The MakerDAO protocol allows users to generate the stablecoin DAI by leveraging collateral assets approved by the “Maker Governance”. Anyone who holds the governance token can vote on decisions regarding the protocol. The ideas of stablecoins and DAOs have quickly grown to be essential elements of the entire DeFi system. Stablecoins offer stability which is vital in the volatile cryptocurrency market and DAOs offer unique growth strategies for various organizations [26].

E. THE FUTURE OF FINANCE

Financial systems have been key elements of civilizations throughout human history. The modern financial system has gone through decades of technological development in attempts to make finance more efficient. Whether it was in the 1920s with punch cards, the invention and adoption of the Internet throughout the 60s to 90s and even post 2008 financial crisis with the emergence of FinTech services, finance as we know it is radically changing [9].

Despite a century of technological innovations, the traditional financial system is far from being perfect. Settlements taking days to process, massive inefficiencies and costs, silos of information and high barriers of entry are just some pain points throughout the system. Intermediaries play an essential role in establishing trust and mediating economic transactions that would otherwise be difficult to execute [9]. Nevertheless, intermediaries often enjoy substantial power in shaping these transactions to maximize their self-interests. The tension between the need for efficient transactions and concern over monopoly power is especially prevalent in this digital age.

Decentralized finance aims to build a new financial system by leveraging the power of cryptography, smart contracts and blockchains. Smart contracts can facilitate peer-to-peer transactions increasing the scope and efficiency of these services. The guarantees of blockchain technology offer fair, permissionless, censorship-resistant services that greatly lowers the barriers of entry and in turn, stimulates innovation. A vast array of unprecedented financial products enable unique wealth strategies such as yield farming; a process of leveraging multiple DeFi protocols to maximize returns, or risk management strategies through innovative derivatives [27]. A key note to remember is that DeFi is still in its early stages. The creation of Ethereum and its smart contract capabilities in 2015 marked the start of this new era and since then has seen tremendous growth. Total value locked (TVL), which is the amount of assets locked into a protocol's smart contract, grew from under 1 billion USD in early 2020, to 20 billion USD in early 2021, to all time highs of 270 billion in late 2021 [13]. DEX volume is another popular metric with monthly averages of 10 billion USD in 2020 to 100 billion USD in 2021 [13].

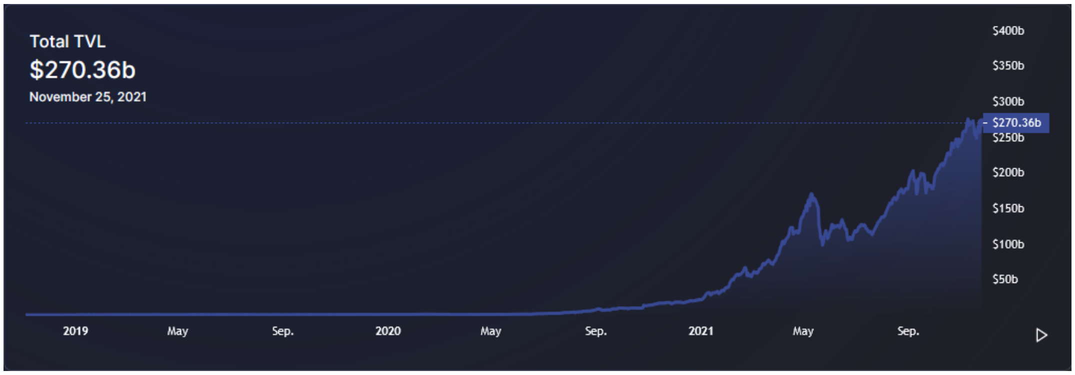

Figure 7. Total value locked into smart contracts (USD) [13]

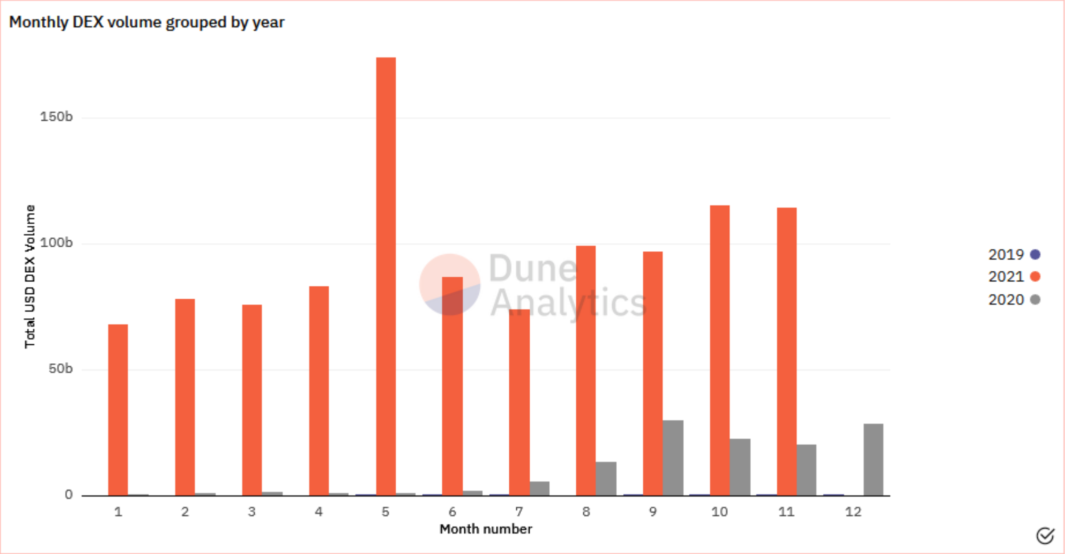

Figure 8. Monthly DEX volume grouped by year [28]

With distributed trust and decentralized protocols enabled by blockchain technology, innovators from all backgrounds have recognized the possibilities of building a new open financial system. By doing so, they hope to ultimately democratize finance, broaden inclusion and empower open access. While this movement is still relatively new, it's clear that DeFi will disrupt existing industries and create new opportunities of innovation.

V. CONCLUSION

The impact of blockchain technology in the FinTech industry has clearly been prevalent. The creation of Bitcoin in 2008 was a revolutionary leap in computer science and mathematics, elegantly combining decades of research in multiple areas. From its shortcomings, we've seen great developments through Ethereum for it's vision of a blockchain ecosystem that is more sustainable, scalable and secure. This has allowed for the development of an unprecedented system, decentralized finance. Despite its young age we have already seen the massive socioeconomic benefits in such a system and it's safe to say there is still untapped potential. At its core blockchains are a way to solve problems, and this technique is already being realized in areas outside of FinTech such as supply chain management, digital identity and healthcare. As blockchain technology continues to be adopted, it will be exciting to follow its development.

REFERENCES

[1] Yaga, D., Mell, P., Roby, N., & Scarfone, K. (2019). *Blockchain technology overview.* arXiv:1906.11078.

[2] Casey, M., Crane, J., Gensler, G., Johnson, S., & Narula, N. (2018). *The impact of blockchain technology on finance: A catalyst for change*. 21st Geneva Report

[3] LLFOURN. (2018). *A brief history of ledgers*. https://medium.com/unraveling-the-ouroboros/a-brief-history-of-ledgers-b6ab84a7ff41

[4] Nakamoto, S. (2008). *Bitcoin: A peer-to-peer electronic cash system*. https://bitcoin.org/bitcoin.pdf

[5] Ledger. (2019). *What are public keys and private keys?* https://www.ledger.com/academy/blockchain/what-are-public-keys-and-private-keys

[6] Buterin, V. (2014). *A next-generation smart contract and decentralized application platform*. https://ethereum.org/en/whitepaper/

[7] CoinMarketCap. (2021). *Cryptocurrency prices, charts and market capitalizations*. https://coinmarketcap.com/

[8] Chainlink. (2021). *Chainlink: Blockchain oracles for hybrid smart contracts.* https://chain.link/

[9] Zetzsche, D., Arner, D., Buckley, R. (2020). *Decentralized Finance, Journal of Financial Regulation.* Oxford University Press.

[10] Zhou, L., Qin, K., Torres, C., Le, D., Gervais, A. (2020). *High-Frequency Trading on Decentralized On-Chain Exchanges*. arXiv:2009.14021.

[11] Capponi, A., Jia, R. (2021). *The Adoption of Blockchain-based Decentralized Exchanges*. arXiv:2103.08842.

[12] Riady, Y., (2018). *Bonding Curves Explained.* https://yos.io/2018/11/10/bonding-curves/

[13] DefiLlama. (2021). *DefiLlama. DeFi Dashboard.* https://defillama.com/

[14] Uniswap. (2021). *Uniswap Protocol.* https://uniswap.org/

[15] Balancer. (2021). *Balancer AMM DeFi Protocol.* https://balancer.fi/

[16] Compound. (2021). *Compound.* https://compound.finance/

[17] Aave. (2021). *Aave - Open Source DeFi Protocol.* https://aave.com/

[18] Finematics. (2021). *Lending & Borrowing in DeFi Explained*. https://finematics.com/lending-and-borrowing-in-defi-explained/

[19] Cryptopedia. (2021). *Blockchain and Financial Derivatives*. https://www.gemini.com/cryptopedia/cryptocurrency-derivatives-trading-synthetic-assets

[20] BitMEX. (2021). *Perpetual Contracts Guide*. https://www.bitmex.com/app/perpetualContractsGuide

[21] Synthetix. (2021). *The Derivatives Liquidity Protocol.* https://synthetix.io/

[22] dYdX. (2021). *Perpetuals, decentralized.* https://dydx.exchange/

[23] Paradigm. (2021). *Crypto/web3 Investment Firm.* https://www.paradigm.xyz/

[24] Ethereum. (2021). *Decentralized autonomous organizations (DAOs).* https://ethereum.org/en/dao/

[25] MakerDAO. (2021). *MakerDAO - An Unbiased Global Financial System*. https://makerdao.com/en/

[26] Ethereum. (2021). *Stablecoins.* https://ethereum.org/en/stablecoins/

[27] Finematics. (2021). *What is Yield Farming? DeFi Explained*. https://finematics.com/yield-farming-explained/

[28] Dune Analytics. (2021). *Free crypto analytics by and for the community*. https://dune.xyz/home

[29] Yield. (2021). *Defi Banking.* https://www.yield.app/post/what-are-decentralized-exchanges-and-why-do-we-need-them

[30] 4ire Labs. (2021). *How to Build a DeFi Lending and Borrowing Platform?* https://4irelabs.com/articles/how-to-build-a-defi-lending-and-borrowing-platform/