APPLICATIONS OF CRYPTOCURRENCY

Cryptocurrency, a major application of blockchain, has become more evident nowadays. A lot of new entrepreneurs and business innovators have started to implement cryptocurrency as solutions to many problems which varies from basic transactions to earning via it. We will discuss few of the prominent applications of cryptocurrencies along with few applications of blockchain in the context of cryptocurrency and some terminologies used in cryptocurrencies.

1. NFTs (Non-Fungible Tokens) [1]

   NFTs are one of cryptocurrencies or one can say a type of cryptocurrency which is a non-fungible meaning it cannot be replaced or exchanged with its identical item. It means that each NFT existing as the smart contact on any blockchain protocol is unique.

   These NFTs are now being traded, loaned, sold or kept secured on various platforms. I will be discussing a platform for a cross chain auction of NFTs and loan called NFTA.
   The making of NFT involves following elements.

   - Blockchain (NFTA use Ethereum as their main blockchain network)
   - Smart Contract (Enables different networks and decentralized parties to have a fair transaction without using any third party and provide a general method for every application build on any network. NFTA use Binance Smart Chain BSC as smart contract)
   - Address (Address in blockchain is a unique combination of private and public key made up of hexadecimal system. For transferring of NFT, the user has to prove the owner ship of its private key)
   - Data Encoding (Involves conversion of NFT to digital signature. NFT ownership can be claimed or confirmed as the owner has a signed digital signature or hex value provided by the creator of NFT)
   - Protocol (involves **digitization, storing, signing, minting and trading.** Digitization is converting NFT to proper format, storing means keeping the NFT inside or outside the blockchain network, signing means signing the contract and owning the hash of it and sending the NFT to the BSC network. After that NFT is minted i.e. adding the new block of a transaction to existing blockchain. It can be traded now.)

2. Gaming (Axie Infinity) [2]

   Axie infinity is a game based on species inspired by a Pokémon game. It is a game which is based on crypto currency and blockchain. One can earn in this game by battling one-on-one with other player species, by breeding their species, by selling the axies (specie) on marketplace. The major cryptocurrency involved in Axie Infinity are SLP (Small Love Potion) and AXS (Axie Infinity Shards). Both tokens can be earned by playing games and completing several missions etc. These tokens can be used to buy more Axies or trade them on decentralized marketplace including Binance. Current market value of SLP is $ 0.21 while AXS is of $40. The game is based on Ethereum blockchain (ERC-721: A standard token of Ethereum for NFTs)

3. DeFi (Decentralized Finance) [3]

   DeFi is financial infrastructure which is an open source whose protocol are built on Ethereum smart chain and decentralized apps (DApps) which makes DeFi a replacing financial system with no one having hold on majority of the financial system. This make DeFi highly transparent with minimum risk of tempering or altercation.

4. Consensus Algorithms

   Consensus algorithms are essential part of blockchain as they approve and verify any activity on blockchain, as blockchain is a decentralized ledger. It make sure that all the nodes are at agreement regarding the changes of state of certain data distributed at different nodes. There have been many consensus algorithms like PoW, PoS, pPBFT, SCP etc.

5. Regulation of Blockchain

   Since blockchain is a public ledger, there is a need that all the details are public yet anonymous. This is not yet possible fully. A lot of privacy and regulations are being made to make it more anonymous.

NFTA: A cross-chain NFT Auction and Loan Platform [4]:

NFTA is a platform which uses a token called "NFTa token" which is based on Ethereum Blockchain standard protocol called ERC-20 which was issued first with market cap of 100,000,000 tokens. The current circulating cap is 15 million with the current market cap of 450,000 dollars having 1 NFTa token = 0.03 dollars. The ecommerce business model followed by NFTA is P2P.

NFTA auction and loaning both operates currently on Binance Smart Chain (BSC) which is a cross chain protocol of managing smart contracts. These smart contracts are based on Ethereum protocols which holds all information of NFT. The company has plans of auctioning with NFTs created on other protocols in coming futures.

NFTA auction platform held platform of all the NFTs to determine their market value as the price and value are subjective, whereas loan market is place to loan the NFT owner instead of making owner wait for right price, in exchange of some collateral. Since NFT price in subjective, for the loan, terms and conditions varies.

Talking regarding the product design of NFTA, there is a front-end which is web based where user and sellers interact with backend which is based on SOTA (A multi-chain digital content NFT P2P platform). SOTA is a similar platform created for same purpose with other company. NFTA have same backend, which enables the NFTA NFTs holders to sell and buy from their platform too.

NFTA auction enables owners of NFTs created on BSC to be auctioned on platform. Once approved by admin, the platform lets buyers to bid for limited time. Once the auction is completed the winner gets the NFT and rest of the participants claim their deposits which were stacked till then. All the transaction are performed via NFTA tokens.

For loan market, NFTA platform provides two types of loan facilities. One is marketplace lending while other is Pool lending. In marketplace lending, the owner places an approved NFT for lending and get offers from lenders. Based on the conditions owner accepts any one lending offer. On acceptance of offer, the owner NFT is transfer to lender and lender pays some amount of NFTA tokens for agreed time frame. On the completion of time, owner has to return the amount along with interest and receive the NFT. On failure of return of money, the loan will be stated as default and the owner will lose the owner ship of collateral.

In pool lending, owner and lender don't have to wait for offer to get or accepted. They can lend or borrow directly from the pool and get NFT or money based on the value which is calculated by the NFTA platform.

Company has plans of having app in future, so that users can create NFTs easily from phone. Further they will be adding non crypto assets like cash to buy and sell NFTs via PayPal or credit cards. All these features are voted by the owners of NFTA token.

Axie Infinity [2]

Axie Infinity, the game who has been ranked #1 game based on Ethereum blockchain by active users, has generated revenue of over $16,000,000. The gameplay is adventure, strategy based game where users plan their species in efficient way to earn SLP token. In beginning of the game, users have to buy Axies from the

marketplace, which have been put on sale by other users. Each Axie has its own characteristics. User can breed their axies to have offspring which can be used in mission or for selling. All the game resources like characters, tokens and land are tokenized meaning users can sell these items or resources on open P2P markets.

Since the involvement of AXS, the company will soon be a totally community owned centralized organization as the owner ship of AXS by the company is reducing timely. Currently the blockchain stack of Axie Infinity Token is that axies and LP are based on Ethereum blockchain which is bridged with loom network sidechain which deals with all the lands, items NFTs etc.

The company is developing a dedicated sidechain linked with Ethereum called RONIN. The main reason behind this transition is that in current Ethereum chain, the gas fees is extremely high. The gas fees is deducted at several stages i.e. from breeding, hatching egg, raising the egg to adult Axie. This cause the Axie prices to rise as cheapest Axie currently is around $300. RONIN will eliminate the gas fee. Along with it, the scalability of game on current congested Ethereum network is hard, slow transaction approvals like taking up to 10 minutes for a single transaction approval. Ethereum side chain like RONIN will solve these issue. Since the company is planning to have staking of its token, AXS, Ethereum will charge a lot of gas fee for claiming and voting which is around 10$ - 50$, side chain like RONIN will be less costly for community to interact.

The Axie Infinity is quite booming game entirely based on blockchain has gathered the mass attention and got partnership with various brands like Samsung, HTC, Binance, Ubisoft etc. The company is planning to have an Android/IOS based game in upcoming months along with staking of AXS.

Blockchain disruption and decentralized finance: The rise of decentralized business models [5]

The financial system of current era has been mostly held by any organization, government, or some group of companies. Since we have moved to digital economy, the financial technology (FinTech) has eliminated the hold of institutions over the financial system but the role of intermediaries are still prevailing in system. The basic idea of introduction of intermediaries was to reduce the transfer cost along with establish connections, negotiate contracts, or enforce agreements. But these intermediaries keeps dominating the system, being centralized, can control or manipulate the system.

So decentralized Finance or DeFi was introduced. It being **decentralized**, resulting in no intermediary in hold or power to manipulate power. Being open-source, DeFi allow many developers to bring new **innovations** as it requires **no permission** to develop applications based on open-source infrastructure. **Combinatorial innovation** can speed up the speed of financial innovation along with increasing the competition, potentially leading to newer, better, and cheaper financial services. DeFi also brings huge **interoperability**. Currently cross blockchain products cannot execute transactions, but intra-blockchain applications have high interoperability. Polkadot blockchain is minimizing this by providing cross blockchain communication. DeFi is also **borderless**, not limiting to any country or geography. Lastly, DeFi offers **transparent** system which is due to the fact that all the ledgers are public on blockchain.

DeFi follows currently the decentralized model based on currency, payment services, funding and contracting. As the fiat currencies of every nation used to be backed by gold which is not the case in current era. So fiat currencies has the risk of being inflated. But DeFi will also never lead to inflation as the Max supply of decentralized blockchain based currencies is fixed. These currencies are also borderless meaning they can directly be stored or traded without involvement of any central entity. Along with it, DeFi offers **decentralized payment** services which results in low gas or transfer fees. Due to cheaper, faster transfer, a lot of centralized finances intermediators are partnering with DeFi. The biggest example is MoneyGram has partnered with Ripple (XRP is the 6^{th} crypto coin based on its market cap which is $35B).

One of the new trending business model proposed by DeFi is about fundraising called ICO (Initial Coin Offering). ICO is the new unregulated raising of funds in which the startup perform private or public sales to

the public investors, in exchange of crypto tokens. Investors buy these pre-sale tokens or services in exchange of any existing crypto coin. ICO enables global fundraising without any middleman or intermediaries. This approach is being adopted my many non-crypto companies like Telegram, which has raised $ 1.7B back in 2018 on its pre released token called TON (Telegram Open Network).

DeFi has a lot of impact but it also has some limits currently. Keeping the ledgers public, distribution causes high cost. Along with it, the transaction details are public which are encrypted by few blockchains but it also increases the processing cost. Lack of accountability is also one of the biggest issue in DeFi as they aren't regulated by any law or body so no one is responsible for any mishap.

Consensus Algorithms in Blockchain-Based Cryptocurrencies [6]

Blockchain's first financial application i.e. cryptocurrency is decentralized finance which has no intermediary between transaction and any use of cryptocurrency. Hence, to filter out the any invalid or faulty transaction or change to blockchain, a consensus system is introduced which isn't based on any centralized method. Blockchain has P2P network whose all nodes are distributed yet synced which each other. Blockchain as name shows is the chained network of interconnected blocks. These blocks contain information like their **version number** which shows the validation rule of that block, **parent hash** which is hash of previous node, **merkle tree hash**, **block hash**, **nonce** which is a random number used for authentication purpose, difficulty which is time taken to add new and **timestamp** of creation of block.

After few transactions, a new block is added to chain which take some time depending on coin. Bitcoin new block is created in 10 minutes on average, Ether takes 15 seconds while ripple takes 1-2 seconds. The major problem called Byzantine Generals problem arises here whose main idea is to deliver a message to some distant people before performing activities and getting confirmation. We can interpret it in language of blockchain as getting the confirmation about validation of block from nodes before adding that block to the ledger. This issue is solved by using consensus algorithms.

First algorithm is used by bitcoin called PoW (Proof of Work). PoW works in the way that each node has to perform some complex brute force calculations which uses huge energy and provide answers to network server. Those node who provide right answer are rewarded. If 51% of the nodes have provided right answer meaning that block is valid. Hence transaction is approved and added to block. Same process is held for creation of block. The network adjust the complexity based on load, number of nodes and power in such way that it takes 10 minutes on average to create a block. The two major problems with PoW are that this process is highly power consuming which make it expensive. Secondly if a group manager to acquire 51% nodes they can approve any transaction and block which will add faulty blocks to ledger. These attacks have been encountered earlier few time.

Second algorithm is used by Ethereum 2.0 called PoS (Proof of Stake). PoS works in the way that instead of using power intensive calculations, nodes stake coins. Staking means that nodes lock few ethers to network and participate in validation. In order to forge a block to blockchain, few parameters play role like amount of ether staked, how long they are staked and randomization in other to keep the chain decentralized. Only limitation of PoS is that the attacker must have to own 51% of the crypto currency which is highly unlikely.

Another algorithm which is based on centralized oriented approach which is called Practical Byzantine Fault Tolerance (pBFT). The main idea is to divide the nodes in secondary and primary nodes. Primary nodes receive the requests and forward it to secondary nodes. The block or transaction is validated if 67% of nodes approve it.

Since blockchain is booming, these algorithms are getting better and more secure day by day. These algorithms define speed, security and reliability of blockchain. Since Ethereum work on low power intensive algorithm, a lot of new blockchains applications are adopting Ethereum. Currently 87% of the DApps are using Ethereum block chain.

Toward Privacy and Regulation in Blockchain-Based Cryptocurrencies [7]

Blockchain integrity is depending in its hash, its digital signature attached by every node consensus algorithm. These things are important part of network as whole network is decentralized. This framework has numerous advantages. Guarantees that members settle on community choices. Likewise, this permits them to join or leave. A few instances of cryptocurrencies incorporate Bitcoin, which was dispatched in 2008 and has acquired a great deal of acknowledgment all throughout the planet. Furthermore, by utilizing public keys to keep up with security, they can utilize quite a few public keys without uncovering the genuine characters of participants. Nonetheless, Bitcoin might have a few limitations. It utilizes the address linking and merges multi-entry transactions. Transaction violation might be another infringement of your security.

In any case, a few approaches that assist with keeping the protection of cryptocurrencies flawless include: once accounts, centralized mixing, decentralized mixing, and exchange sum camouflage. Centralized mixing is way to accomplish protection, and its fundamental goal is to accomplish obscurity. When clients contribute their assets and afterward converge with other clients' assets, all subsidizes will be gotten back to another location to guarantee that the first source isn't leaked.

Moreover, decentralized mixing, otherwise called Coinjoin, is another approach to assist with keeping up with client protection. All ledger are consolidated, and all assets are blended in with the joined signatures, all things considered, guaranteeing that the info of the payer's particular payee stays covered up. This approach is typically predictable with Bitcoin. Furthermore, hiding the transaction amount is another way to regulate privacy that is, hiding the identity and the amount of the payment.

Let’s consider Altcoins Dash is the initial security upgraded cryptocurrency, a changed variant of Bitcoin, which utilizes secrecy to acquire protection. Likewise, it additionally consolidates the Master node network with a high level of compatibility. Furthermore, there is Zero coin, which utilizes a decentralized laundromat. In the wake of picking the base currency, clients are approached to pick an uncommon chronic number and an irregular number to arrive at a tradeoff. Zero cash is another technique intended to conceal public keys and exchange sums. What's more, Monero is a security cognizant cryptocurrency. It utilizes the Crypto Note convention, so you can flawlessly execute exchanges by making a key pair that is just utilized once. Also, confirmed moment private exchanges are joined with test conventions to accomplish security. On the edge, the new name of Dark Doge Coin infers low exchange expenses and obscurity.

Nonetheless, anonymity is viewed as a key component in keeping up with security and can at times be too disliked on the grounds that it might abuse unofficial laws. Some confidential or illicit exchanges are done too under the privacy of anonymity. Programmers likewise use cryptocurrencies to acquire illicit assets. In spite of the fact that anonymity and guideline have all the earmarks of being two totally different parts of cryptocurrency, they likewise give off an impression of being basic. In this manner, it is as yet important to discover an answer for organize these two perspectives. One approach to conquer this issue is being traced, which empowers bunch signatures. Here, the gathering head shapes a gathering and allocates a key pair to each and every individual who has a place with the gathering. The payer can play out the mysterious signature of the exchange here, and just the gathering executive knows the genuine character of the payer. Other potential arrangements incorporate the utilization of key age, exchange age, and payer following. The private key is followed here by the following organization to interpret the code text in the exchange.

Works Cited

[1] Q. Wang, R. Li, Q. Wang and S. Chen, "Non-Fungible Token (NFT): Overview, Evaluation, Opportunities and Challenges," *ArXiv*, vol. abs/2105.07447, 2021.

[2] Sky Marvis, "Axie Infinity: Official Axie Infinity Whitepaper," Sky Marvis, 15 December 2020. [Online]. Available: https://whitepaper.axieinfinity.com/. [Accessed 1 August 2021].

[3] F. Schär, "Decentralized Finance: On Blockchain and Smart Contract-Based Financial Markets," *Federal Reserve Bank of St. Louis Review,* vol. 103, no. 2, pp. 153-174, 2021.

[4] NFTA, "NFTA: A cross-chain NFT Auction and Loan Platform," NFTA, 2021.

[5] Y. Chen and C. Bellavitis, "Blockchain disruption and decentralized finance: The rise of decentralized business models," *Journal of Business Venturing Insights,* vol. 13, no. e00151, 2020.

[6] R. Yousuf, Z. Jeelani, D. A. Khan, O. Bhat and T. A. Teli, "Consensus Algorithms in Blockchain-Based Cryptocurrencies," in *2021 International Conference on Advances in Electrical, Computing, Communication and Sustainable Technologies (ICAECT)*, 2021.

[7] Y. a. S. W. a. Y. G. a. Y. Y. a. D. X. a. L. D. a. G. N. Li, "Toward Privacy and Regulation in Blockchain-Based Cryptocurrencies," *IEEE Network*, vol. 33, no. 5, pp. 111-117, 2019.