Ellen Wei
December 5, 2022

ECON 19: Financial Architecture of the United States

Course Paper: Research on crypto currencies, in particular on the Ethereum platform

In 1982, American cryptographer David Chaum published a paper titled “Computer Systems Established, Maintained, and Trusted by Mutually Suspicious Groups”. This would mark the beginning of a new financial system and alternative currency, the “future of money”: crypto currency. In 1983, Chaum invented eCash, an encrypted system of money and 3 years later, Chinese computer engineer Wei Dai formally established the idea of the decentralized cryptographic payment system. However, this idea of crypto payments did not become popular until the economic crash of 2008, where there was significant contraction of liquidity in global financial markets due to the collapse of the US housing market. This was also known as the “subprime mortgage crisis”. The value of paper money plummeted globally, and some turned to a new form money, immune to the traditional ideas of centralization.

Decentralized finance (DeFi) became a centerpiece of conversation to remove third parties and centralized institutions from financial transactions through stablecoins, software, and hardware. The peer-to-peer (P2P) financial networks could meet an individual’s loan needs using an algorithm that matched peers that agreed on the lender’s terms. Hence, it eliminated intermediaries and increased accessibility, presented lower fees and high-interest rates, more security, transparency, and autonomy. Yet, there are negatives to this structure: participation is complex and not easily understood due to the advanced technology, there exists risk of fraud and scams as demonstrated by past events, and a high level of volatility. The future of DeFi, if left untouched, is an unregulated ecosystem filled with infrastructural mishaps and hacks. Fortunately, developers have been finding new ways to address these problems. The unregulated nature of the system does bring up other critical questions: Should DeFi be regulated? If so, what regulations could be enforced and how? Who is responsible for investigating a financial crime that occurs across borders, protocols and DeFi apps? These questions will be discussed later in this paper after an examination of some existing systems.

Many companies invented their own cryptocurrencies to buy their specific products, known as tokens. These tokens operated like tickets, only for use in the establishment that issued them. This prompted interest from investors. These tokens could be traded for profit, similar to real-world trading currencies. Currently, more than 10, 000 different cryptocurrencies are traded publicly, and this number only continues to increase as more firms offer Initial Coin Offerings (ICOs). The leading cryptocurrency by market cap is Bitcoin, which drew influence from previous gold-influenced tokens, with a proposed scarce supply of 21 million bitcoins. The main takeaway is that cryptocurrencies do not generate money in a traditional sense and just a way of moving money. To make a profit, someone must pay more for the currency than they did.

Ellen Wei
December 5, 2022

In October of 2008, Satoshi Nakamoto (presumed pseudonym, identity unknown) published a white paper outlining his vision for the first true cryptocurrency, Bitcoin. In January of 2009, Satoshi Nakamoto and Hal Finney, a cryptographic activist and developer, performed the world's first digital currency transaction. In October of 2009, the first Bitcoin exchange opens a service to buy and sell digital currencies. The applicable rate of exchange from Bitcoin (BTC) to US dollar was determined by the cost of electricity consumed by the user's personal computer to mine the cryptocurrency. In February of 2010, users negotiated the first Bitcoin transactions informally via online forums. It was not all smooth sailing, however, as the largest Bitcoin exchange Mt. Gox suffered a major security breach in 2014 where hackers stole 850,000 BTC. This signified that technology for crypto wallets were still immature, and there did not yet exist any insurance protections or centralized crypto exchanges, which are now standard. Afterwards, Bitcoin experienced a surge of popularity in 2017-2018 where it soared to hit $20,000 but then fell into a "crypto winter". Developers were divided on how to scale the Bitcoin network and some created Bitcoin Cash while loyalists proposed a special settlement layer on top of Bitcoin, later known as Lightning Network. Non-fungible tokens (NFTs) were also created as unique digital collectibles. Projects like decentralized exchanges (DEXs) were developed on Ethereum. In 2020, crypto returned and Bitcoin topped at almost $70, 000 per coin. Notably, El Savador made Bitcoin a legal tender. In the current year of 2022, crypto has suffered significant blows, such as when TerraForm Labs' US dollar stablecoin UST fell to $0. Nevertheless, the crypto market has retained its $1 trillion market cap.

Bitcoin uses a census mechanism called proof-of-work (PoW) to verify transactions. The initial concept was introduced with "hashcash", a failed '90s project whose original purpose was to cut back on spam emails. PoW forces computers to solve algorithms to post new transactions on the blockchain. The blockchain network is a digital database or ledger that is distributed among the nodes of a peer-to-peer network. A blockchain collects information in groups. These are known as blocks and once the storage capacity has been reached, they are closed and linked to the previously filled block, hence a blockchain. This data structure makes an irreversible timeline of data, given an exact timestamp, permanently recording transactions, and making them viewable to everyone. The blockchain network generates a public key and a private key. The public key is the user account number, and the private key is a secrete number that serves as a signature when transactions are being processed. The network handles transactions through the computing power provided by users, which is known as cryptocurrency mining. The program finds a block in which transactions are stored when solving a complex task where the "solution" (hash value) contains parts of the previous blocks. The hash value of previous blocks always forms the basis for the new block, so if a cryptocurrency miner finds a new block, they can earn bitcoins. Thus, new coins or tokens are generated. The blockchain system is a pure peer-to-peer (P2P) network where each unit can be removed without affecting other organizations. Messages are distributed quickly with the flooding algorithm that ensures all recipients receive information. If transactions with mismatched keys

are submitted, the transaction will not be acknowledged by the clients and processing fails automatically.

In 2015, Ethereum was launched. Ethereum an open-source, decentralized software platformthat uses blockchain technology to enable smart contracts and cryptocurrency. It has a native coin that is known as Ether (ETH). Developers can build solutions and applications on Ethereum as a base- in fact, it can be used by anyone to create any secured digital technology. Before Ethereum, non-Bitcoin crypto projects were mostly peer-to-peer payment systems with slight technical tradeoffs. Ethereum sought to decentralize the internet and rose to become the second largest cryptocurrency.

Central to this platform are smart contracts which can be used to pay for goods and services through smart contracts. Smart contracts are automatic and self-executing agreement that operates without the need of a central authority or rent seeking third party. They are digital agreements whereby each party inputs several predetermined conditions or provisions that must be completed for the contract to be executed. They are used to ensure each transaction is legitimate, transparent, and trustless. Thus, they are faster, more secure, and more efficient than traditional central methods, abiding to the statement “code is law”. Some use cases in DeFi applications (DApps) are the facilitation of exchange of goods, services, data, funds, payments, and supply chains. The main issue is that the processing of external data needs to be verified. This issue has been addressed by utilizing data-oracle platforms such as Band Protocol, which provides access to trusted, verified data from multiple sources.

In September 2022, Ethereum changed from a proof-of-work (PoW) method to a proof-of-stake method. The Ethereum blockchain was written in the Solidity programming language. The blockchain is validated by a network of automated programs that reach a consensus on the validity of transaction information. The network of participants, validators, create new blocks and work together to verify the information they contain. The blocks contain information about the state of the blockchain, a list of attestations (a validator's signature and vote on the validity of the block), transactions, and much more. In this way, proof-of-stake does not require mining, which is energy-consuming computing, to validate blocks. It uses a finalization protocol called Casper-FFG and the algorithm LMD Ghost, combined into a consensus mechanism called Gasper, which monitors consensus and defines how validators receive rewards for work or are punished for dishonesty. To activate their validation ability, solo validators must stake 32 ETH while individuals can stake smaller amounts but are required to join a validation pool and share rewards. The validator creates a new block and attests that the information is valid (attestation), where the block is broadcast to other validators (committee) who verify and vote for its validity. Validators who act dishonestly are punished, where their staked ETH is removed. This is known as a decentralized autonomous organization (DAO).

Noteworthily, the amount of ETH is unlimited in contrast to the cap on number of Bitcoins. It is only limited by the time taken to process a block of ETH. Currently, there exists more than 122 million units. The future of Ethereum includes the development of “sharding”-

dividing the Ethereum database amongst its networks. This is similar to the notion of cloud computing. These smaller sections are called shards and allow more validators to work at the same time, reducing time to reach consensus. Ethereum also set a stage for other new items and methods. NFTs created using Ethereum introduced tokenization: giving one digital asset a specific digital token identifies and stores it on the blockchain. This establishes ownership, can be traded, or sold and is viewed as a transaction. For example, sports fans can buy and trade sports token, treated like trading cards.

DeFi has become increasingly popular and have already begun disrupting existing industries in traditional finance, such as borrowing, lending, insurance offerings, trading, and credit card use. By-passing the middlemen, the landscape of lending and borrowing have drastically changed. Users are no longer required to provide personal information and retain complete self-custody of their assets. The security of lending is assured by the over-collateralization of loans, addressing concerns of potential default of repayment and excessive volatility of cryptocurrencies as collateral. Users supply and lock their funds into smart contracts from where other users may borrow them under a certain interest payable. In 2021, the growth in Total Value Locked (TVL) rose from $7.1 billion to $46.8 billion, a 559.2% increase.

The P2P marketplaces, Decentralized Exchanges (DEX), maintain pools of different assets, handling the pricing and distribution of these assets in an automated way based on supply and demand. In this way, P2P refer to peer-to-contract with a liquidity pool rather than peer-to-peer. This acts as an alternative to traditional banks and Fintech products. In the future, these establishments may be entirely replaced in favor of trusted, secure technology.

Cryptocurrency has been gaining attention but has its share of issues. In November of 2022, FTX Exchange, a leading centralized cryptocurrency exchange filed for bankruptcy. The collapse was cited as a result of “a complete failure of corporate control”, with investigations still ongoing. FTX’s collapse dropped the value of the volatile crypto market, and a class-action lawsuit was filed alleging that FTX was built on a fraudulent cryptocurrency scheme. Decentralized finance is being viewed in a more positive light considering this event. Some may argue that rather than depending on human intervention and possibly faulty regulation, we can look to technology to provide security. However, the inherent anonymity and risk of DeFi makes it difficult to determine where and if governments can effectively implement safe practices. In this way, a transparent set of policies must be outlined, but intervention should not be made possible. International governments and economies need to consider how to incorporate DeFi as a stable alternative in times of volatility, such as in a recession.

Ellen Wei
December 5, 2022

Citations

"A Brief History and Overview of Cryptocurrency." *A Brief History and Overview of Cryptocurrency - Cyberlaw: Difficult Issues Winter 2010*, https://cyber.harvard.edu/cyberlaw_winter10/A_brief_history_and_overview_of_cryptocurrency.

"History of Cryptocurrencies: Cryptocurrency Investing." *Precious Metal Investing | Cryptocurrency Investing*, 8 June 2020, https://www.harvardgeo.org/history-of-cryptocurrency/.

CoinMarketCap. "A Dive into Smart Contracts and Defi: CoinMarketCap." *CoinMarketCap Alexandria*, CoinMarketCap, 12 Jan. 2021, https://coinmarketcap.com/alexandria/article/a-dive-into-smart-contracts-and-defi.

Person. "History of Cryptocurrency: The Idea, Journey, and Evolution." *Worldcoin*, Worldcoin, 29 Nov. 2022, https://worldcoin.org/articles/history-of-cryptocurrency.

Rawcut. "Defi: Blockchain Potential to Disrupt Traditional Finance." *Digitalwaves*, https://www.digitalwaves.com/learn/news-insights/defi-blockchain-potential-to-disrupt-traditional-finance.

Sharma, Rakesh. "What Is Decentralized Finance (DEFI) and How Does It Work?" *Investopedia*, Investopedia, 22 Sept. 2022, https://www.investopedia.com/decentralized-finance-defi-5113835.