Ethereum

Manuel F. Moreno

1 Summary

My paper is going to be about the cryptocurrency Ethereum. Its history, a high level technical explanation of how it works, and some of its applications. The intended purpose is to educate my audience about what Ethereum is and how it works; while also educating the reader on why its interesting. The intended audience is people who are interested in technology, have some very basic understanding of how code works, but may have little to no understanding of cryptocurrency. I chose to use IEEE format for my project.

2 INTRODUCTION

ETHEREUM is an open source computing platform and operating system.

2.1 Why Should I care about Ethereum?

2.1.1 Ethereums Value Proposition

In order to understand why you should care about Ethereum; you must have a rudimentary understanding of what the technology is and why it is important. Ethereum is a relatively complicated technology which solves a complex issue. Ethereum aims to create a decentralized and censorship resistant financial system. A financial system with little to no barriers to entry and permissionless leverage.

2.1.2 A Brief History of Crypto-currency and Ethereum

Ethereum is a rather ambitious project with a lot of history, philosophy, and game theory backing it. The ideas which lead to the formation of the Ethereum project go as far back as the early cypher-punk movement of the 1980's also more importantly the early 2010's crypto-currency community. The so called cypher-punk community was comprised of people who advocate for the widespread use of strong cryptography and privacy enhancing technologies as a route to social and political change. With increasing corporate censorship and a trend towards restrictions on free speech, cryptographic privacy is becoming a mainstream topic. Bitcoin was invented to be a hedge against inflation and the devaluation of fiat currency. The early 2010's crypto-currency community which formed around bitcoin began after the 2008 financial crisis. Essentially Bitcoin was intended to be a decentralized, deflationary, global reserve currency similar in many ways to Gold. Bitcoin launched on January 3rd 2009. It was created by an anonymous individual known as Satoshi Nakamoto who invented the Blockchain data structure. The Blockchain is the basis for how the majority of all cryptocurrencies work; it is essentially a way to keep an accurate ledger of transactions amongst a distributed network of computers. Without the need for trust amongst any agents in the network of computers. Ethereum is an experiment in pseudo-anonymous cryptographic currency similar to bitcoin but with far more applications and possibilities. Ethereum is not just a coin that can be bought and sold like bitcoin. It is also more importantly a decentralized distributed computing platform and operating system not just a currency. In short Ethereum is a currency that is: not controlled by any government, censorship resistant, and Turing Complete. Ethereum is basically programmable money.

2.2 Why Do Developers Use Ethereum?

Decentralising the financial system could change the world as we know it and somewhat already is. There are potentially unlimited decentralized applications that can be built on the Ethereum network. Anything that can be coded which needs to be censorship resistant and on a distributed network can be with Ethereum Smart Contracts. The invention of block chain ledger technology has taken the world by storm in just a little over 10 years. The various blockchain networks have reached over a trillion dollars in market capitalization or almost 1 % of golds market capitalization. Any person can create a project and have it hosted on the Ethereum network.

2.3 What is Decentralization and Why is it Important?

Decentralization is a property of a system. In general if a system is decentralized it means that there is no single authority that controls the consensus of the network or group. There are philosophical and political reasons for people to believe in decentralization. Those who argue for decentralization in these regards believe that central authorities will never be as efficient as the consensus of a group with a common goal and aligned incentives. However, there are a few practical reasons that are detached from such ideological idealism. With regards to the the application of decentralization in software here are a few reasons.

2.3.1 Fault tolerance

Decentralized systems are less likely to fail because they have many separate components that don't rely on each-other [5].

2.3.2 Attack resistance

Decentralized systems are more difficult to attack and manipulate. Since there is no single point of failure unlike a centralized system [5].

2.3.3 Collusion resistance

It is much more difficult to collude in a decentralized system than it is in a centralized system. It is much easier for government figures in a centralized power structure to collude, for instance, since they are single points of failure [5].

2.4 Ethereum's Blockchain

Now that we have a cursory understanding of some of the history behind block-chain technology we can dive into how it works.

2.4.1 understanding Blockchain

A Blockchain is essentially a type of database. The reason why it is called a block-chain is because, it is a chain of blocks. Blocks are essentially nodes in a linked list of transactions on the network. These nodes contain transnational data from within a certain time period. The difference between a database and a Blockchain lies in the fact that a Blockchain is a database that is propagated by a peer-to-peer network of computers that are ran by random anonymous users who want to participate in the network. Whereas a database is often a network of computers ran by a single entity. Participants in the network are incentivized by the blockchain to correctly update the next block of transactions and keep the state of the Blockchain accurate in hopes of getting a mining reward. Mining rewards are a share of the circulating supply of the block-chain from the network. A property of Blockchains is that as the network grows and the main chain gets longer the more certain the network can be that attacks on the network are too expensive to execute. This peer-to-peer network of computers runs a proof-of-work consensus algorithm to validate transactions on the Blockchain. The proof of work consensus-algorithm in the case of Ethereum works by having computers in the network try to guess the next nonce [8]. A nonce is essentially a one use password in cryptography. This works because the algorithm is sufficiently difficult, requiring high levels of compute, and the difficulty of finding the next block increases over time. The previously described consensus algorithm is the proof-of-work algorithm. Proof-of-work algorithms consume substantial amounts of electricity around the world as the network grows.

2.4.2 How does a Blockchain have value?

A common question people have is the following: "how does this have any real world value?". In order to understand that we have to look at what money actually is. Humans first started transacting for desired items by trading using a barter system. The barter system was simple: you can trade one item for another item that you think is of equal value. After the barter system came the invention of currency which was based on limited natural resources. You have some gold, silver, and or copper coins that you can trade for anything because, they're shiny rocks that humans decided have varying levels of value. After the use of coin humans invented paper money because carrying around heavy gold all day just isn't convenient and its expensive to protect. Governments started issuing slips of paper which were equivalent to some amount of gold. After this fiat currencies were created because, gold is a scarce resource and didn't allow for governments to create more money easily. Governments needed inflation which they could use for debt in case they wanted to pay for something which they could pay back at a later date. Centralized authorities or governments removed the paper slips backed by gold as the standard for the currency systems. After this currencies became based on nothing more than belief that the currency has value because, they say it has value relative to its circulating supply. A circulating supply which can change and actively changes every year based on the rate of inflation. De-

centralized crypto-currencies like Bitcoin and Ethereum are similar to gold in that their value is based on scarcity. The only difference is that Ethereum and Bitcoin are digitally scarce where as gold is physically scarce on earth. Bitcoin has a limited supply of coins. Ethereum does not have a limited supply of coins. However, a circulating supply change has to be agreed upon by the users of the network vis-à-vis governance. There are are disincentives for users on Ethereum to inflate the network since the price of their coins would go down. So there is a defacto limited supply for this reason. Ethereum in a sense is more honest than bitcoin considering that the bitcoin network could agree to change the supply at a later date as well if need be. This limited supply gives Ethereum a self fulfilling network effect where users want as large of a share of the network as possible because they believe or speculate that the network has value. Ultimately, it is belief that gives any currency value not just Bitcoin and Ethereum. After just five years from launch Ethereum has attained a total market capitalization of 215 billion at the time of writing this.

2.4.3 How does Ethereum's Blockchain work?

Ethereum uses a hybrid consensus model. There are essentially two proof of consensus algorithms that verify all transactions on the network. The proof-of-work algorithm mentioned previously where computers with expensive graphics cards try to mine the next block correctly by guessing the nonce of the next block mathematically. Then there is proof-of-stake which is another consensus algorithm. Proof of stake is much more efficient in terms of energy use and doesn't require the same level of environmental electrical costs that proof-of-work has. Proof-of-work requires significantly more compute power and electricity than proof-of-stake. Ethereum is transitioning from proof-of-work to proof-of-consensus completely by the end of 2021.

2.4.4 Proof-of-Stake

Proof-of-Stake is a distributed consensus algorithm that was first theorized in 2011 on the bitcointalk forum [8]. Proof-of-stake on the Ethereum network works by having a user lock up at least 32 Ethereum as collateral to run a validating node on the network. The higher the size of the users stake the higher their node has a chance to validate a block which results in a reward. The reward is a greater share of the tokens on the network, users receive more Ethereum for staking. Users have an incentive to also not take their nodes off the network because having their tokens unspent (not involved in a transaction) for longer periods of times increases their probability of getting a block reward for staking. Proof-of-Stake prevents double spending from 51 % attacks. The 51 % of attack is when a user is able to double spend and change the Blockchain database because they control most of the compute. Proof-of-Stake prevents this attack because a user is disincentived to crash the price of an asset that they control 51 % of the price of. Also its an astronomical amount of money that most nations on earth do not have because the buying would keep pushing up the price so it is not really possible for someone to get 51 % of the tokens. Proof-of-Stake is a secure consensus mechanism that Ethereum has been using to phase out Proof-of-Work. Sometime during 2021 Ethereum will fully phase out Proof-of-Work in its Ethereum 2.0 update. This will reduce the emissions cost of the global network significantly, which is good for the environment and the strength of the network.

2.5 Ethereum Smart Contracts

2.5.1 What are Smart Contracts?

Smart contracts are self-executing contract between a buyer and seller. Smart contracts are written directly as code and distributed over a decentralized network. Smart contracts enable anonymous users of a network to have trusted agreements without the need for for a centralized third party such as a legal system. Smart contracts were first conceived and defined by the computer scientist Nick Szabo in 1997. Ethereum is the first project to implement this idea successfully. The Ethereum network currently has a total market cap valuation of 215 Billion Dollars. Most of the original funding for

the Ethereum project came from a 100 thousand dollar Peter Thiel fellowship grant, given to Vitalik Buterin the founder of Ethereum in 2014.

2.5.2 How do smart contracts work?

Ethereum smart contracts are programs that run on the Ethereum Blockchain. These smart contract reside at specific addresses and can be interacted with by other users of the Ethereum network. Smart contracts can define some rules and enforce them programmatically much like a normal contract [10]. The interactions with smart contracts are verified by the Ethereum Blockchain. These smart contracts are written in Ethereum's native language solidity and then compiled by the Ethereum virtual machine. Every transaction on the Ethereum network requires a fee which prevents possible attacks. Without fees for instance the creation of a bunch of useless smart contract could theoretically spam the network and slow it down until its unusable. However, there are fees on the Ethereum network and they're rather high so that can't really happen because an attacker would run out of money.

2.5.3 Ethereum Virtual Machine

The Ethereum virtual machine is a single operating entity that is maintained by thousands of machines and proof-of-stake nodes validating the network [11]. The Ethereum protocol exists to keep this continuous uninterrupted virtual machine running. A virtual machine is an emulation of a computer system; effectively it is a virtual operating system. The nodes in the network validate and compile code written on the network.

2.5.4 Solidity

Solidity is an object orientated programming language meant for writing smart contracts. It is Ethereum's native programming language. Since solidity is Turing Complete any application or program can be written in solidity and then compiled by the Ethereum Virtual Machine.

2.6 Ethereum Blockchain Complex Network and Anonymity

Complex networks theory allows us to analyze the Ethereum network, and to extract several mathematical properties that describe it. Complex networks theory is used to describe many phenomena mathematically [2].

2.6.1 Small World Networks

A small world network is a type of mathematical graph where there are a high number of nodes with a high degree of connections interspersed with nodes that have few connections. These small world networks create cliques or hubs which are nodes of the graph that are highly connected. Small World Networks are a negative thing in a decentralized system if the goal is to keep users anonymous. Although Ethereum is not a privacy centered coin it is somewhat important to keep the identity of users on chain at least pseudo-anonymous in order to keep the network censorship resistant.

2.6.2 Ethereum's Decentralization

Since Ethereum is a widely distributed network it contains many hubs. [2] Therefore, although all Ethereum accounts are anonymous. It is possible to deanonymize users if they interact with unpopular smart contracts or hubs in small world networks. Therefore Ethereum is pseudonymous which is fine considering there is still a layer of obfuscation which allows for addresses to be pseudo-anonymous. This makes it so not just any person can know the Ethereum balance of a particular user and their real identity.

2.7 Ethereum Scalability

The scalability of the Ethereum network has been at the forefront of concerns with the network since 2018 when it seen the price of gas fees (fee cost to transact on the network) skyrocket astronomically as large amounts of smart contracts and tokens were added to the network [1]. There are several proposed solutions to both layer 1 and layer 2 in order to scale the network. Ethereum Layer 1 is the protocol itself and layer 2 are the networks or side chains built

on top of the Ethereum protocol that are still verified by the main Ethereum protocol.

2.7.1 Layer 1 Scaling

The most important and popular layer 1 scaling solution for Ethereum is sharding. Currently the network has to sequentially work on every single transaction. With sharding the network would break these transactions into smaller datasets and increase parallelism. Effectively this would increase the overall throughput of the Ethereum network allowing transactions to scale to more users and reducing network fees by using the computation of the network more effectively [6]. Essentially it would improve Ethereums efficiency in dealing with data on its network.

2.7.2 Layer 2 Scaling

Layer 2 refers to off chain transactions. Essentially these are side chains which are blockchains that are built on Ethereum's but are not apart of the main network. These networks are however verified by the main Ethereum network. Proposed solutions here are zero knowledge rollups which are a type of cryptographic proof that allows hundreds of off chain transactions to be verified as a single transaction. This would greatly improve performance of the main chain as there would be much less data to process for the network while still maintaining a cryptographically secure implementation.

2.7.3 Scaling and Fees

Every transaction on the Ethereum network costs some amount of gas. Gas is the name for fees on the Ethereum network it is a fractional amount of Ethereum that is required to transact on the network. Currently gas fees on Ethereum have been at all highs since the rapid adoption of Defi by speculators in 2020. The layer 1 and layer 2 scaling solutions should help Ethereum to scale to more users and reduce fees significantly.

2.8 Ethereum Applications

As stated previously Ethereum is an open source computing platform and operating system. This open source computing platform and operating system allows for Open Source Decentralized Applications(Dapps) to be built on the network permissionlessly by anyone. Just five years after its launch there have been over a million Smart Contracts and hundreds of thousands of tokens created on the Ethereum block-chain.

2.9 Prediction Markets

Prediction markets on Ethereum were one of the first decentralized applications on the Ethereum network. The idea of a prediction market is essentially being able make bets on the outcome of future events. Augur is a betting platform or prediction market built on Ethereum. Users can bet any amount of Ethereum on anything; for example world events like the presidential elections have been bet on using the decentralized application. In the early days of augur when it was relevant in the crypto-currency community there was concern over the possibility of assassination markets. Since any user could bet on any event in the world. However, as we know Ethereum is a pseudo-anonymous network and the real identity of an address can most likely be figured out if the person interacts with an unpopular smart contract. These concerns ultimately turned out to not be a major issue.

2.10 Governance

Ethereum has allowed for a variety of governance models to be tested. Governance tokens were also among the first decentralized applications on the Ethereum Blockchain. Typically governance tokens allowed users to vote for changes to the Smart Contract and also even allowed users to vote on feature implementation to developers of the open source applications. Usually governance is one part of a protocol that does something more interesting because, governing a project that has no users or reason for users is just not worthy of someones time.

2.11 DeFi Decenteralized Finance

DeFi or decentralized finance is a broad term for describing a set of applications that are

designed to remove financial intermediaries. Financial intermediaries such as exchanges can also be single points of failure and lock people out of transacting on the network. Most of the DeFi applications on the Ethereum network were funded back in the 2017 initial coin offering craze which is a historic event in the crypto-currency community where speculative investors were spending hundreds of millions of dollars on projects that had nothing but a white paper and a team of developers to back them.

2.11.1 Why Defi?

The current financial system is inefficient. Settlement of financial instruments can take days and requires many humans intermediaries and a lot of bureaucracy to function. Banks have slightly improved in recent years for the end user with instant transfers of funds through third party companies. However, if you want to send something like a wire transfer, you have to wait for a weekday and it has to be sent before a certain time or else you have to wait until the next day. Not to mention that there are many unbanked people in various countries without access to any banks. There are also large inefficiencies and high costs associated with international banking. Finally there are very high barriers to entry for new financial companies which stifles innovation in the sector. Defi gives decentralized permissionless access to anyone in the world with an internet connected device. Allowing users to access well known financial services like: payment, lending, borrowing, and savings accounts.

2.11.2 Decenteralized Exchange

In finance an exchange is a marketplace where various financial instruments are traded. Exchanges are platforms which give the general public the ability to purchase stocks, securities, derivatives, and bonds. Much like the normal world of finance, crypto-currency exchanges have been centralized companies that provide a trading platform for the general public. However, Since crypto-currency is all about decentralization; developers have taken it upon themselves to leverage networks like Ethereum to build powerful layer 2 decentralized exchanges. A decentralized exchange is a Decentralized Autonomous Organization(DAO) that allows users to transact as they would on a normal centralized exchange except without the need for the centralized third party. These decentralized exchanges do not require any form of identification and require little to no human interference to run properly. One such exchange is uniswap which is a layer 2 Ethereum protocol.

2.11.3 Automated Market Maker

An Automated Market Maker(AMM) is an essential part of the decentralized exchange. In normal finance a problem arises when buying a stock that is low market capitalization and low daily trading volume because it is difficult to transact with since it has low liquidity. Liquidity is the ability to buy and sell an asset for cash easily. Automated Market Makers use liquidity pools which are crowd sourced amounts of tokens that are locked into a smart contract [12]. These crowd sourced tokens can then be bought or sold without the need for a seller. This works because the exchange allows the user to interact with a smart contract that contains the crowd sourced tokens. Thus Automated Market Makers give defi decentralized exchanges liquidity.

2.11.4 Borrowing and Lending

Smart contracts allow for permissionless Borrowing and lending. The way borrowing works by having users put up a certain amount of coins as collateral and then another user can lend their tokens for a certain interest rate like how normal lending works. Except this is all done by smart contracts and there is no need for trust between either party since you have to have collateral which could cover the loan. A protocol that handles this is AAVE which was a 2017 initial coin offering project that has grown 18000 % in market capitalization since its launch in 2020.

2.11.5 Savings Account (Annual Percentage Yield)

Similar to a savings account it is possible for users of crypto-currency to invest in and hold

stable coins which are coins that are equivalent to the dollar. On layer 2 platforms like compound which are Ethereum smart contract that algorithmically look for the best percentage yields and help users earn up to 8 % APY a year from holding tokens pegged to the value of the dollar. 8 % is a very high interest rate on a savings account considering current high yield is .4 % which does not beat the current inflation rate of 1.81 % at the time of writing this. This is all made possible by leveraging the defi ecosystem the yields come from lending out tokens to users and APY is variable overtime.

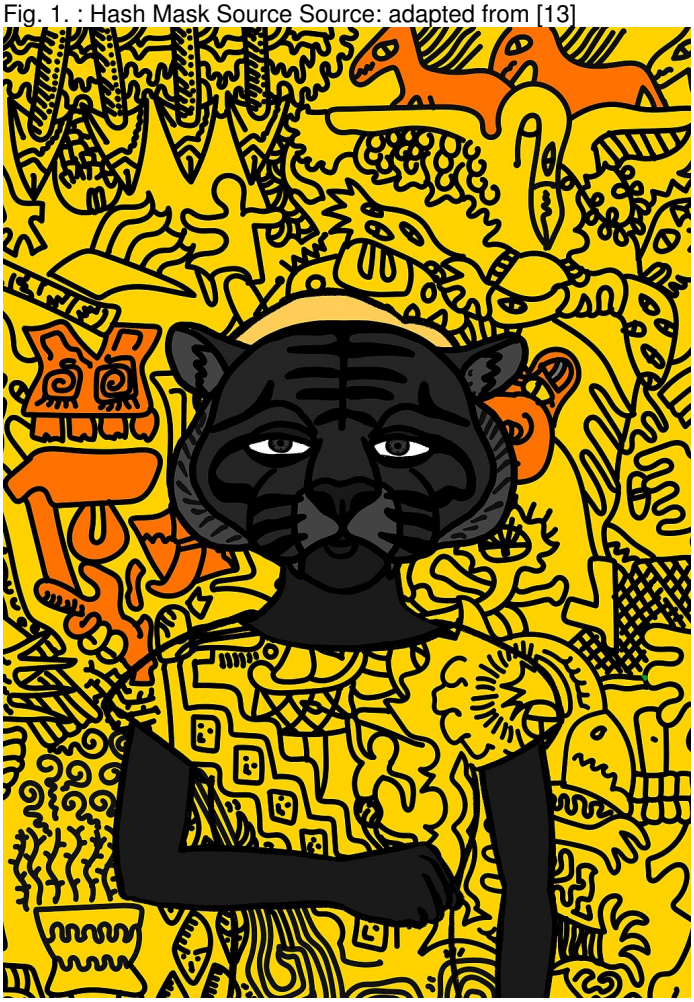
2.12 Non-Fungible-Token/NFT

A Non-fungible-token or NFT is a digital file with an ownership that has been verified on a Blockchain. Recently non-fungible-tokens have garnered mainstream attention because some NFT's are selling for absurd prices. An NFT's unique identity is verified by the Ethereum Blockchain with a smart contract. Below is an example of a Hash Mask which is a unique digital collectible some of these collectibles have sold for millions. Hash masks are a collection of 16,000 unique digital portraits with various rare attributes. There are currently no hashmasks worth less than 1 eth. ($1775 at the time of writing this)

2.13 Conclusion

Ethereum is a decentralized network, distributed Blockchain ledger, smart contract platform, and operating system. Decenteralized networks are a powerful tool for creating censorship resistant applications. Ethereum has several proposed solutions to many of the problems with the network that are currently being implemented. Ethereum's network is distributed enough to keep most users identities anonymous. Some uses of the Ethereum network are: Defi, Prediction markets, governance, and NFT's. Ethereum is interesting because of its premissionless and censorship resistant nature.

Fig. 1. : Hash Mask Source Source: adapted from [13]



REFERENCES

[1] M. Bez, G. Fornari and T. Vardanega, "The scalability challenge of ethereum: An initial quantitative analysis," 2019 IEEE International Conference on Service-Oriented System Engineering (SOSE), San Francisco, CA, USA, 2019, pp. 167-176, doi: 10.1109/SOSE.2019.00031.

[2] Gencer A.E., Basu S., Eyal I., van Renesse R., Sirer E.G. (2018) Decentralization in Bitcoin and Ethereum Networks. In: Meiklejohn S., Sako K. (eds) Financial Cryptography and Data Security. FC 2018. Lecture Notes in Computer Science, vol 10957. Springer, Berlin, Heidelberg.

[3] Ferretti, S, D'Angelo, G. On the Ethereum blockchain structure: A complex networks theory perspective. Concurrency Computat Pract Exper. 2020; 32:e5493. https://doi.org/10.1002/cpe.5493

[4] V. Buterin, "Ethereum Whitepaper," ethereum.org. [Online]. Available: https://ethereum.org/en/whitepaper/. [Accessed: 19-Feb-2021].

[5] V. Buterin, "The Meaning of Decentralization," Medium, 06-Feb-2017. [Online]. Available: https://medium.com/@VitalikButerin/the-meaning-of-decentralization-a0c92b76a274.

[6] "Layer 2 scaling," ethereum.org. [Online]. Available: https://ethereum.org/en/developers/docs/layer-2-scaling/.

[7] L. Conway, "Blockchain Explained," Investopedia, 18-Nov-2020. [Online]. Available:

https://www.investopedia.com/terms/b/blockchain.asp. [Accessed: 14-Mar-2021].
[8] "Proof-of-work (PoW)," ethereum.org. [Online]. Available: https://ethereum.org/en/developers/docs/consensus-mechanisms/pow/
[9] "Proof-of-stake (PoS)," ethereum.org. [Online]. Available: https://ethereum.org/en/developers/docs/consensus-mechanisms/pos/. [Accessed: 14-Mar-2021].
[10] "Introduction to smart contracts," ethereum.org. [Online]. Available: https://ethereum.org/en/developers/docs/smart-contracts/. [Accessed: 14-Mar-2021].
[11] "Ethereum Virtual Machine (EVM)," ethereum.org. [Online]. Available: https://ethereum.org/en/developers/docs/evm/. [Accessed: 14-Mar-2021].
[12] "Cryptopedia: Crypto Content Platform," Gemini. [Online]. Available: https://www.gemini.com/cryptopedia..
[13] Suum Cuique Labs GmbH, hashmasks. [Online]. Available: https://www.thehashmasks.com/detail/15753.