Ethereum: Introduction, Expectation, and Implementation

Qichen Huang

Economics University of Washington, Seattle, WA, USA

qhuang5@uw.edu

Abstract. As the Blockchain technology develops, more and more cryptocurrencies were invented after Bitcoin. This paper introduces the technology of Blockchain, including the basic concept of Blockchain and how Blockchain works to allow decentralization of trades; The system of Ethereum and the cryptocurrency Ether (ETH), how it was invented, what was the central mission of its invention, as well as how it differs from Bitcoin and how can it allow more decentralized application to be developed, which in turn illustrates what it means and where its values lie. As all cryptocurrency markets have a huge fall in value in the year 2022, as shown in figure 1, many people are losing faith in cryptocurrency. Many believe that since it is entirely digital and non-government based, it has no actual value, that the entire cryptocurrency market is a bubble. Meanwhile, cryptocurrencies introduce a very revolutionary concept, which is the decentralization of applications, and this decentralization can apply to many things, leading to a great technological structure modification, even for social structures. Because of its anonymous and democratic nature, there is also always going to be demand for cryptocurrencies. Thus, this paper also analyzes the expectations of cryptocurrency, mainly Ether, and the predictions of its future development.

Keywords: Ethereum, Ether, Blockchain, cryptocurrency, decentralization.

1. Introduction

In the Ethereum website, the official definition of Ethereum is "the community-run technology powering the cryptocurrency Ether (ETH) and thousands of decentralized applications." [1] According to Ethereum: Platform Review, The Ethereum platform was conceived to create a more generalized platform in November 2013. It uses proof of work to combine the notion of public economic consensus. With the power of a stateful Turing-complete virtual machine, it allows application developers to create applications that benefit from the decentralized and secure Blockchains with convenience, without needing to create a new Blockchain for every new application [2].

As Ethereum: A Secure Decentralised Generalised Transaction Ledger EIP-150 Revision pointed out, Ethereum is a project that aims to build the generalized technology, which all transaction-based state machine concepts may be built, as well as providing to the end-developer “a tightly integrated end-to-end system for building software on a hitherto unexplored compute paradigm in the mainstream: a trustful object messaging compute framework" [3].

As figure 1 shows, the price of the cryptocurrency market rose at a surprisingly high speed, and also crashed within a very short amount of time. This led people to rethink their perception and understanding of cryptocurrencies, as well as what to expect from them in the future.

Figure 1. The Ethereum Price from Ref [4]

In 2022, major cryptocurrencies such as Bitcoin and Ethereum are facing huge devaluation, with its price dramatically decreased within a very short amount of time. According to ETHEREUM'S PRICE IS DOWN! IS IT CALM BEFORE STORM IN 2022? "On the fifth day of the year, Ethereum's price fell below its resistance level of US$3,500, signaling an approaching slump in the cryptocurrency market." [5] Many claim that the cryptocurrency has always been digital and therefore does not hold true value. People have also been losing faith in cryptocurrencies as it seemingly operates purely on people's faith and expectations, that it is just a bubble, unlike gold which holds solid value and will never "disappear". In this paper, the technology of Ethereum is researched and analyzed to see what it truly is and means, thus determine whether it really has no value and is going to be worth nothing one day.

2. The Development of Ethereum

This section introduces a brief development of Ethereum, as well as illustrating the Ethereum ecosystem and how it works. Main concepts such as the Blockchain technology, smart contract, EVM, and Ethereum account are introduced.

2.1. The Blockchain Technology and Ethereum

The way most people understand currency and trade is that it is centralized, meaning it is issued, managed, and governed by an authority or a third party, such as how US dollars are governed by the Fed. In 2008, Satoshi Nakamoto published a paper which mentioned a revolutionary concept: it describes a new way of storing and distributing data among individual nodes with verifiable integrity, meaning that decentralized trade is made possible. This is the invention of the Blockchain technology.

It presents data as ledgers, which is a way which records the data when a transaction happens. In Ethereum for Dummies, it mentions that you can add data to this ledger only, after which you cannot change anything. Which means that the only two operations you can perform on this ledger are adding and reading data, which is known as the immutability property, and it is crucial for the technique to work [6]. The data added to this ledger is in blocks, hence the name "Blockchain". A blockchain is a continuous link of blocks, which are records of transactions, each contains information of the transaction data, timestamp, and cryptographic hash of the block in the front. When a new block is created with enough transactions, it is added to the ledger. One main feature is that once the block is added, the data in any existing block will not retroactively get altered. Unless all blocks that are subsequent are altered [7].

As the concept of Blockchain was proposed, cryptocurrency and Bitcoin were created right after. The cryptocurrency uses cryptographic hashes to ensure the integrity. As Bitcoin was known by more and more people, the Blockchain technology started to be implemented in more places. In 2013, a more functional implementation of Blockchain was proposed, which is the Ethereum Blockchain technology, which was later implemented and launched by the Ethereum Foundation in 2015. Like Bitcoin, Ethereum also has a digital currency Ether (ETC), and is also decentralized, without the governance of a central bank. Different from Bitcoin, Ethereum was not created just to exchange currency, it is programmable. In Ethereum's official website, the fact that it is programmable means that people can build apps that use the Blockchain to store data or manipulate the functions of the app. It generalized the Blockchain technology, which means people can do more, be more creative and innovative with the Ethereum platform. The Ethereum official website also presented a parable to point out the main difference between Bitcoin and Ethereum: "While Bitcoin is only a payment network, Ethereum is more like a marketplace of financial services, games, social networks and other apps that respect your privacy and cannot censor you." [1]

2.2. Ethereum Account and Smart Contracts

As mentioned in the second section, Ethereum is programmable. It allows everyone to set their own rules, transaction formats and state functions with its summarized layer. This is achieved by the

smart contract. In Ethereum official website, it states that smart contracts are fundamentally computer programs that are in the Ethereum Blockchain. When there is a transaction from a user or another contract, smart contract gets triggered and executed. They make Ethereum distinguishable from other cryptocurrencies as they make Ethereum flexible. These programs are also called decentralized apps, or dApps [1]. As introduced earlier, the Blockchain technology operates based on individual nodes, and each Ethereum node runs a copy of the Ethereum Virtual Machine (EVM), which runs the smart contract code and ensures all nodes have the same output.

As for Ethereum account, it is described in Hyperledger, Ethereum and Blockchain Technology: A Short Overview as "The Condition of Ethereum contains accounts with a 20-byte address and transformations for each account. The condition of the planet is a diagram between account and addresses." [8] The Ethereum account and currency exchanged will also be illustrated with more details in later sections. In figure 2, a simple illustration of a typical transaction is presented.

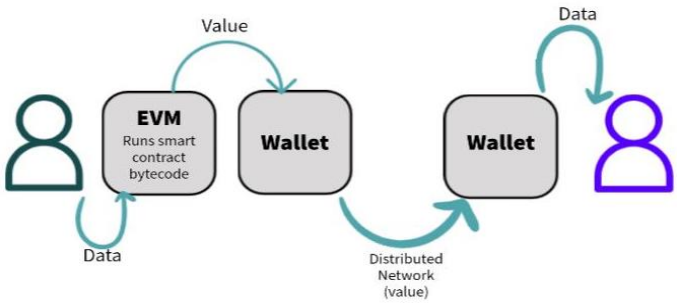

Figure 2. An Illustration of The Transaction

3. The Ethereum Technology

This section explains in more detail the technology behind Ethereum, including its ecosystem, how its account operates, process of smart contract, and the Blockchain technology.

3.1. Ethereum and Ether

Ethereum is a decentralized platform which aims to innovate in three key areas: currency assurance through Ether, Decentralized Autonomous Organization (DAO), and as mentioned earlier, smart contracts. Ethereum has several main features:

- Security. Since it is nearly impossible to tamper with the transactions within the blocks, it makes the transactions secure.
- Community support. Ethereum has established its user base as well as attentions from various individuals and organizations, thus it has a strong community support on many platforms such as Reddit, GitHub, and so on.
- Corporate-friendly structure. Many corporates can test and build applications based on Ethereum.
- Asset Issuance. It provides the potential to create assets on Ethereum Blockchain, which can be used as a currency, an identification, and other similar functions.
- Speed. Ethereum is also featured for its high processing speed, while Bitcoin requires a processing time of 10 minutes, Ethereum only needs a few seconds.
- Ethereum is uncensored. Its networks allow transparency to all transactions.

In addition to the main features, Ethereum uses multiple languages, including Solidity, Julia, LLL, Mutan, Serpent, Vyper, while the contracts are compiled into EVM bytecode and deployed to Ethereum Blockchain for execution. The fundamental block of Ethereum ecosystem is referred to as gas in Ethereum. It is paid for every operation performed on Ethereum Blockchain, and therefore is the crypto fuel for Ethereum, or the transaction fee that is paid when transferring to another party. Meanwhile, Ether is the cryptocurrency that fuels the Ethereum platform, and it is different from Bitcoin in several ways. Bitcoin uses secure hash algorithm (SHA-256), while Ether uses ethash algorithm; Bitcoin was designed and is mainly used for purchasing goods and services, as Ether is

designed for making decentralized apps; Bitcoin is priced much higher currently than Ether; Bitcoin is a currency created to compete with fiat currencies, while Ether is a token created for facilitating smart contracts; Also as mentioned in the main features, the transaction speed of Ether is much higher than of Bitcoin [9].

3.2. Ethereum Account and Smart Contract

There are two main types of Ethereum accounts which will be illustrated, externally owned accounts (EOA) and contract account. EOA's main features are: it is controlled by a private key, it has Ether balance, it can send transactions, and it has no associated code. Meanwhile, contract account has an Ether balance, it has an associated code, it is triggered by transactions or messaged, and it performs operations of arbitrary complexity. Contract accounts have smart contract code, which an EOA does not have. Because a contract account does not have a private key, it cannot initiate a transaction, but they can react to transactions by calling other contracts, building complex execution paths [10].

Smart contract is under the spotlight in the Ethereum world as it has several advantages: it is the simplest form of decentralization, it has a higher degree of security, it provides automatic agreement enforcement, it eliminates the need for a third-party, it turns legal obligations into automated processes, and it lowers the transaction costs, since the smart contract is self-verifying and self-executing, it is also cost-saving and tamper resistant. According to What Is Ethereum? | Ethereum Explained | Blockchain Tutorial for Beginners | Simplilearn? The process of smart contracts consists of three main parts: "An optional contract between the parties is written as a code in the Blockchain. The individuals involved are anonymous, but the contact is made through a public ledger", then "a trigger event like an expiration date or a strike price is hit, and the contract executes itself according to the coded terms", followed by "regulators can use the Blockchain to understand the activities in the market while maintaining the privacy of an individual's position." [10]

The language of the most popularity currently for writing smart contracts that run on Ethereum is Solidity, which is a language that was proposed in August 2014 by Gavin wood. Solidity is similar to JavaScript, with some influences from other programming languages such as C++ and Python, and the purpose of this language is to support operations that are Blockchain-specific with code that runs on an EVM. One key feature of Solidity is that it must enforce determinism, which means that the results must be uniform for all nodes running on this smart contract code with the same input [6].

3.3. The Blockchain Technology

According to Research Handbook on Digital Transformations, Blockchain technology can eliminate the double-spend problem from happening by using a public key cryptography, with each agent being assigned a private key kept secret and a public key publicly shared. When the receiver of the cryptocurrency sends their public key to the original owner, a transaction is initiated, and the cryptocurrency will be transferred by the digital signature on a hash. Public keys, as cryptographically generated addresses, are stored in the Blockchain, with each crypto coin associated with one address, and the transactions are essentially the trade of coins from one address to another. As mentioned, the Blockchain technology allows anonymity since the public keys are not tied to a real-world identity.

When talking about Blockchain technology, the concept of miners is often introduced, since Blockchain is a transactional record which is enriched by a subset of network participants, known as the miners, by solving difficult computational problems. When they compete solving mathematical problems in the most efficient way, therefore adding a new block, they receive a reward to their public address, and the miner will need to sign a private key in order to spend these rewards. The difficulty is adjusted to keep a reasonable mining speed, which is why before it could be solved by individuals with personal computers, but nowadays it usually requires a supercomputer to perform the calculations.

Blockchain technology relies heavily on hash and hash functions. As mentioned earlier, while Bitcoin uses SHA-256, Ethereum uses ethash. A cryptographic hash function is extremely difficult to

revert known as the “collision resistance” property of a hash [11]. Figure 3 shows the Blockchain structure of Bitcoin.

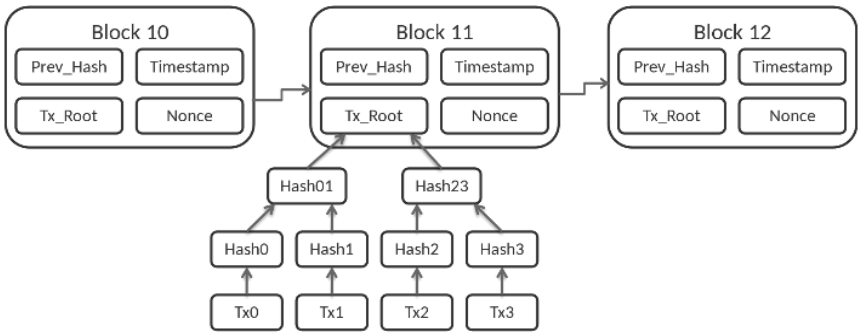

Figure 3. Bitcoin Blockchain Structure from Ref [14]

3.4. Data Structure: Patricia Merkle Tries

Patricia Merkle Tries, also known as the Radix Tries, is an important data structure in Ethereum used to store (key, value) bindings with cryptographic authentication. Patricia stands for “Practical Algorithm to Retrieve Information Coded in Alphanumeric”. Different from the Merkle trees used in Bitcoin, Patricia Merkle Tries used in Ethereum has three parts: stateRoot, transactionRoot, and receiptsRoot.

Starting with complexity. Patricia Merkle Tries allow data integrity verification. It computes the leaf nodes into one hash and store it in the parent node, same with branch nodes, until getting a single hash in the root node. This means the root hash of the trie can be computed with the Hash function, and that if any value pair get updated, the root hash would alter as well. This further indicated that if two tries have identical value pairs, they will be identical down to the last byte. This overall gives the insert, lookup, and delete function a complexity of $O(\log(n))$.

To understand the hash structure better, the illustration of an example hash is provided on the Ethereum documentation page. First of all, suppose 4 value pairs are wanted: ('do', 'verb'), ('dog', 'puppy'), ('doge', 'coin'), ('horse', 'stallion'), shown by Code 1.

```
<64 6f> : 'verb'
<64 6f 67> : 'puppy'
<64 6f 67 65> : 'coin'
<68 6f 72 73 65> : 'stallion'
```

Code 1. Value Pairs in Example Trie from Ref [15]

Then the example trie would look like what is shown in Code 2.

```
rootHash: [ <16>, hashA ]
hashA:  [ <>, <>, <>, <>, hashB, <>, <>, <>, [ <20 6f 72 73
65>, 'stallion' ], <>, <>, <>, <>, <>, <>, <>, <> ]
hashB:  [ <00 6f>, hashD ]
hashD:  [ <>, <>, <>, <>, <>, <>, hashE, <>, <>, <>, <>, <>,
<>, <>, <>, <>, 'verb' ]
hashE:  [ <17>, [ <>, <>, <>, <>, <>, <>, [ <35>, 'coin' ], <>,
<>, <>, <>, <>, <>, <>, <>, <>, 'puppy' ] ]
```

Code 2. Example Trie from Ref [15]

One important features the trie data structure provides is that it allows verification of a key-value pair without giving the access to all the key-value pairs [16].

4. Analysis and next step

This section analyzes the value of Ethereum, cryptocurrency market and the next step the author is going to take.

4.1. Misunderstanding of Cryptocurrency

As many people first learned the concept of cryptocurrency through the rapid increase in the Bitcoin market price, it is easy to mistakenly assume cryptocurrency as a technology that centers around currency and market. Many people believe that cryptocurrencies are "virtual currencies", which its value is not based on and tangible items, unlike other fiat currencies at all, and there is no governance from a central bank or a third party. If cryptocurrencies are perceived this way, it is easy to conclude what many people are claiming today, which is that cryptocurrencies had a huge increase in value only people expected them to have a higher value, but their entire value is based on this expectation instead of actual value, which means they are essentially a bubble. Now as the market value of cryptocurrencies is crashing, people believe that the bubble is breaking, and people are going to realize that cryptocurrencies will eventually reach a market price of zero since they have no value.

4.2. Cryptocurrencies, The Blockchain Technology

As introduced in previous sections, instead of saying cryptocurrencies serve as a new form of currency, it is more appropriate to say that cryptocurrencies are a successful implementation of the Blockchain technology. The essential purposes of cryptocurrencies and platforms such as Ethereum being created is less about creating a currency, but more about implementing the decentralizing technology, with Bitcoin firstly implemented it to decentralize trading and Ethereum further implemented it into generalizing decentralized applications. Moreover, since the Blockchain technology itself has the security feature, it makes cryptocurrency trades and transactions unique, with their security, anonymity, and the fact that it is a direct transaction between two parties. This unique feature also determines that the Blockchain technology and cryptocurrencies are irreplaceable so far and have their unique functions and purposes, thus they will always be in demand and have value if no other technology can replace its unique feature.

4.3. Next Step and Future Expectations

Being a revolutionary technology, Blockchain as well as Ethereum provides many potentials and innovation. It is unquestionable that this potential is going to be discovered and developed. There have been several proposed applications of decentralization, such as video game, which the game benefits from Blockchain technology for the non-fungible tokens and system transparency, user generated content (UGC) network, which benefits from the privacy and security, as well as internet of things (IoT), sharing economy credits, enabling offline transactions, and so on. There are also many features that await to be invented or improved via the Blockchain technology and dApps [13]. After the research and analysis of Ethereum's technological and economic value, the author is going to step forward into implementing a decentralized application via Ethereum, to further understand the framework, process, implementation, and design of a decentralized application, while looking forward to being able to apply this decentralized feature into future studies.

5. A preview of building a dApp

This section presents a preview of building a dApp, include the general structure, things that need to be cautious of, and the general workflow.

5.1. Smart Contract

Smart Contract is usually based on Solidity, the most well-known programming language for writing a Smart Contract [9]. It is usually written on various platforms; Remix is one of the IDEs

which allows users to write Solidity. Note that it is very important to test the Smart Contract code, since once it is added to the block it cannot be edited or changed, which could be problematic. Truffle is the most well-known and most frequently used framework for developing and testing the Smart Contract code. Truffle is written in Node.js as a npm package. One other thing to keep in mind after finishing developing the basic Smart Contract is that it needs to be made more user friendly, otherwise users will need to use a command line interface, which could hugely limit the user experience. Therefore, people often build a webpage to interact with the Smart Contract, thus many choose to use HTML, CSS, and JavaScript for the client side of the program [14].

5.2. Ecosystem of The Application

To start with writing the application, it is important to examine the blockchain structure of Ethereum, find the right tools, and to fuel the application with gas. The total cost is going to be the gas used times the gas price. In an Ethereum transaction, it includes several parts: once, signature, gas price, gas limit, to, value, and data. For the tools that need to be used in developing an Ethereum application, it often includes several categories: Ethereum Blockchain client, developing/testing Blockchain, compiler and testing framework, source code editor and integrated development environment. For the Ethereum Blockchain client, Geth is selected for this project, which is downloaded directly from the Ethereum page at https://geth.ethereum.org/. For the development and testing of Blockchain, a selection between Truffle and Ganache, or maybe both, will be made. For compiler and framework, as mentioned before, Remix is going to be implemented, it can be used as the IDE at the same time. For an Ethereum product life cycle, it is similar to the development of other software: planning, development, testing, and deployment [6].

6. Conclusion

By introducing the development of Ethereum, it is shown that the Ethereum platform has a revolutionary value in creating decentralized applications with the security as well as other properties of the Blockchain technology. From the development of Ethereum, it is seen that Ethereum was not created mainly as a cryptocurrency, in contrast, it focuses much more on the generalized as well as decentralized features. It is a great tool for developing decentralized applications, which are now currently being implemented by many organizations and individuals. It also has a huge community support, with people contributing to its GitHub page every day. From the technology side, we can see that Ethereum's implementation of the Blockchain technology ensures security and immutability, and its hash algorithm makes it much faster in transaction speed than of Bitcoin. Since this feature is unique and important in many scenarios, the Ethereum and Blockchain technology will always be in demand in the foreseeable future.

References

[1] What is Ethereum? (n.d.). Ethereum.org. https://Ethereum.org/en/what-is-Ethereum/.

[2] Buterin, V. (n.d.). Ethereum: Platform Review Opportunities and Challenges for Private and Consortium Blockchains. http://www.smallake.kr/wp-content/uploads/2016/06/314477721-Ethereum-Platform-Review-Opportunities-and-Challenges-for-Private-and-Consortium-Blockchains.pdf.

[3] ETHEREUM: A SECURE DECENTRALISED GENERALISED TRANSACTION LEDGER EIP-150 REVISION. (n.d.). https://www.gavwood.com/paper.pdf.

[4] @Refinitiv. Retrieved from https://www.refinitiv.com/en.

[5] You are being redirected... (n.d.). Www.analyticsinsight.net. Retrieved July 31, 2022, from https://www.analyticsinsight.net/Ethereums-price-is-down-is-it-calm-before-storm-in-2022/.

[6] Laurence, T. (2019). Ethereum for Dummies. Wiley & Sons Canada, Limited, John.

[7] Wikipedia Contributors, "Blockchain," Wikipedia, Mar. 14, 2019. https://en.wikipedia.org/wiki/Blockchain.

[8] Mohammed, A. H., Abdulateef, A. A., & Abdulateef, I. A. (2021, June 1). Hyperledger, Ethereum and Blockchain Technology: A Short Overview. IEEE Xplore. https://doi.org/10.1109/HORA52670.2021.9461294.

[9] Simplilearn. (2020). What Is Ethereum? | Ethereum Explained | Blockchain Tutorial For Beginners | Simplilearn. In YouTube. https://www.youtube.com/watch?v=04f1YsVntw8.

[10] Antonopoulos, A. M., & Ph.D, G. W. (2018). Mastering Ethereum: Building Smart Contracts and DApps. In Google Books. "O'Reilly Media, Inc." https://books.google.com/books?hl=en&lr=&id=nJJ5DwAAQBAJ&oi=fnd&pg=PR4&dq=Ethereum+and+smart+contracts&ots=uBLOalH_uG&sig=VH-AfmGTjpwMrA-XzBxRqr5e1QE#v=onepage&q=Ethereum%20and%20smart%20contracts&f=false.

[11] Pilkington, Marc. "Blockchain Technology: Principles and Applications." Research Handbook on Digital Transformations, 30 Sept. 2016, www.elgaronline.com/view/edcoll/9781784717759/9781784717759.00019.xml.

[12] Wikipedia Contributors. "Blockchain." Wikipedia, Wikimedia Foundation, 21 Apr. 2019, en.wikipedia.org/wiki/Blockchain#/media/File:Bitcoin_Block_Data.svg.

[13] Cai, W., Wang, Z., Ernst, J. B., Hong, Z., Feng, C., & Leung, V. C. M. (2018). Decentralized Applications: The Blockchain-Empowered Software System. IEEE Access, 6, 53019–53033. https://doi.org/10.1109/ACCESS.2018.2870644.

[14] FreeCodeCamp, "Build 5 Dapps on the Ethereum Blockchain - Beginner Tutorial," www.youtube.com, Oct. 07, 2019. https://www.youtube.com/watch?v=8wMKq7HvbKw&t=1024s (accessed Aug. 11, 2022).

[15] Joseph Cook. Patricia Merkle Trees. ethereum.org. Retrieved from https://ethereum.org/en/developers/docs/data-structures-and-encoding/patricia-merkle-trie.

[16] Leo Zhang. 2022. Merkle Patricia Trie Explained. Medium. Retrieved August 26, 2022 from https://medium.com/@chiqing/merkle-patricia-trie-explained-ae3ac6a7e123.