Ethereum Reading Report

Weiting Li

April 2022

1 Summary

Based on the success of Bitcoin invented by Satoshi in 2008 and creation of Blockchain that is behind Bitcoin architecture, inventor of Ethereum Vitalik Buterin camp up with this idea of decentralized applications called "Dapps" for finance, cloud computing, messaging and distributed governance. Ethereum is a platform that is specifically designed for people to build these kinds of decentralized applications. Ethereum client which Vitalik called the ether browser includes the ability in peer to peer network for sending messages and a generalized blockchain with a built-in programming language allowing people to use to use the blockchain for any kinds of decentralized applications that they create. Ethereum can assure full transparency and trustworthiness for decentralized finance. It consist of a cryptographically secure system for managing properties and contracts, social networks that allows the user to control their own data flow, systems for trading under utilized computational resources like CPU time and hard drive space and eventually tools for online voting and distributed governance. Ethereum allowed developers to easily build innovative new products on a censorship and collusion-resistant foundation.

2 Problem

In the Ethereum whitepaper, the problem the author wants to solve is that although Bitcoin is a huge success as a novel decentralized currency cornerstoned by the Blockchain concept, the inventor of Ethereum Vikalik believes that aside from Bitcoin which is only for transactions, blockchain is capable of doing much more things. There were four main subbranches: colored coin, smart property, Namecoin, smart contract, and decentralized autonomous organization. However, Bitcoin does not have enough functionality to do all of these tasks: namely **Bitcoin does not allow easy reuse, re-direction of bitcoin protocol for alternative blockchain applications** . Because Bitcoin's script has some limitations: 1. Lack of Turing Completeness: Missing loops which leads to space inefficient if statements; 2. Value-blindness: cannot fine-grain control the amount that can be withdrawn; 3. Lack of state: UTXO can either be spent or unspent. There is no opportunity for multi-stage contracts or scripts; 4. Blockchain-blindness: UTXO are blind to blockchain data such as the nonce, the timestamp and previous blockhash.

3 Importance

To solve the problem above, developers have three choices of how to build an advanced application framework on top of Bitcoin: 1. building a new blockchain; 2. using scripting on top of bitcoin; 3. building a meta-protocol on top of Bitcoin.

Therefore, Vikalik came up with a new idea that is to build a upgraded blockchain which has a more complete Turing programming language so that it can achieve the subbranches of blockchain all together. In ethereum, dapps can be space-efficent, secure, and assurance for rapid development speed. Because of the added power of Turing completeness, value-awareness, Blockchain-awareness and stage, it can offer vastly more power than blockchain scripting. The concept of an arbitrary state transition function as implemented by the Ethereum protocol for a platform has unique potentials.

Vikalik proposed:

" Ethereum is open-ended by design and it is extremely well-suited to serving as a foundational layer for a very large number of both financial and non-financial protocols. "

---- Ethereum White Paper Conclusion.

4 Technical challenges

1. Lack of Turing Completeness: Although bitcoin script language supports a large subset of computation, it does not nearly support everything. The main category missing is loops. This is because of the intention to avoid infinite loops during transaction verifications. But it is technically solvable.
2. Value-blindness: cannot fine-grain control the amount that can be withdrawn; Because UTXO can either be spent or unspent, the only way to achieve this is to use ver yinefficient hack of how many UTXO of varying denominations and having O pick when UTXO to send to the users.
3. Lack of state: UTXO can either be spent or unspent. There is no opportunity for multi-stage contracts or scripts; This leads to that UTXO can only be used to build simple, one-off contracts and not more complex contracts such as decentralized organizations and meta-protocols.
4. Blockchain-blindness: UTXO are blind to blockchain data such as the nonce, the timestamp and previous blockhash. This limits applications in gambling and other categories.

5 Key Insights Contribution

There are a few innovative points from the framework of Ethereum to other blockhains:

Account: Unlike Bitcoin, Ethereum's state is made up of **accounts**. An account consists of: a nonce value; account's ether balance; contract code; storage. Ether is the main fuel used in Ethereum and is used for transaction fees. There are two types of account: 1. Externally owned accounts; 2. Contract accounts.

Gas: To run a contract on Ethereum, there is a new concept of "**Gas**", where one gas is equal to the cost of one step of computation in a contract. However, sometimes some operations cost more gas because they are computationally more expensive. In short, gas paid is proportional to the number of complexity of computations done on blockchain.

Transaction: A transaction in Ethereum looks like this: First 3 similar to bitcoin ---- recipient, sender signature, amount of transfer. And then there are **Data(something smart contract will read and execute), StartGas(max of gas available), Gasprice(fee per step)**. The last two item can be helpful in preventing DDOS. Because every computation cost money, the attacker will have to pay if they want to attack.

Messaging: Contract can send other contracts **messages**. It is created by contract itself. When a c ontract is called , it will generate this message and recipient account then receive and execute some code based on the message.

And then the whitepaper also touches on the Ethereum state transition function and code execution.

These attributes of Ethereum makes it capable of execute these these types of applications:

Financial Applications: hedging contracts etc.;

Semi-Financial Applications: self-enfocing bounties;

Non-financial Applications: DAOs(Decentralized Autonomous Organization), an organization that runs totally upon democracy: every member vote to determine what the organization's next step is.

Currency system: Ethereum has its own token, Ether which is used in the transactions and computations.

Namecoin Application: It only takes about two lines to write a simple namecoin system. This is essential in Votes for president.

Decentralized storage: Similar to Dropbox, Ethereum allow people to rent their storage to others. To increase the security, Ethereum could send the files to different locations and build a contract upon them to send the money if the verification shows that they are storing still.

6 Strength/Weakness

Strength:

1. Simpleness: Ethereum is designed to be a simple contract and open to anyone. Programmers can have all the freedom to do what the want in a fast, storage efficient manner. This helps realize the full potential of blockchain technology.
2. Generalization: Ethereum supports any smart contract because of its Turing Completeness. Programmers can build anything possible if they have enough gas to execute the contract.
3. Sky is the limit: Unique attributes of Ethereum like flexibility, limitless for creativity can support applications that are both financial and non-financial in the future.

Weakness:

1. It seems like Ethereum is yet complete and with questionable security assurance. There was already a failure in Ethereum classic when one hacker found a flaw in one of the loophole of Ethereum which leads to the Ethereum today. And the earlier version became Ethereum Classic.

7 Personal intake

From this whitepaper, I get to learn more about the second largest cryptocurrency- Ethereum and the idea behind its invention in 2014. It seems to me that if Ethereum has much more potential than Bitcoin because Vitalik aims to do more with Blockchain rather than just a currency replacement. After I did some research, I found that NFT is actually related to Ethereum. As many knows, NFT has been a hot topic in crypto- area. Many NFT arts were sold very expensively on the market in this recent 2021. For example, Steph Curry buys $180000 bored ape yacht club NFT in Aug.30 of 2021. This shows the potential of Ethereum platform and establish trust in its expandability. However there are still issues like the electricity consumption are not ignorable. According to Digiconomist's, Ethereum costs 113 terawatt-hours per year, quote: the same power consumption as Netherlands. And it has other drawbacks ----- it is slow. There are only averagely 15 transactions got resolved per second.