Evolution of Blockchain from 1.0 to 3.0

Youguang Lin
1155169171@link.cuhk.edu.cn
The Chinese University of Hong Kong
HongKong, China

Li Jialang
1155160950@link.cuhk.edu.cn
The Chinese University of Hong Kong
HongKong, China

Kong Fan Nap
1155152768@link.cuhk.edu.cn
The Chinese University of Hong Kong
HongKong, China

ABSTRACT

In this paper, we will have a quick study about Blockchain's Evaluation. From Blockchain 1.0 to 2.0 to 3.0, analyzing the features of each of them. The term Blockchain 2.0 is more broadly used to distinguish between bitcoin as an asset and "Blockchain as a programmable distributed trust infrastructure," and adds new extendable features to the variety of utilities and extensibility on the Blockchain. Following by the improvement on scalability and interoperability of Blockchain 3.0 compared to Blockchain 2.0. Moreover, introduced the representative solution DAG in scalability and pioneer AION in interoperability respectively. In the comparison part, we review the scalability differences between Blockchain 3.0 and Blockchain 2.0, and compared with Ethereum and Cardano as their application example. Finally at the experimental part, we uses python to simulate the generation of the Blockchain and adopts the proof of work consensus mechanism.

KEYWORDS

Blockchain,bitcoin, ethereum, consensus mechanism, smart contract, DAD, AION, Cardano

ACM Reference Format:

Youguang Lin, Li Jialang, and Kong Fan Nap. 2021. Evolution of Blockchain from 1.0 to 3.0. In *Woodstock '18: ACM Symeosium on Neural Gaze Detection, December 06, 2021.* ACM, New York, NY, USA, 11 pages. https://doi.org/10.1145/nnnnnnn.nnnnnnn

1 INTRODUCTION

Blockchain technologies contain techniques like mathematics, statistics, cryptography, and algorithm, combining forms of peer-to-peer networks and distributed consensus to settle the traditional distributed database synchronize problem, and it's an integrated multi-functional infrastructure construction. Blockchain is defined as a distributed ledger that uses algorithms to record each transaction as a chain of blocks just like a tracking database. All participants can access the distributed ledger but are not able to edit the historical transaction records. The data held in each block act as a shared database since each block has its own copy of the chain and gets updated once new blocks are added, the whole network update data in real-time. Therefore, all transactions can be transparently viewed by every node in the network thus, it provides visualization of the operation flow. Blockchain is a hot tech trends topic nowadays. The first application of Blockchain, Bitcoin always hit the headlines because of its meteoric rise in value. Beside the use of cryptocurrency, it can be applied to any multi-step transaction where traceability and visibility are required. The supply chain is a notable area where Blockchain can be leveraged to better manage the flow of goods, sign business contracts and trace product provenance thus enhancing the chain's transparency. It could also apply to areas like election platforms, develop an accurate internal of thing (IoT), serve as an open-source application development platform and etc. Although the Blockchain 1.0 cryptocurrencies seem robust since it's never been heard that any has ever been successfully hacked or cracked yet. The novel Blockchain platform is keen to solve the efficiency, scalability and compatibility problems of it. Blockchain technologies contain techniques like mathematics, statistics, cryptography, and algorithm, combining forms of peer-to-peer networks and distributed consensus to settle the traditional distributed database synchronize problem, and it is an integrated multi-functional infrastructure construction. Blockchain is defined as a distributed ledger that uses algorithms to record each transaction as a chain of blocks just like a tracking database. All participants can access the distributed ledger but are not able to edit the historical transaction records. The data held in each block act as a shared database since each block has its own copy of the chain and gets updated once new blocks are added, the whole network update data in real-time. Therefore, all transactions can be transparently viewed by every node in the network thus, it provides visualization of the operation flow.

1.1 Characteristics of Blockchain

Decentralized: The fundamental feature of Blockchain, refers to the transfer of control and decision-making from a centralized entity to a distributed network. Blockchain network does not need to rely on centralized node, the data can be record, store and update dispersed.

Open Source: The novel Blockchain system is open to everyone such as Ethereum, Cosmos, Cardano and etc. The public can use the platform's Blockchain technologies to create applications on it and enhance the variety of use.

Autonomy Base on the consensus, every node on the Blockchain network can process or update data safely since the concept is to trust from a single person to trust the whole system, and no single one can intervene it.

Immutable: The transaction records are preserved permanently, and cannot be edited unless someone takes control of more than 51% node in the same time but it's almost impossible.

Anonymity: Base on the trust consensus, the transaction between a nodes to a node can be anonymous, the data transfer only needs the Blockchain address. Transparent. The data stored in the Blockchain

Woodstock '18, December 06, 2021, HongKong, CN

ACM ISBN 978-1-4503-XXXX-X/21/12…$15.00
https://doi.org/10.1145/nnnnnnn.nnnnnnn

system is transparent to every node so it is visualized and no fabricate is allow. This is one of the element make Blockchain trustworthy.

Proof of Work (PoW)

It requires network participants to spend time to solving an arbitrary mathematical puzzle in order to prevent the system from being hacked. Due to the very low probability to solve successfully, this makes it unpredictable which worker will be able to generate the next block. Thus, it is widely used in cryptocurrency mining for validating transactions and mining new tokens. This helps the peer- to-peer transactions security without the need for a trusted third party.

Proof of Stake (PoS)

Use an election process, one node is randomly chosen to validate the next block as a validator to mint or forge new blocks. Each validator has a chance at being selected to write the next block and receive its rewards. To become a validator, a node need to deposit a certain amount of coins to the network as stake, a security deposit, and the node may be selected by the system but it is not a guarantee. Validator ordering transactions and creating new blocks so that all nodes can agree on the state of the network.

1.2 Overview

In this paper, we will have a quick study about Blockchain's Evaluation. From Blockchain 1.0 to 2.0 to 3.0, analyzing the features of each of them. Following by a comparison part with the Blockchain 1.0 versus 2.0, showing how 2.0 can improve the downsides of 1.0 as well as 2.0 pros and cons; Blockchain 2.0 versus 3.0 and showing how it can improve the downsides of 2.0. Next are two sets of experiments on Blockchain1.0 and Blockchain2.0. Finallywe draw a conclusion of the paper.

2 SYSTEMATIC REVIEW OF BLOCKCHAIN

2.1 Blockchain 1.0

In 2008, Satoshi Nakamoto (2008) introduced the first application of Blockchain technology, the decentralized peer-to-peer electronic cash system - naming Bitcoin. The world's first decentralized currency, which replaced the digital cash centralized server signature mechanism, with a consensus based proof of work and highly ensure Bitcoin's security. Proof of Work algorithm based on the SHA-256 hashing function in order to validate and confirm transactions as well as to issue new bitcoins into circulation. In a process called mining, blocks are created in about 10 minutes each, after the solvers of the computation challenges are rewarded a certain amount of new Bitcoin. Follow by the extraordinary rise in value of Bitcoin, mining activity are getting larger around the world. Using 10 minutes to generate a new block is not efficient in the business world when it comes to other application, moreover, the proof of work algorithm take a lot of computing power and energy consuming. According to Business insider (Kim, 2021) the annual Bitcoin mining activity consumes is almost 0.5% of all electricity consumption worldwide, meanwhile that is more annual electricity use than all of Finland, which is a country of 5.5 million people.

2.2 Blockchain 2.0

2.2.1 Brief introduction. The term blockchain 2.0 is more broadly used to distinguish between bitcoin as an asset and "blockchain as a programmable distributed trust infrastructure," and adds new extendable features to the variety of utilities and extensibility on the blockchain. Blockchain2.0 no longer sees blockchain as part of the decentralization of money and payments, but expands the scope of the technology to achieve a more general decentralization of the market, and by providing certificates and registers of rights and obligations, transactions will involve other types of assets real estate, intellectual property, cars, art, etc. Since blockchain2.0 is programmable, the new application is said to run on a new set of protocols (the "Blockchain2.0 protocol"). A comparison with Internet protocols and their stack layers illustrates the relationship between blockchain1.0 and blockchain2.0. The former can be seen as the TCP/IP transport layer, while the latter can be seen as HTTP, SMTP, and FTP. In this context, blockchain2.0 applications resemble browsers, social networks, and file-sharing services.

2.2.2 Smart contract. Blockchain2.0 introduces smart contract. A smart contract is a computer protocol designed to propagate, validate, or enforce contracts in an informationized manner[4]. The term "smart contract" was coined probably around 1993 by Nick Szabo, a computer scientist, to bring what he called "highly evolved" contract law practices and related business practices into the design of e-commerce agreements between strangers. An early adaptation of smart contracts is digital rights management schemes. These are copyrighted smart contracts, and financial cryptographic schemes for financial contracts. A smart contract program is not just a computer program that can be executed automatically: it is a system actor in its own right. It responds to incoming information. It can receive and store values, and it can send information and value out.The program acts like a person you can trust to temporarily hold assets, always following prior rules.The diagram below is a model of a smart contract: a piece of code (smart contract) deployed on a shared, replicated ledger can maintain its state, control its assets and respond to incoming external information or assets. Smart contracts in the blockchain field have the following characteristics:

- The rules are open and transparent, and the rules and data in the contract are visible to the outside world;
- All transactions are publicly visible and there will be no false or hidden transactions.

Developers use smart contracts to formulate a set of rules, and then post them online. People interact with smart contracts, and machines finish the business, so as to avoid cheating that may be caused by human execution. The statically typed programming language, Solidity, is the programming language for Ethereum's smart contract implementation, running on Ethereum's Virtual Machine, Ethereum Virtual Machine (EVM). With Solidity, developers can write self-executing applications. The program can be treated as an authoritative and unchangeable trading contract. For people who already have the ability to edit programs, writing Solidity is as easy as writing a normal programming language.

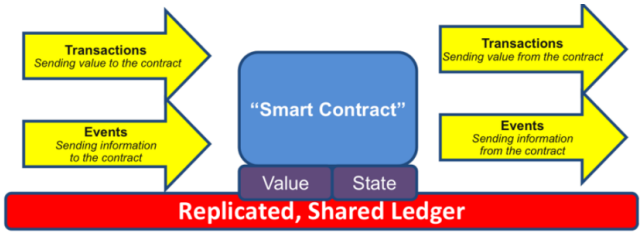

Figure 1: Smart contract

2.2.3 Ghost Protocol. Compared to blockchain1.0, blockchain2.0 has increased the block output time from 10 minutes to 15 seconds, which is a huge improvement, but it also brings a problem, that is, the block consensus problem. In the span of 15 seconds, a newly published block has most likely not spread to the entire blockchain network. In this case, how to achieve the consensus protocol in Bitcoin, how to better comply with the "Chain length is king" – the longest chain is considered the main chain? There are two main problems:

- It is difficult to determine the longest chain because of the fast block producing speed.
- Because of the network, the computing power of the ore pool has the advantage of asymmetry.

To address these two issues, Ethereum introduced the Ghost protocol to address these issues.There are frequent forks in Ethereum, and in order to determine the longest chain as quickly as possible, these forks need to be merged as quickly as possible. As shown in the figure, it is assumed that the ethereum system has the following situation: A, B, C and D are on four branches. Finally, as time goes by, the chain where B is located becomes the longest legal chain, so the orphan block/stale block of A, C and D becomes invalid. However, in order to compensate for the work of the miners who belong to these blocks, Give these blocks some "compensation" and call them "Uncle blocks ". It is stipulated that block E can include A, C and D uncle block when it is released. Block A, C and D uncle block can get 7/8 of the block reward. In order to encourage block E to include uncle block, it is stipulated that each block E contains an uncle block can get 1/32 of the block reward. In order to prevent E from containing A large number of uncle blocks, it is stipulated that A block can only contain two uncle blocks at most. Therefore, E can only contain two blocks at most in A, C and D as its block producing reward.

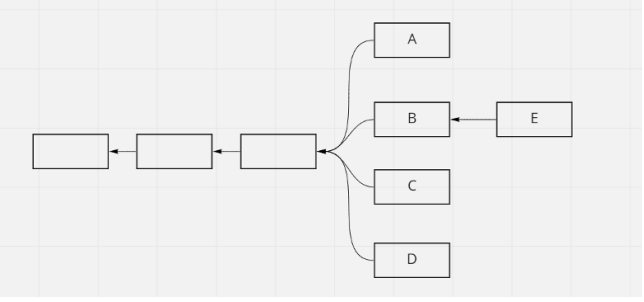

Figure 2: Ghost Protocol

2.2.4 Ethererum. Prior to Ethereum, the development of blockchain was very difficult, resulting in the development of a very simple form of products, the main products are only digital currency. At that time, in addition to Bitcoin, there were also some "copycat coins". Because the source code of "copycat Coin" is very similar to bitcoin, so bitcoin has some limitations, copycat coin also has, there is no substantial leap, nor out of the "digital currency" this single landing product. Ethereum is a substantial leap forward for blockchain technology. Ethereum has made it possible to commercialize blockchain technology beyond the limitations of being used only as a "digital currency." Therefore, if the blockchain1.0 represented by Bitcoin provided new ideas and technical means for value transfer, then the Blockchain2.0 represented by Ethereum has greatly expanded the application scenarios of blockchain and made the commercial application of blockchain a reality. Ethereum is a platform, it offers a variety of module allows users to build applications, if compared build applications to build a house, then the Ethereum provides modules such as walls, roof, floor, users only need to set up the house like a brick, so the cost of building applications on the Ethereum and speed are greatly improved. Specifically, Ethereum builds applications through a Turing-complete scripting language, which is similar to assembly language. We know that programming directly in assembly language is a pain, but programming in Ethereum does not need to be in EVM directly, but rather in high-level languages such as C, Python, Lisp, etc., which are converted into EVM by the compiler. The applications above are contracts, which are at the core of Ethereum. Contract is a live in the etheric lane system automatically agent, he has an own etheric currency address, when the user to address after sending a deal in the contract, the contract was activated, and then according to the additional information of the transaction, contract will run its own code, the final returns a result, the results from the address of the contract issued another deal. It should be noted that transactions in Ethereum are not just about sending Ethereum, they can embed quite a bit of additional information. If a transaction is sent to a contract, this information is important because the contract will use this information to complete its business logic. The business that contracts can provide is almost endless, and the boundary is your imagination, because Turing's complete language provides complete freedom for users to build applications. The white paper gives several examples, such as savings accounts and user-defined sub-currencies.

2.3 Blockchain3.0

2.3.1 Brief introduction. In the blockchain industry, blockchain 3.0 is a comprehensive term which describes an attempt to fix current issues, specifically scalability and interoperability that many claim. While Blockchain 1.0 (think Bitcoin) and Blockchain 2.0 (such as Ethereum) have launched Distributed Ledger Technology (DLT) out there, Blockchain 3.0 is needed to win mainstream adoption. It should be the last push. Blockchain 2.0 witnessed the birth of smart contracts, computer programs that run automatically when predefined conditions are met and stay on the blockchain network. The second version is better than the first. Much better and faster but can't really keep pace with centralized payment media such as Visa and PayPal. Visa can handle an average of about 1,700 transactions

per second, while PayPal can handle about 10 million transactions per day. Therefore, we needed to make blockchain a viable technology for fintech players. And to achieve this, scalability issues had to be first considered and resolved. On the other hand, there are so many distinct blockchains on the world. Therefore, the communication between them has become an important issue. However, the current blockchain industry lacks protocols for communication between different platforms. At present, many companies and organizations have proposed solutions to problems from different angles. This paragraph mainly talks about the development of blockchain 3.0 in scalability and interoperability.

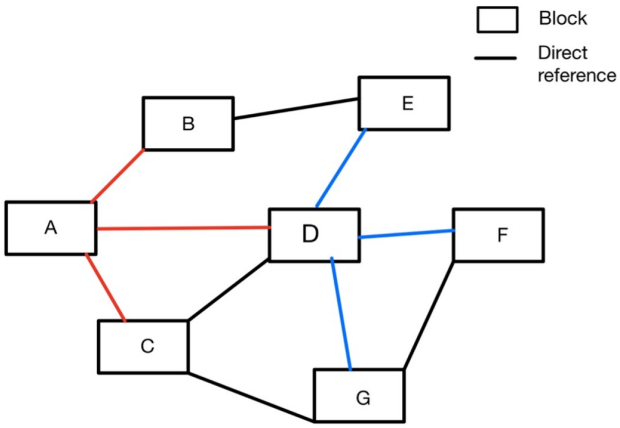

Figure 3: An overview of DAG: Each rectangle in the graph represents a block.One previous block can generate multiple blocks by linking together. (i.e. three red arrows pointing to A and three blue arrows pointing to D)

2.3.2 Scalability. At present, there are many solutions to the scalability problem. But like the CAP theory, the blockchain system also has three similar important aspects. The first is decentralization, the second is security, and the third is scalability. However, they cannot exist well [5]. So, it is significant to balance these three properties of blockchain system. Currently, there are mainly two types of solutions [6]. One way to focus on the on-chain design of blockchain. This means solving the problem from the perspective of block' structure, consensus algorithm or main-chain's specific structure. What's more, second way concentrates on off-chain methods to reduce the burden on the main-chain. But in general, they all have their own advantages and disadvantages, and they all try to realize that the blockchain system can meet the requirements of decentralization, security and scalability at the same time. Here, I mainly talk about one of the methods DAG (Directed Acyclic Graph) which makes blockchain 3.0 notable and viable. It belongs to the first category mentioned above.

2.3.3 Directed Acyclic Graph. As the name implies, the data on a DAG-based network flows acylically. It is a finite directed graph without directed cycles. In order to transform blockchain, it allows a block act as vertex in DAG and connect to some previous vertices. Unlike traditional methods, DAG allows multiple vertices to be connected to the same previous vertex. As Figure shows, each edge represents that the new transaction has approved the previous transaction and multiple blocks can link to a same previous block. With this operation, the system become more efficient as the network grows and accommodate more transactions. This structure eliminates the need for block time (10 minutes for Bitcoin, 20 seconds for Ethereum) and allows transactions to be processed in near real time. DAG is used in the IoT Chain (ITC) and processes 10,000 transactions per second. This is much better than Visa.

2.3.4 Interoperability. As we mention before, many companies and projects are tackling this issue from every angle. There are three prime examples of blockchain3.0 specialized projects in interoperability. They are Aion, Wanchain, and most recently, Polkadot. The goal of these projects is to provide a mechanism for transferring data and assets between blockchains without the need for a centralized third party. So, for example, you can exchange Bitcoin for ether directly from one blockchain to another. Interoperability is also not limited to communication between blockchains. It also needs to connect the blockchain to the traditional infrastructure. Enterprises like ChainLink are working to do that by building an ecosystem of oracle that feeds real-world data to blockchain networks. Google, Oracle, and SWIFT have already partnered with Chainlink to receive oracle data and easily integrate the blockchain network into their systems. On the other hand, traditional financial institutions like Santander and Barclays have also created their own interoperability standards.

2.3.5 AION. The purpose of the first generation of blockchains was to replace currencies, led mainly by Bitcoin. The second-generation blockchain projects are basically dapp platforms, and the current leader of this generation is Ethereum. The third generation block -chain enables seamless interconnection between independent block -chain networks. AION is a pioneer in this aspect in the third generation of blockchain. AION will support different blockchain networks to communicate on a global scale. The background of AION is that the current blockchains are all running in independent networks, and different blockchains use different programming languages and protocols, which makes communication with each other particularly difficult. AION is a blockchain project that aims to be a bridge between all blockchain projects (including private and public). In order to achieve this goal, AION will achieve the following functions. The first is the exchange of data and value between blockchains that comply with the AION standard (which already

supports the Ethereum blockchain). The second is the rapid processing of transactions and the increase in data capacity. The third is to create customized public and private blockchains to maintain interoperability with other blockchains, while allowing publishers to control consensus mechanisms, token issuance, etc. In terms of consensus, the inter-chain and on-chain transactions of the AION platform have different consensus mechanisms. This means that the consensus failure of inter-chain transactions will not lead to the failure of the intra-chain consensus, and vice versa. The on-chain consensus mechanism combines BFT (Byzantine Fault Tolerance), DPoS, and a new neural network-inspired verification algorithm PoI (proof of intelligence), which is called proof of intelligence. Inter-chain transactions are managed by bridges. These bridges use the clear consensus mechanism of the AION main chain, and each bridge is protected by a personal consensus. Bridge validators will be rewarded through inter-chain transaction fees and partial blocks.

3 COMPARISON

3.1 Blockchain1.0 vs Blockchain2.0

In this section, we will compare several aspects of Blockchain1.0 and Blockchain2.0.

Type of State: Compared to Blockchain1.0, blockchain2.0 has more states,which provides Blockchain2.0 more flexibility so that it can deal with more complex business logic. In contrast, Blockchain1.0 only have two states: successful or unsuccessful.

Block Time: Transactions are broadcasted immediately after the user confirm the transaction, but they are not being trusted until they become a part of the next block. For this reason, it's important to reduce block time, because users don't want to spend more than ten minutes waiting for the transactions to be committed. Blockchain2.0 improve significantly in reducing block time, the transactions can be committed in just a few seconds.

TPS(Transaction Per Second): As we explained earlier about block time, we know that TPS is just a theoretical number that is calculated as the number of transactions per block divided by the block time. Although it does not mean how many transactions are processed per second, it is a good indication of network bandwidth because they are processed in the next block.TPS can also demonstrate the performance of blockchain. In bitcoin applications, the world can only process 3.3-7 transactions per second, which is obviously not enough for the increasingly large bitcoin world. In contrast, Ethereum can process 15 transactions per second, which is two to three times more efficient than Blockchain1.0.

Programmable: Blockchain2.0 introduces smart contract.The smart contract program acts like a third party you can trust to temporarily hold assets, always following prior rules.The diagram below is a model of a smart contract: a piece of code (smart contract) deployed on a shared, replicated ledger can maintain its state, control its assets and respond to incoming external information or assets.It provides the foundation for blockchain 2.0 to support more complex applications.

Consensus mechanism: A consensus mechanism is a secure fault-tolerant mechanism for reaching agreement on the state of a block -chain network. This involves validating and authenticating each transaction, and each transaction becomes part of a new block. Simply put, consensus is to ensure that the data that will become part of the ledger is valid and true, and that other participants confirm its authenticity.Blockchain1.0 uses Proof-of-Work as its consensus mechanism. This brought some drawbacks. Some people collect computers with strong computational power and use them together for mining, wasting a lot of computational power and electricity.Blockchain2.0 mitigate this problem by introducing another consensus mechanism: Proof of Stake. Blockchain2.0 is now using a combination of PoW and PoS, and gradually changing to only relying on PoS. It is much energy-saving and environmentally friendly.

Technology scalability: Ethereum holds the largest blockchain developer ecosystem, with 200,000 active online developers.They are trying to build some new decentralized application to benefit the world.We can foresee a future where blockchain 2.0 will develop rapidly.

Final Goal: Blockchain1.0 and Blockchain2.0 have different final goal. Bitcoin could be the gold of digital currencies in the future, thanks to its value preservation and potential for appreciation.Blockchain2.0 store data in the blockchain and therefore it is a more trustworthy system than the centralized one.It might become a Financial operating system in the future.People can do things on the system quickly and easily without being charged expensive fees.

Applications: Blockchain1.0 only has one application which is bitcoin. Blockchain2.0 have more applications like decentralized application, decentralized finance and Non-Fungible Tokens.More and more applications in blockchain2.0 is being creating by thousands of developers.In the future, these applications will also come into our life and bring us more convenience

3.2 Blockchain2.0 vs Blockchain3.0

As we mention in the Blockchain3.0, Blockchain 3.0 aims to address the scalability and interoperability dilemmas that arise in Blockchain 1.0 and 2.0, promising a better solution with a sophisticated framework.

First of all, in the direction of scalability, we will compare DAG with Ethereum, which is one of the representative solutions in blockchain3.0. With the special data structure, DAG eliminates the block times, which is 10 minutes for bitcoins and 20 seconds for Ethereum, thereby allowing transactions to get processed almost in real-time. DAG is being used by IoT chain (ITC) and it processes 10,000 transactions per second, which is far more than Visa. Visa can handle on average around 1,700 transactions per second.

What's more, Blockchain 1.0 and Blockchain 2.0 have failed so much in their efforts to gain public, we have a new era of the technology waiting for us to embrace it - BLOCKCHAIN 3.0.Cardano - Spearheaded by Charles Hoskinson (one of the co-founders of Ethereum). Cardano is an advanced blockchain platform that includes smart contracts, transaction systems and Dapps, developed from scientific philosophy and advanced research. Cardano is responsible for Blockchain 3.0, pioneering a whole new approach to digital currencies. Next, we will use it to represent blockchain 3.0 in some important aspects and compare it with the representative Ethereum of blockchain 2.0.

Table 1: Blockchain1.0 vs Blockchain2.0

Properties	Blockchain1.0	Blockchain2.0
Type of state	Only two(successful or unsuccessful)	Multiple types
Block Time	Long(in minutes)	Short(in seconds)
TPS(transaction per second)	3.3-7	15
Programmable	No	Yes
Consensus mechanism	PoW	PoW+PoS
Technology scalability	The largest blockchain developer ecosystem, with 200,000 active online developers	Few
Final Goal	Digital gold	Financial OS
Applications	DeFi,dApp,NFT	Bitcoin

Cardano uses the Haskell programming language, while Ethereum uses Solidity. Haskell is a widely accepted programming language with non-strict semantics, while Solidity is a contact-oriented language explicitly built to create smart contracts. Haskell allows developers to write code accurately and establish efficient and secure protocols. Robustness, on the other hand, has serious security issues. On the performance, Cardano achieves 1 million TPS with Hydra Scaling while Ethereum 2.0 only achieves hundred thousand TPS with Sharding. For other comparisons, please refer to the table. In general, the design and development of Cardano is a more mature smart contract blockchain platform after strict academic considerations and peer review.

4 EXPERIMENT

4.1 Small demo of Blockchain1.0

4.1.1 Description. In this part, I will introduce a tiny program demo about creating a blockchain in python. In the function page, there are three sections on the function page. The first part is used to generate blocks. The second function is used to modify the block content. The third function is used to detect whether the block has been modified. The first is to create a block function. Each block contains six attributes, namely index, timestamp, preHash, curHash, data and countNum. Index represents where the block sits on the chain. The timestamp tells us when the block is created. The data is what we want store, now in case of the transaction, it will represent how much money was transferred and who was the sender and receiver. Previous hash is a string that contains the hash of the block before this one. This is very important because it ensures the integrity of our blockchain so to keep track of all these values. Finally, the count num means the number of calculations needed to generate a block. Blockchain are great because once a block is added it cannot be changed without invalidating the rest of the chain. In order to prove that the blockchain will be invalid once it is modified, I designed the modification block function and the verification block function. When you use the modify block function to modify the content of a block, you will find that the state of the entire block chain will change from valid to invalid. So if you detect that a new block broke your chain or if something is wrong with your chain then you should have a mechanism that rolls back the changes and them puts your block chain back in a correct state.

While creating the block, I realized the consensus mechanism (Proof of work) in the blockchain by matching the hash value. For bitcoins, it requires the hash of a block to begin with a certain number of zeros, and because you cannot influence the output, you simply must try a lot of combinations and hope you get lucky with the hash that has a sufficient number of zeroes in front of it. This is also called difficulty. We can also increase the difficulty to control how fast new blocks can be added to our block chain.

4.1.2 Demonstration. Click the button 'Block Chain Demo', you will go to the function page.

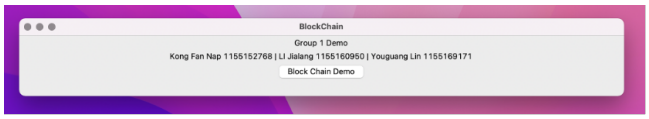

Figure 4: Blockchain1.0 Demo 1

There are three functions. You will see three part, add new block, edit block and check block.

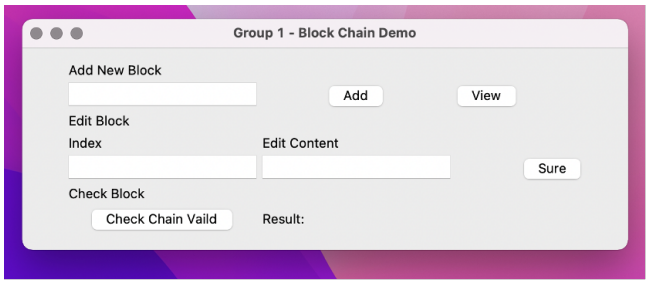

Figure 5: Blockchain1.0 Demo 2

You can enter the content you want to store in the block in the input box, and then click the Add button. At this time, a block is created. Then you can click the view button to view the blocks you have created.

Table 2: Cardano vs Ethereum 2.0

Cardano	Ethereum 2.0	
Consensus Mechanism	Proof of Stake	Proof of Stake
Staking Reward	Around 7% a year	Around 6% a year
Performance	1,000,000 TPS with Hydra Scaling	100,000 TPS with Sharding
Whether to support smart contracts	Yes	Yes
DAPP programming language	Haskell	Solidity
Development style	Peer Review, Academic	Do and consider while improving, more practical
Market value (2021.08)	43 billion U.S. dollars (the fifth in the coin circle)	300 billion U.S. dollars (second in the coin circle)
Main target market	Africa, Southeast Asia	Europe and America

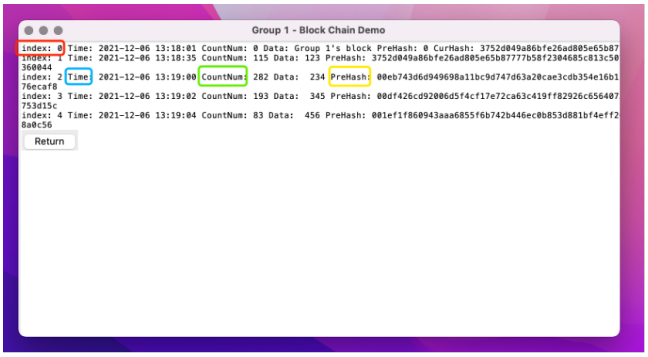

Figure 6: Blockchain1.0 Demo 3

You can click 'check chain valid' button to check whether the blockchain is valid or not.

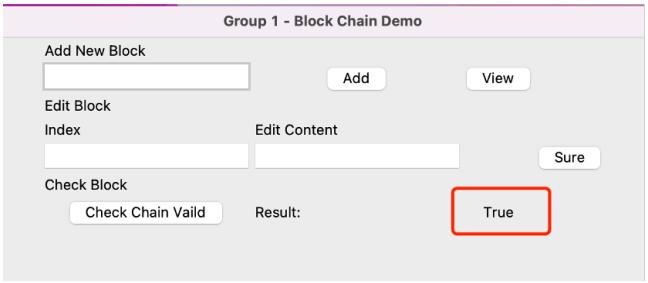

Figure 7: Blockchain1.0 Demo 4

You can randomly modify a block. Then his hash value will also change at this time, then the blockchain is destroyed. Click the check button again, and you will find that the result of his check becomes false.

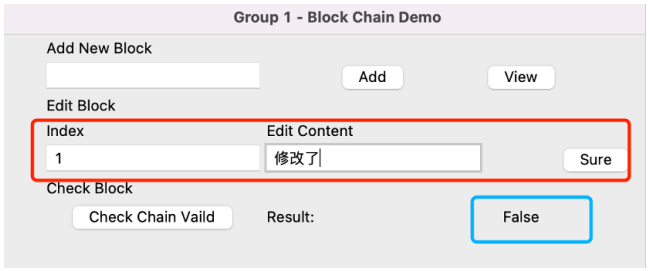

Figure 8: Blockchain1.0 Demo 5

Changing the difficulty from 2 to 4, you will see the number of hash function calculations to generate each block has increase.

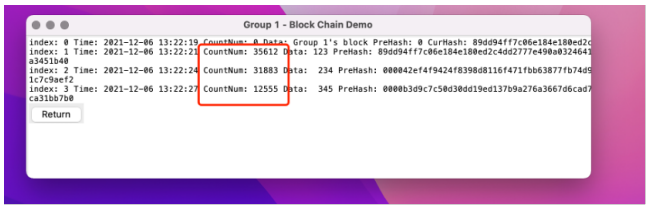

Figure 9: Blockchain1.0 Demo 6

4.2 To-do-list application on Ethereum

4.2.1 Architecture. The representative application of blockchain2.0 is Ethereum. And we made a to-do-list app on Ethereum, It can demonstrate how exactly the Ethereum application work.The architecture of traditional web application and blockchain application is different.

The architecture of a traditional web application is shown in the below graph. When accessing the data in a traditional web application, users would use a web browser that communicate with a web server over the Internet. All the data and files are stored in the server. The following files can be found in the server side:

- Front end code including HTML,CSS,Javascript files
- Back end code which executing the business logic
- Database that contains all the data for the application

This server is a centralized entity that fully controls over every aspect of the application. Anyone user with access to the server can change any code in any component or the data at any time as they want.

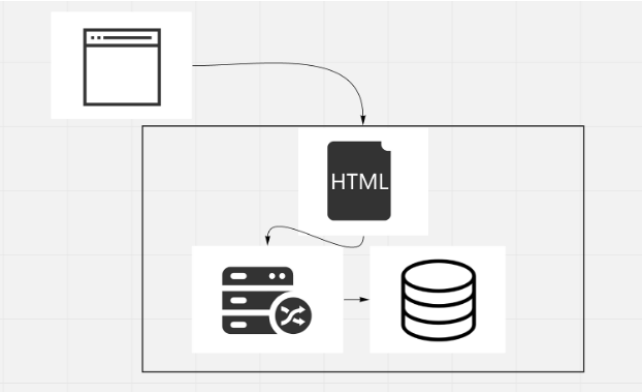

Figure 10: Architecture 1

However, the blockchain application works differently, the graph is shown below. In the architecture of blockchain application, the front end architecture is the same as traditional web application. But in the back end side, the client side application is talking to the blockchain through smart contract. And the data is does not lie in a centralize database. All the data is stored in the blockchain. When the smart contract try to change the data stored in the blockchain, the blockchain is migrating from the previous state to the next state. A migrate module written in javascript is needed to act as a middleware, deploy the smart contract to the blockchain.

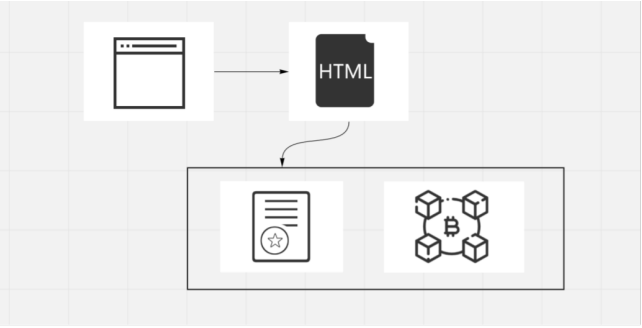

Figure 11: Architecture 2

To summarize how the to-do-list work, the steps is listed below:

- Build a client side web application for the to-do-list that will send request to the blockchain using smart contract.
- We'll use the Ethereum blockchain in this tutorial, which we can access by connecting our client side application to a single Ethereum node.
- Connecting client side application to a single node Ethereum node.
- Use smart contract to powers the to-do-list, and use the migrate module to deploy it to the Ethereum blockchain.
- Connect to the blockchain network with our personal account using an Ethereum wallet in order to interact with the todo list application. In this experiment, we will use ganache and Metamask to connect to our Ethereum wallet.

4.2.2 Demonstration. Here is a screenshot of our application. At the top is a input box, where you can type in some thing. When something is typed in, and the user click 'enter', that means the user is trying to store some data inside the blockchain. In this example, we type in 'Learn blockchain'.

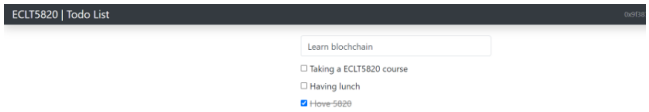

Figure 12: Blockchain2.0 Demonstration 1

After clicking 'Enter', a metamask window will pop up,asking users whether they are going to commit this transaction.They are also some other information showing there, on the top of the window, we can see that we are transfering some Ether from Account2 to another account 0x8F80...F6F4. The metamask also shows us the estimated gas we are going to use in committing this transaction to the blockchain. But the transaction fee is not a fixed number, it depends on how busy the Ethereum network is. The more people commit their transactions at the same time, the higher the current cost of committing transactions.

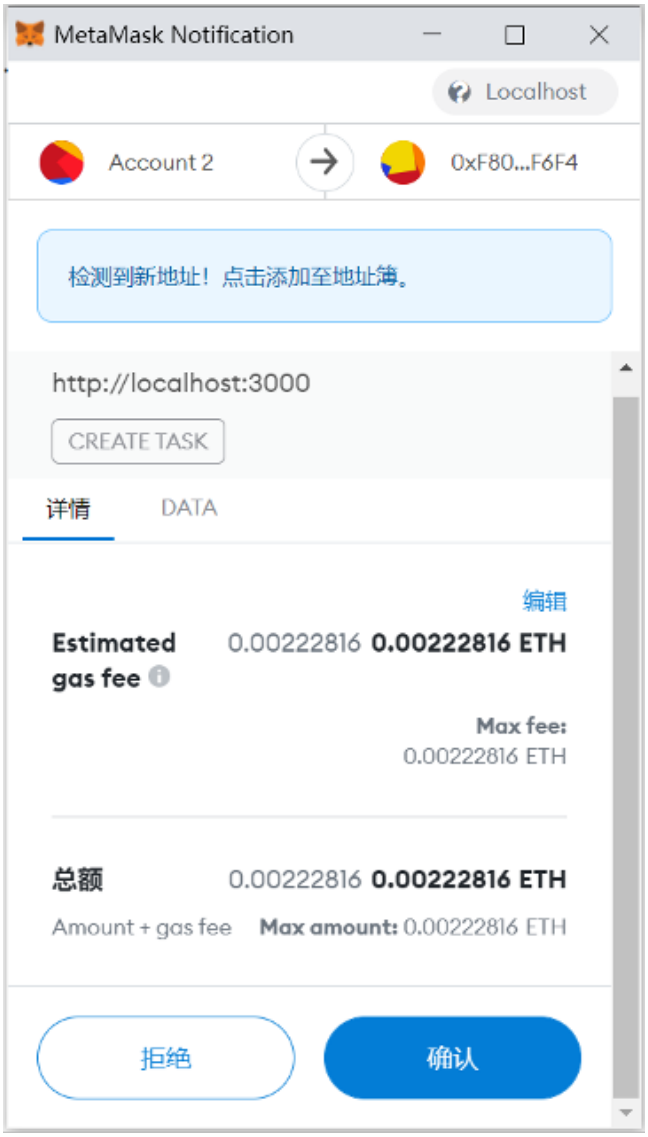

Figure 13: Blockchain2.0 Demonstration 2

After clicking the confirm button, we can see the 'Learning Blockchain' to-do-list item has been added to the web page successfully.

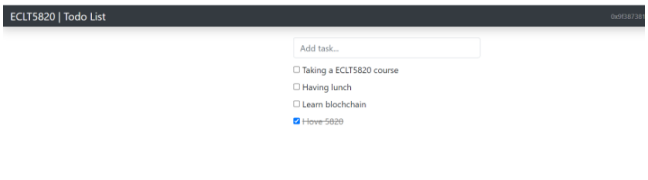

Figure 14: Blockchain2.0 Demonstration 3

We can check this transaction in Ganache. First we take a look at the our account.The screenshot is shown below.We are using the account which still has 99.61 ETH inside, and we can also check its address. Some other information is also being shown, for example, the total block number, the network id and the RPC server address.

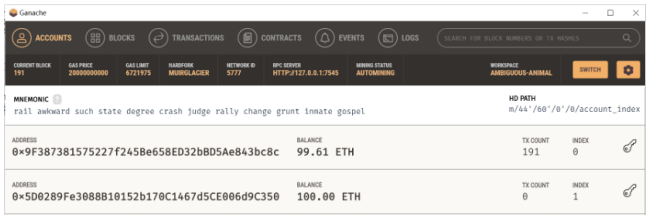

Figure 15: Blockchain2.0 Demonstration 4

We can check the detail information of the blocks.The block that we just added is No.191 block,and we can check the gas usage, gas limit,creating time, block hash, TX hash, the command source's address and the smart contract's address.

Figure 16: Blockchain2.0 Demonstration 5

Some similar information about transaction can also be check.

Figure 17: Blockchain2.0 Demonstration 6

We can also complete the task by clicking on the existing to-do-list item, and then confirm the transaction.The result will be like this.

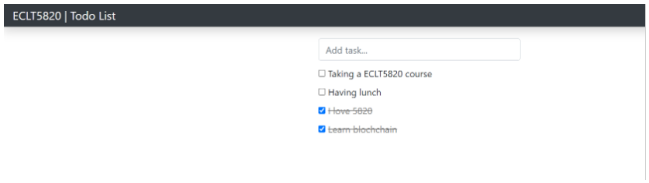

Figure 18: Blockchain2.0 Demonstration 7

4.2.3 Conclusion Future Work. In this experiment we create a simple demo to show how user can store data, alter data in the blockchain, and simulate the process of paying Ether and committing transactions. But its function is simple, in the future we can further develop it into a blog website, storing some more complex data like images, videos in our blog website. Also, we can add more css style and js code to make it more attractive and dynamic.

5 CONCLUSION

In this paper,We first introduced the concept and development history of blockchain. Then Then we further introduced some characteristics related to blockchain including open source, autonomy, immutable , PoW, PoS etc. We discuss three generations of blockchain in section 3.We introduce the basic concept of blockchain1.0 as well as blockchain 2.0 related topics such as smart contracts, ghost protocols and applications. In blockchain3.0, we mainly talk about the improvement in scalability and interoperability compared to blockchain2.0. Moreover, introduced the representative solution DAG in scalability and pioneer AION in interoperability respectively. In section 4, we compare blockchain1.0 and blockchain2.0 as well as blckchain 2.0 and blochain3.0 in many aspects, We summarize what the next generation of blockchain has improved over the last generation of blockchain, and introduce what blockchain technology is driving these advances. section 5, we do two experiment and we record our steps, the basic idea and concept of the experiments and the results of our experiments.

REFERENCES

[1] Bitcoin: A peer-to-peer electronic cash system. (2008, October 31). Nakamoto Studies Institute. https://nakamotostudies.org/literature/bitcoin/

[2] Iuon Chang Lin, Tzu Chun Liao. (2017). A Survey of Blockchain Security Issues and Challenges. International Journal of Network Security, 19. DOI: 10.6633/IJNS.201709.19(5).01

[3] Kim, E. (2021, September 6). Bitcoin mining consumes 0.5% of all electricity used globally and 7 times Google's total usage, new report says. Business Insider. https://www.businessinsider.com/bitcoin-mining-electricity-usage-more-than-google-2021-9

[4] I. Tonev, "Energy Trading Web Platform Based on the Ethereum Smart Contracts and Blockchain," 2020 12th Electrical Engineering Faculty Conference (BulEF), 2020, pp. 1-4, doi: 10.1109/BulEF51036.2020.9326010.

[5] The Scalability Trilemma in Blockchain. Accessed: Sep. 1, 2019. [Online]. Available: https://medium.com/@aakash 13214/the-scalability-trilemmain-blockchain-75fb57f646df

[6] Q. Zhou, H. Huang, Z. Zheng and J. Bian, "Solutions to Scalability of Blockchain: A Survey," in IEEE Access, vol. 8, pp. 16440-16455, 2020, doi: 10.1109/ACCESS.2020.2967218.