DUBU^4 BLOCKCHAIN SYSTEM

WHITEPAPER

DISCLAIMER

The software and technology you are about to use functions as a free, open source, and multi-signature digital blockchain and wallet.

The software does not constitute an account where the developer of this software or other third parties serve as financial intermediaries or custodians of your notes or other valuables.

While the software has undergone beta testing and continues to be improved by feedback from the open-source user and developer community, we cannot guarantee that there will be no bugs in the software.

You acknowledge that your use of this software is at your own discretion and in compliance with all applicable laws.

You are responsible for safekeeping your passwords, private key pairs, PINs and any other codes you use to access the software.

IF YOU LOSE ACCESS TO YOUR DUBU4 WALLET, YOU ACKNOWLEDGE AND AGREE THAT ANY NOTES OR OTHER VALUABLES YOU HAVE ASSOCIATED WITH THAT DUBU4 WALLET WILL BECOME INACCESSIBLE.

All transaction requests are irreversible.

The authors of the software cannot retrieve your private keys or passwords if you lose or forget them and cannot guarantee transaction confirmation as they do not have control over the DUBU4 network.

To the fullest extent permitted by law, this software is provided "as is" and no representations or warranties can be made of any kind, express or implied, including but not limited to the warranties of merchantability, fitness or a particular purpose and no infringement.

You assume any and all risks associated with the use of the software.

In no event shall the authors of the software be held liable for any claim, damages or other liability, whether in an action of contract, tort, or otherwise, arising from, out of or in connection with the software.

We reserve the right to modify this disclaimer from time to time.

ABSTRACT

The year 2015 was the year of Cryptocurrency that grew explosively. The blockchain, which was previously known only as a bitcoin data structure, is also getting attention. As Nakamoto Satoshi (known by the nickname Nakamoto Satoshi) refers to the 'block' and 'chain' mentioned in his white paper, The concept of 'connected block' has promoted the arrival of a new era, 'revolution of value' since 'information revolution on the Internet'..

This timing, started with the bitcoin, is called Blockchain 1.0. At this time, Ethereum extended the blockchain to the decentralized application platform as expending the bitcoin protocol, when people classify it as Blockchain 2.0.

These two base technologies, which were successful by 2017, stared to have problems that cannot be solved with the data structures that link linearly structured blocks as people are increasingly used them and gradually the size of the block chain become gradually larger. People have come to believe that a new paradigm is about to emerge, developers and scholars are starting to offer new alternatives. DAG (Direct Acyclic Graph), Directional noncircular, began to be strongly suggested as an alternative.

The era of Blockchain 3.0 has just begun

The blockchain has now become a time to respond to the demands of the new era. The greatest advantage of a blockchain called 'Sharing' and "Transactions directly between parties" need to present a comprehensive and viable solution to the various methods required as it removes the inefficiency of the double-edged sword as much as possible. Therefore, in our blockchain, DUBU4 would like to suggest ways I have studied between the future assurance of this blockchain and the realistic alternative.

This whitepaper is a description of the design and technical design of the DUBU4 Blockchain system.

DUBU4 WHITEPAPER

1 BLOCKCHAIN TO PRESENT 6

1.1 SUMMARY 6

1.2 TYPICAL PROBLEMS WITH EXISTING BLOCKCHAINS 6

1.3 PRESENT IN BLOCKCHAIN TECHNOLOGY 7

1.4 FUTURE IN BLOCKCHAIN TECHNOLOGY 9

2 DUBU4 BLOCKCHAIN SUMMARY 11

2.1 FUTURE SHAPE OF DUBU4 BLOCKCHAIN 12

2.2 COIN LAYER OF DUBU4 BLOCKCHAIN 15

2.3 DIRECTION OF DUBU4 BLOCKCHAIN 17

2.4 CORE TECHNOLOGY OF DUBU4 BLOCKCHAIN 18

3 DUBU4 BLOCKCHAIN TECHNICAL DETAIL 21

3.1 DUBU4 CORE 21

3.2 TRANSPARENCY AND ANONYMITY 24

3.3 DUBU4 BLOCKCHAIN – CONSENSUS 25

3.4 SUPPORTED DEVELOPMENT WITH MULTI LANGUAGE 33

3.5 GUI DEVELOPMENT TOOL 34

3.6 ATOMIC SWAP P2P EXCHANGE 35

4 ROADMAP 37

5 REFERENCE 38

5.1 EXPLANATION OF TERMINOLOGY 38

5.2 TECHNICAL REFERENCE 39

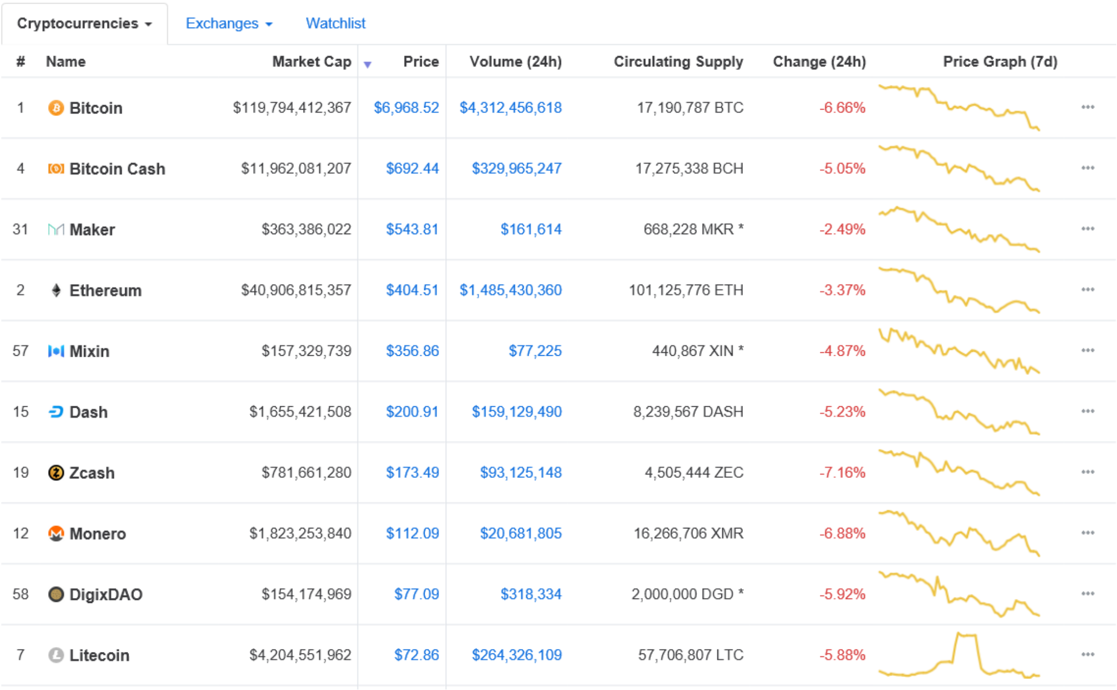
1 Blockchain to Present

1.1 Summary

Cryptocurrency triggered by bitcoin has been amplified the interest in the blockchain technology itself with the expectation of a new paradigm called the 'permanent and transparent' economy that has no the third party intervention. It also leads to develop various research and new complementary technologies.,

It was introduced in 2008 and explosive growth in 2012. At that time, it was able to fully meet the concepts and needs of blockchain technology that users have. There are not many consumers and security issues or technical requirements due to limited transactions. It appeared to be a satisfactory technology at that time with the exception of technical errors.

However, as interest and expectation are amplified at such a speed that Satoshi or Buterin cannot even imagine, the specific needs of the usability increased proportionally, and the system cannot accommodate these demands.



#	Name	Market Cap	Price	Volume (24h)	Circulating Supply	Change (24h)	Price Graph (7d)	
1	Bitcoin	$119,794,412,367	$6,968.52	$4,312,456,618	17,190,787 BTC	-6.66%		•••
4	Bitcoin Cash	$11,962,081,207	$692.44	$329,965,247	17,275,338 BCH	-5.05%		•••
31	Maker	$363,386,022	$543.81	$161,614	668,228 MKR *	-2.49%		•••
2	Ethereum	$40,906,815,357	$404.51	$1,485,430,360	101,125,776 ETH	-3.37%		•••
57	Mixin	$157,329,739	$356.86	$77,225	440,867 XIN *	-4.87%		•••
15	Dash	$1,655,421,508	$200.91	$159,129,490	8,239,567 DASH	-5.23%		•••
19	Zcash	$781,661,280	$173.49	$93,125,148	4,505,444 ZEC	-7.16%		•••
12	Monero	$1,823,253,840	$112.09	$20,681,805	16,266,706 XMR	-6.88%		•••
58	DigixDAO	$154,174,969	$77.09	$318,334	2,000,000 DGD *	-5.92%		•••
7	Litecoin	$4,204,551,962	$72.86	$264,326,109	57,706,807 LTC	-5.88%		•••

<Figure 1. Top 10 Coins in 2018>

1.2 Typical problems with existing blockchains

① The fundamental problem of the blockchain itself - inefficiency of data size and speed

a A blockchain is a database that allows the addition of information in a line. All node that you want can create a block, but there is only one block to be adopted and only approved blocks by a number of consensus can be connected to the chain as a final block. The faster the blocks are piled up, the slower they are since there are complicated processes to find, verify, and sync for new data to add to the database.

b In addition, the size of the blockchain itself continues to increase due to the addition-only data structure. All nodes must keep a copy of this final database and the sync operation itself takes a considerable amount of time.

② Inefficient algorithm used for block generation

a In the case of the bitcoin PoW consensus algorithm, the amount of electricity consumed to generate one block Is about 250 ㎾h as of 2017, which is equivalent to monthly electricity used by a family in Seoul. This amount of electricity is being used to build just one block.

b BitCoin's Mining Pool has performed far more than the sum of all the computing power used by 500 supercomputers around the world and has outperformed the electricity used by the lower 160 countries around the world for one year. This tremendous resource consumption is being used to simple block building.

c Even though numerous consensus algorithms have emerged to improve this, Bitcoin and Ethereum having similar algorithms with it, are still the world's first and second largest cryptocurrency, and still more than 70% of the mining pools are running for them.

1.3 Present in blockchain technology

① The blockchain is not a complete technology.

a There are many people who have skepticism with whether the cryptographic algorithm used in the blockchain can be resistant to future quantum computing. There are already studies that the SHA-256 hash algorithm used by bitcoin is likely to be decrypted by quantum computing in the future b The dangerous situation is to believe and use the encryption algorithm that takes years to verify is guaranteed by the developer only. Typical case is an argument about P-Curl, which is a combination of IOTA's own hash algorithm SHA-3 (Keccak) and Curl. There is still a lot of controversy over the verification of the encryption algorithm.

c Also, any of the following defects can occur; the user's assets are no longer available due to a simple coding error in virtual machines used by Etherium, or if the Bitfinex Exchange is stolen 120,000 ETH due to the vulnerability of BitGo wallet in 2016

d The biggest enemy of a block chain is not a hack, but a lack of technology and a poor application structure.

② Blockchain is not universal databases

a Blockchain can lead to greater problems because of its the inherent structural limitations and the problem of adding and linking data. In some cases, traditional database approaches that rely on traditional relational databases and distributed network storage can be much more efficient.

b In particular, in the case of private blockchains, the advantages of decentralization are rather ambiguous, requiring a lot of development and utilization. This is because it is much better to use an existing database than to use a blockchain, unless you need "sharing" and "strong manipulation” and “change resilience".

c Since the blockchain is in the form of a 'chain', block inserts must be serialized, which makes data update speeds slower than traditional databases that do parallel updates. In a global network where a large number of many unspecified people can participate, such expensive costs and slow speeds can be tolerated, but in a business environment where participants are strictly controlled, the need to spend so much energy and time on the blockchain technology is not necessary

③ Is a smart contract really universal?

a Smart contracts in terms of autonomous and self-executing contracts are one of the most attractive features of the blockchain in that they do not require a separate executing enforcement entity. Basically, this is a system in which the promised assets are automatically transferred to the contracting parties when the terms of the agreement agreed by the parties are met.

b Although conceptually a great idea, it is much more difficult and complex to move the automation of these business processes into code than it is, whereas the scripting language developed for blockchain development to date is very rudimentary and has simple branching and condition settings. In addition, the errors of these scripts themselves are significant and sometimes even bring about the worst situations, such as ethereum hard forks.

c Smart contracts are not yet smart enough to implement practical blockchain operations methods, such as detailed implementation of transaction compliance and resolution of conflicts. Especially, 'Kill Switch' which stops the contract in abnormal situation has a self-contradiction which is against the principle that the blockchain cannot be changed. Developing a blockchain that does not violate the principles is a huge obstacle for smart contracts to overcome while adding solutions to many of these problems

1.4 Future in Blockchain technology

① Ensure scalability and reliability

a The blockchain technology is basically an attempt to replace the trust of two individuals, companies and organizations to mathematical principle. In other words, as the greater dependence on the mathematical principles of the blockchain technology, the more nodes (servers) are needed and the operating environment becomes more computationally intensive, which lead to increases the cost. This inevitably causes a vicious cycle that further aggravates the scalability of the block chain.

b In addition, the public blockchain, which is also the most widely used blockchain type, is transparent to many unspecified persons, so anyone can view the ledger. This is the case with Bitcoin and Etherium, and this transparency is not necessarily good when used in a commercial environment. For example, what if blockchain technology is used on a stock exchange platform as an instant settlement mechanism? Each participant will be able to read all intentions and actions of the other participant, and as a result, the mechanism itself may not function properly.

c As another example, if a manufacturer uses blockchain technology as an open ledger for a vendor, a contractor will be able to view transactions for all other traders on the blockchain. Against this backdrop, companies have to worry about how to keep this transaction data private. In current technology, it is better to use a traditional database in this case.

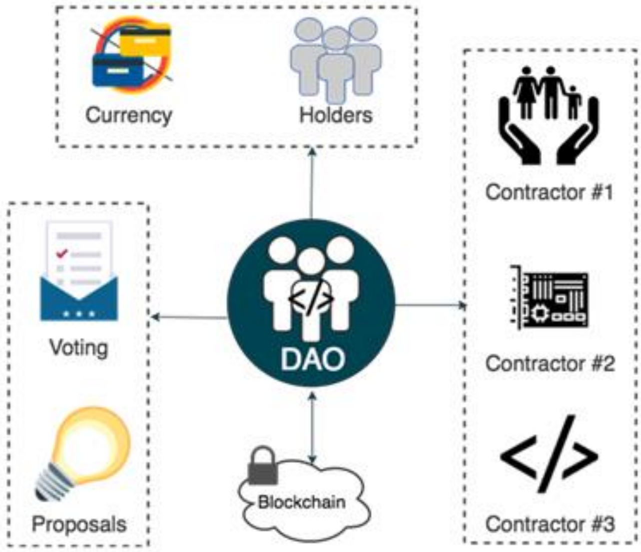
d If you need to use a blockchain, when you only need a non-trust based 'transaction', a 'shared' system opened to all participants, and a 'robust manipulation and change resistance'.

② Future of Cryptocurrency

a Futurist and author Thomas Frey said, " Cryptocurrency has become a part of life. Cryptocurrency will replace 25% of the legal currency by 2030. " citing the currency as a much more efficient system.

b “Cryptocurrency has shown the potential as a new asset over the past two years," said Dr. James Canton of the Global Future Institute. "Cryptocurrency investment will exponentially increase" he added.

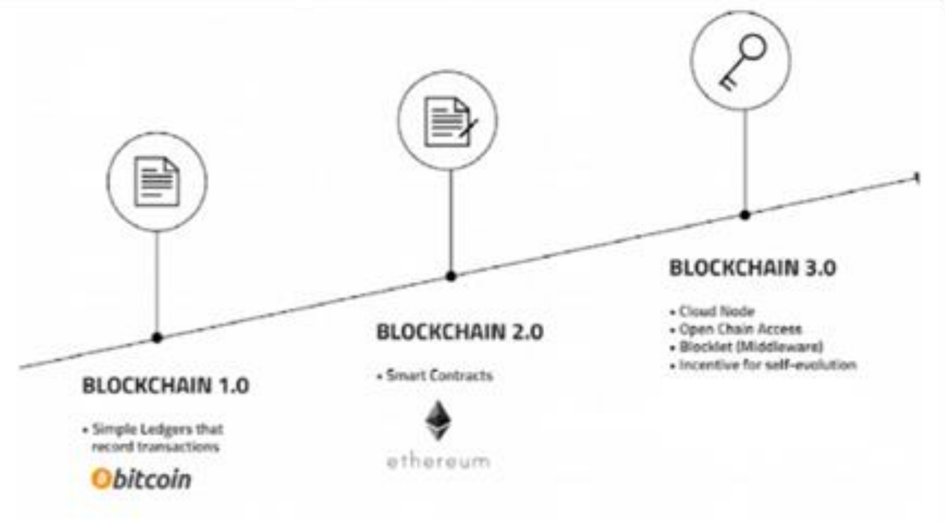
③ DAO Structure



<Figure2. Distributed Autonomous Organization; DAO structure>

a It was a system in which former reliable third parties are selected and assigned roles by members in the past. However, it will be transformed into the way that a blockchain provides that various stakeholders can make decision using collective intelligence, resulting in a "Distributed Autonomous Organization (DAO)" and all services will be based on blockchain.

④ Blockchain 3.0



<Figure 3. Blockchain 3.0>

a After the era of Blockchain 1.0 and Blockchain 2.0, the emergence of blockchain 3.0 technology that can immediately reflect reality with the transaction processing speed of 1,000 TPS per second and quantum computing resistance.

2 DUBU4 Blockchain Summary

We believe DUBU4 is a bright future with the development of the blockchain. The notion of a 'trustless' trading system, guaranteed by mathematical algorithms, can be said to be the best conceptual economic revolution that humankind can ever conceive, and sometimes even beautiful

However, as we have seen above, there are obvious factors to overcome. Our focus is on improving ‘efficiency’ and ‘usability’. We believe that it is our task to make it possible for real customers to easily utilize the various transaction demands that are required in reality and the unique characteristics that only the blockchain has.

We will explain the service our DUBU4 Blockchain and Economic System will provide in more detail in terms of the concept and technology.

2.1 Future shape of DUBU4 Blockchain

① Digital ID(Identification)

a A digital ID system that is free from counterfeiting, tampering, and simplifies the complexity of the ID verification process. Users have full control over their own information and determine their own utilization of information. Distributed Ledger Technology minimizes the risk of counterfeiting, tampering, and theft, while simplifying the issuance process to reduce costs and minimize information exposure.

b When you need to use personal information in a variety of fields, you can quickly and easily find data based on the amount of exposure you have allowed yourself, which can significantly reduce the number of steps you need to go through the process of ID verification that must be done through government offices and specific companies

② Digital Stamping

a Application of the consistency of the transaction and time information provided by the blockchain makes it easy to guarantee and verify the submitted original electronic document by simultaneously displaying the hash of the issued electronic document and the transaction hash

b The inefficiency and costly structure of existing third-party certification delegation processes classified as trusting bodies, certification bodies and registrars, etc. can be improved at once, and can provide excellent security for the prevention of fraud and authenticity

③ Provenance

a For enterprise distribution channels, the administrator verification and approval records are managed by a DUBU4 blockchain, allowing monitoring of the entire process at once and streamlining the authentication and authorization process among stakeholders.

b This can be used to promptly check epidemiological studies, origin and manufacturer sources when problems arise due to food degeneration or livestock diseases, etc., and enable effective responses. Due to the distribution information which contains the full information of all steps, integrity-guaranteed information is shared among a wide variety of users who participate in this transaction. Therefore, you can speed up the entire process without a tedious double or triple check.

c It is also possible for consumers to quickly and easily check origin and distribution information, rather than simply believing in the promise of manufacturing and suppliers by eliminating the opacity of source and origin verification

④ Logistics

a Logistics can be considered a huge blockchain involving from manufacturing to sales, to consumers, to public agencies in the middle as a circulating network. In our current approach, the verification and validation procedures required for each step are costing us immense money, apart from the travel time of the actual product or service.

b These problems can result in higher management and distribution costs and, consequently, higher overall distribution costs. This complexity increases exponentially in the case of logistics involving international transactions.

c What if we introduce the efficient blockchain system of DUBU4 here? If contents of all logistics processes is recorded in a transparent blockchain that is impossible to counterfeit and tamper, the communication between the participants of the logistics network can be dramatically improved. Effective monitoring in public institutions will enable transparent and rapid progress of compliance processes such as tariffs, taxes and quarantine. It becomes the foundation on which smart logistics management can be provided to participants throughout production, consumers, and throughout the logistics process.

d From the user's point of view, it is possible to easily monitor the detailed process of the whole one, which is far from the limitation of the existing logistics information inquiry provided by the agency or the supplier, so that the error of the buyer level can be greatly improved

e The DUBU4 blockchain is the foundation for revolutionary changes in logistics.

⑤ Realize uniform, autonomous and effective asset transaction system through Full Stack Governance

a We prepare and provide various systems for efficient transaction of digital assets. We plan to present various technical steps for the seamless exchange of real and digital assets that exist outside the DUBU4 blockchain and assets that exist within the DUBU4 blockchain.

b DUBU4 allows you to easily create assets if a user wants. The asset may be a user-issued Token or a Bridge asset associated with a separate asset. Full-scale support of user-created assets (UCA) enables easy implementation of special-purpose asset transaction systems. Provides Core Assets of DUBU4 itself for the main purpose, and enables users to extend User Assets on their own.

c First of all, we will provide various Gateway and Bridge systems to connect digital assets (bitcoin, etherium, etc.), outside DUBU4 blockchain. This enables DEX and Atomic Swap for DUBU4 Coin Type-1 as a medium of exchange. Real-world types of assets, such as Fiat currency (money) and resources, provide a trusted third party with a dedicated blockchain node to associate with assets within the blockchain.

d This is a concept similar to Ripple or Stellar's Anchors in Paypal or blockchain systems and can be driven by the involvement of a trusted third party. Of course, anchors also all transactions proceed under the same protocol as the blockchain of DUBU4. This application can easily be combined with various payment systems (ATM, Credit Card, etc.) existing in the real world.

⑥ DUBU4 Supports various trading methods through ICO and token issuing system

a The blockchain has now become an era that cannot be discussed except DApp. Users want to create a new trading method that is more appropriate for them than the transactions created with the provided 'basic system'. Also users want to implement unique ideas. DUBU4 will actively support the blockchain ecosystem that develop indigenously by supporting their base token and additional new token issuance and connection with external token when ICO is in progress b Users and companies can freely design their own trading ideas under a guaranteed value system in various directions such as asset type, equity type, and product type

c DUBU4 provides a foundation for the decentralization of services in the economic ecosystem

d By utilizing leverage of utility tokens blockchains, it supports to connect with a variety of services.

e Because it uses utility token regardless of monetary policy, it is relatively free from regulation and easy to understand the usage concept. Users can secure high transparency due to the counterfeit and tamperproof ledgers, and they can preemptively support areas that can improve existing structures and develop and provide the base technology accordingly.

2.2 COIN LAYER OF DUBU4 BLOCKCHAIN

① Coin layer Summary

a Composed of four types of coins

i Coin Type-1

ii Coin Type-2

iii Coin Type-3

iv Coin Type-4

b Four coins will be developed and released in the next three years. We will soon give the official name.

② Coin layer details

a Currently, DUBU4 Blockchain 1 is first developed and tested, and Coin Type-1 will be created on this blockchain. DUBU4 Blockchain 1 is designed as an experimental blockchain which is designed to accommodate the basic part of our blockchain and expand it, which can confirm the compatibility and efficiency of each function. Coin

Type-1 will be issued in a total of 1 billion coins, all of which will be issued in advance and will be held by the Foundation except for approximately 40% of external releases.

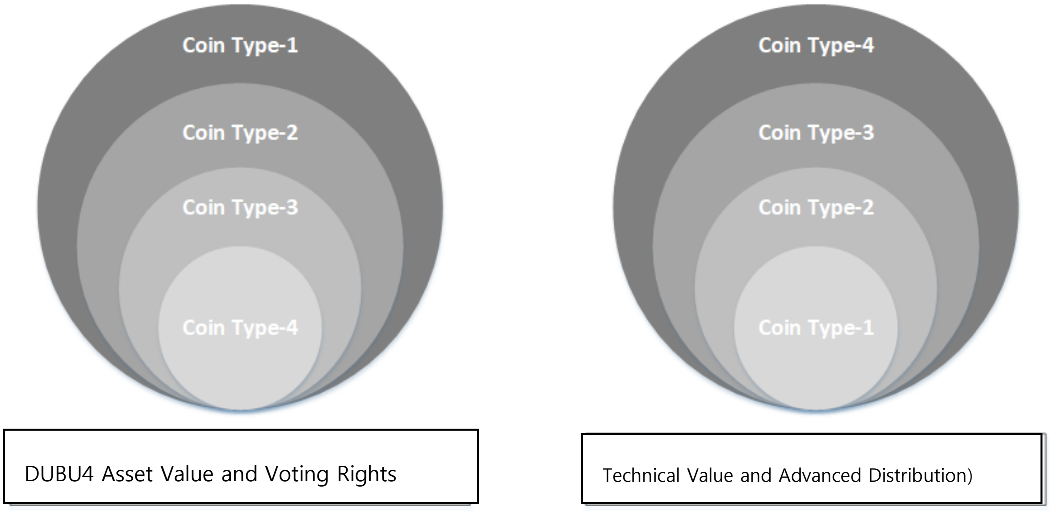
b DUBU4 Blockchain 2 is a full-fledged blockchain. Based on the proven contents of the DUBU4 Blockchain 1 and the various opinions of ICO participants, it will be released after the major improvements and improvements are made. It will serve as a base blockchain for Coin Type-2, 3 and 4 in the future. It can be said that DUBU4 blockchain actually released

c DUBU4 Blockchain 1 continues to exist, and Coin Type-1 will be a bridge coin that links coins and outer coins in the blockchain, which will be developed in the future. Coin Type-1 in DUBU4 has this very important meaning. It is also a promise to hold the first private sale investors and ICO participants as important participants and will serve as a reference coin to evaluate the value of all DUBU4 coins developed in the future

d For example, Witness node operation to be applied to DUBU4 Blockchain 2 will be designed to enable Coin Type-1 to be deposited, and a voting right will be given if important agreement on the direction of development of DUBU4 Blockchain is necessary. In DEX, which we plan to offer, we will exchange or sell our base resources to Atomic Swap as coins that already have value. It is our promise to the owners of Coin Type-1 that all shareholders of DUBU4 come from Coin Type-1.

e CoinType-2 will be designed as a PoS / PoW Hybrid, with 30% Pre-Mined and 70% Mining Liquid. 30% of coin issued is derived from the whole amount of the value of Coin Type-1. If you want to exchange Coin Type-1, coinType-2 coin will be paid after the incineration. Detailed technical specifications of Coin Type-2 will be released in detail through update of the white paper version and the release of the Git-Hub source.

f Coin Type-3, 4 are currently designed and developed with PEG Coin and Bridge-Anchor coin. Detailed technical specifications for this part will be released in a sequential manner in accordance with future roadmap.



<Figure 4. 4 Types Coin value inherence >

2.3 DIRECTION OF DUBU4 BLOCKCHAIN

① DAG based blockchain core - The fastest and lightest blockchain in existence.

a No Blocks with Unlimited Transactions

b Conditional Payment – Conditional payment, simple smart contract available to the public

c Witness Consensus Algorithm – Prevent Double Spending

d Quantum Resistance – Quantum computing resistance

e D4VM – DUBU4 Virtual Machine, Virtual machine support in various languages

② UAM - Unified Assets Management System, Unified asset management system support

a Remittance, Withdraw

b P2P Exchange Market

c Trusted Data Oracle, Third party data feeding system

d Dual Transaction, Dark/White transaction system based on reliability control e Messenger Based Asset management, Text coin Messaging

f Blockchain Schema & Deploy GUI Tool

g Transaction Search

③ DEX – A thoroughly decentralized exchange system

2.4 Core Technology of DUBU4 Blockchain

The DUBU4 blockchain system is aim to be linkable between the main chain and other derived chains with fast transaction and modular system configuration. The underlying algorithm that makes up the main chain uses a DAG-like algorithm. Let's take a closer look at DAGs implemented in DUBU4.

① WHAT IS DAG?

a DAG is simply a directional graph data structure that uses topological ordering. The order of the entities is a constant direction, and there is no reverse order, so a circular structure is not created. It is a data structure that is mainly used for data processing, scheduling, optimal path finding, and data compression.

b Bitcoin has an inefficient data structure due to limitations of Proof-of-Work systems. Blocks cannot be created at the same time, and there is only one connection data structure available across the entire network. All transactions occurring in similar time zones around the node are recorded in the same block and adopted as a formal block with transactions containing only those blocks that have acquired block integrity by the miner. Transactions that are not included in a successful block in the Proof of Work are switched to the 'Unconfirmed' state and passed to the next block creation. All of this is done in every 10 minute. Unacceptable transactions may require hours to days.

c NXT makes an attempt to improve this inefficient structure and reconfigure a chain of data structures into a DAG format for the first time. It was the idea to expand the number of blocks on the network several times without changing the mining time. Nevertheless, it was the character of side-chains at this time, and still borrowed the concept of block. It was only an approach to deal with different types of transactions concurrently in different chains, and in fact, this side-chain is now being used as a complement to existing block-chain 1.0 and 2.0 technologies

d However, the block creation time, bottleneck is still not resolved. Bitcoin requires every 10 minutes, and Ethereum, a little better, more drink needs 15-20 seconds. These blockchain systems put a lot of transactions into a block and the transaction sequences are connected and maintained by block-to-block hashes. However, we started from the fundamental question "why should we make a block?" And started to find a solution." What if we deal with transactions and blocks at once?" "'Are not all transactions itself directly used to maintain the entire sequence as a single block?" "'If the transaction is authenticated, the process of mining can be omitted at once, and can it be a more efficient system of a single transaction base that does not need the block itself?' DAG is born from all these questions.

e This is a blockless blockchain system, Blockless-DAG.

② Technical issues of DAG

a Solving the fundamental problem of double-spending

i In a DAG, there can be more than one Miner that resolves the hash function at the same time. DAG is a system in which a new transaction verifies the previous (at least) two transactions. At this time, it verifies the validation of the transaction that occurred at the same time with the number of transactions connected (or 'vote'). It resolves problem of double-spending with a structure where transactions that are associated with more transactions are adopted.

b Network bandwidth

i When each transaction is verified, it must be connected with the previous transactions included in the existing network. At this time, if the transaction is linked with the previous transaction node, there is a problem that the route of the transaction to be verified becomes long and the network itself becomes too large. Therefore, the DAG network has an algorithm to connect the old node to be connected to the relatively recent node when a new transaction occurs. Its purpose is to keep the network within a certain range and to quickly verify new transactions

c Quick transaction

  - i Since DAG does not generate blocks, the transaction itself is inserted directly into the network and the transactions are performed much faster than PoW and PoS based blockchain as a whole

- d Unnecessary mining

  - i DAG does not have Miner. Transaction validation occurs in the transaction itself. For users, this means that transaction closes almost immediately.

- e Micro-Payment

  - i It is advantageous for small immediate settlement. Due to the structural nature of the DAG, you can drive high skill of functions with minimal commission. You can build a much more flexible, faster, and more affordable payment system than Bitcoin or Etherium, which costs more when you pay a small fee. Therefore, you can dramatically expand the areas you can actually use.

- f Application Scalability

  - i DAG can also be useful for applications that require thousands of transactions per second. Ethereum's DApp called CryptoKitties is powered by its tremendous popularity, resulting in a whole network of Ethereum having slower and more expensive commissions. Even though Ethereum has offered a solution called Sharding, it has been five years and has not been solved fundamentally. DAG can be a new alternative in developing DApp.

3 DUBU4 Blockchain Technical Detail

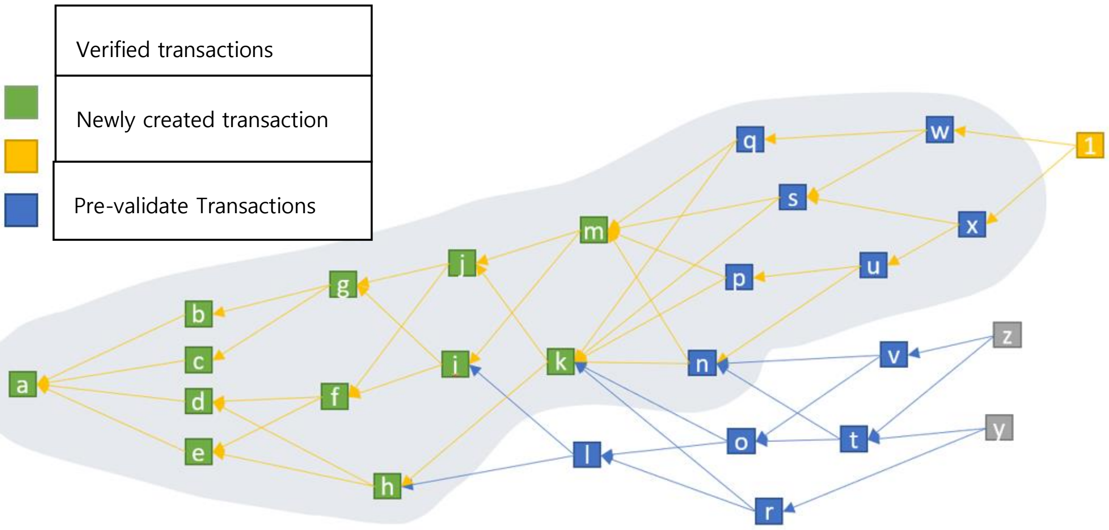
3.1 DUBU4 Core

① Flexibility, agility, integration

a At this point, the blockchain is not much different from the technology at its starting point, and the data size of the old blockchain platform grows so much. Therefore, the time and cost of processing a single transaction is increasing day by day. For this reason, it is true that the combination of real business sectors and the blockchain systems so far has had a difficult time impacting on actual business. Here is the starting point for developing a DUBU4 blockchain. The DUBU4 blockchain core is based on DAG technology to enable anyone to use the blockchain technology in combination with existing environments and business, away from the current state of the block chain, which is merely coined above the blockchain technology. Also 9.7K TPS completes transactions quickly and ensures the integrity of its data.

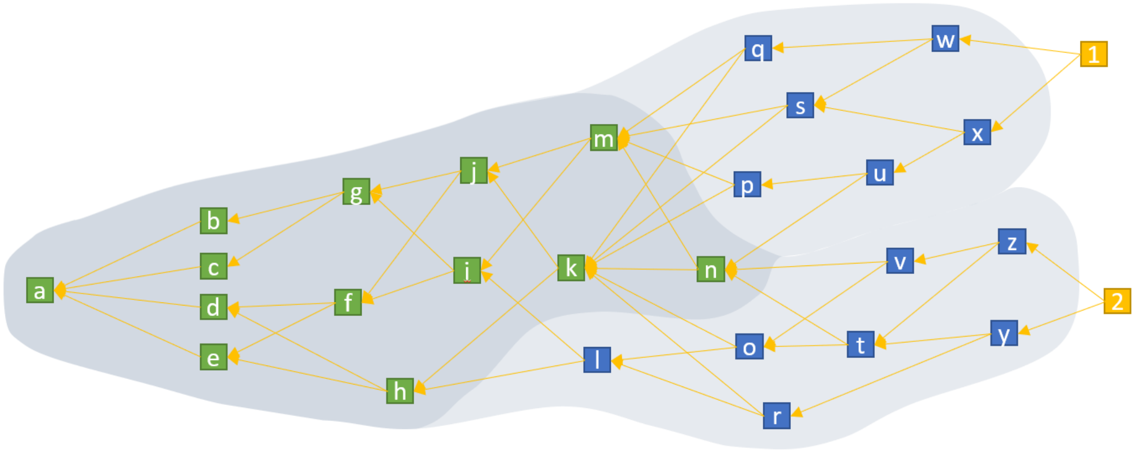
b The DUBU4 blockchain is designed to make it easy for users to create their own independent network from the beginning of the design and anyone can configure coins and networks including technical contents that they want by using the development tools provided in GUI form,

c In addition, all of these networks can be transformed and developed independently, and all of them can easily be combined with the DUBU4 main network to complete the DUBU4 enterprise.



To add a new transaction 1, you need to randomly select two transactions w and x, and then verify them. In addition to verification, the transaction is checked for conflicts with past transactions that it directly or indirectly refers. If there is no problem with the selected transaction, the user adds a new transaction 1 to the entire chain, referring to the two transactions w and x. The transaction (l, o, r, t, v, y, z outside the gray bounds) that is not directly or indirectly referenced by two transactions selected w and x is not verified as 1 is added to the transaction. These transactions are verified later when another transaction is added

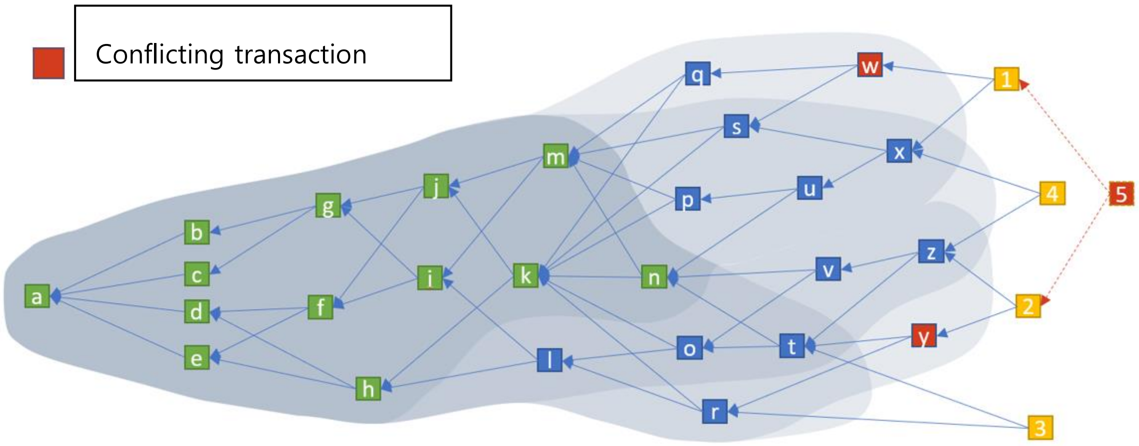
<Figure 5. DUBU4 DAG Transaction processing >



Overlap the verification path by 1 and 2 as shown above. Some transactions are validated by either 1 or 2, and some transactions are validated both 1 and 2. It is said that transactions that have been verified and completed by all of the existing transactions at that point in time are 'validated'. Therefore n is now fully completed and goes deeper into DUBU4 then changes to verified (green square). In addition, child transactions added to 1 or 2 continue to revalidate n.

<Figure 6. DUBU4 DAG Transaction Verification Complete Process>

>



Suppose that you have two conflicting transactions w and y in different areas of the DUBU4 blockchain. Subsequent transactions are likely to include only one of the conflicting transactions w and y in the verification path because of the selection or propagation delay of the verification transaction.

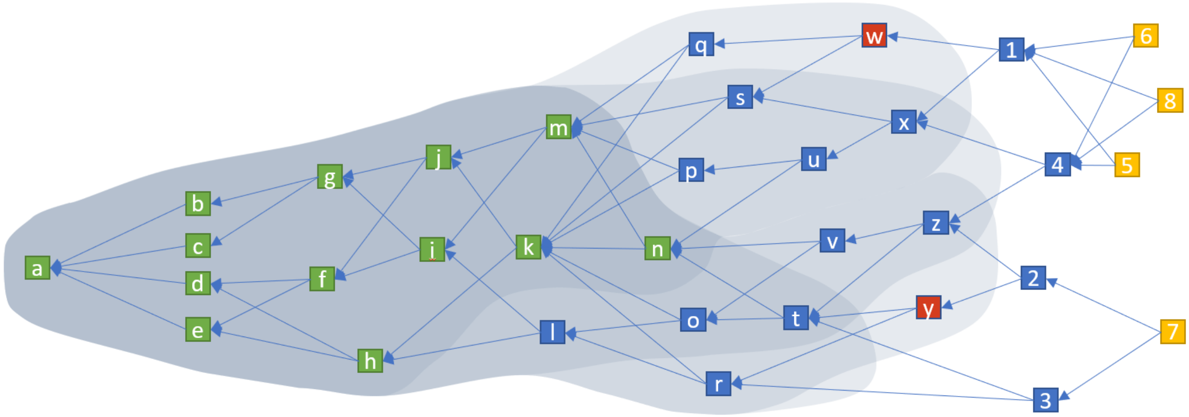
For example, a user adding 1 and a user adding 2 will not know that w and y are in conflict, and will consequentially determine w and y as valid, non-conflicting transactions.

But the conflict will soon be discovered. If 5 that refer to 1 and 2 is added, then 5 will see conflicts because 5's verification path includes both w and y. So 5 will not select 1 and 2 and will reselect the other two transactions without conflicts. This is because 5 itself can be vilified as a valid transaction by later transactions

Because many users, including only one of w and y in the verification path, can not find a conflict between w and y before the conflict is apparently found in the validation process, it is possible to recognize w and y as valid transactions

However, primarily, only one of w and y is committed, and the other is discarded eventually, depending on whether users add a new transaction to either the transaction that includes w in the verification path and the transaction that contains y in the verification path. Although transactions added to the abandoned side did not know that there was a conflict, they are also thrown away together. However, those discarded transactions will not disappear from the DUBU4 blockchain at all, but they will always be selected, re-added and validated by other users.

<Figure7. DUBU4 DAG Transaction double payment>



In the previous double-payment problem, users tried to add 5 to 1 and 2, but found that w and y conflicted. Therefore, they chose another transaction again to select 1 and 4, and no conflicts were found for 1 and 4. As a result, 5 was added to the DUBU4 blockchain by 1 and 4. Other users (not necessarily other users) have added 7 to 2 and 3. This will result in a branch with a path containing w and two paths containing y. However, one of them will be discarded and only one will survive, as described in the previous double payment section. Random selection logic that takes into account the cumulative weights of the transactions will add more offspring transactions to one of the two-branched paths. And over time, the selection algorithm that consider the cumulative weights makes it impossible to add transactions in the normal way to one path. In the previous figure, new transactions can be added after 5, 6, and 8, but no transactions can be added after 7. So y, 2, 3, 7 will no longer be validated and cannot be verified. As described in the double payment problem, y, 2, 3, and 7 in the discarded path can be added back to the chain once they have been detached from the DUBU4 blockchain network and then verified by other new transactions. If y, 2, 3, and 7 each are valid transactions, they can be finalized like any other normal transaction. Therefore 2, 3, 7 can be confirmed, but y with collision content cannot be finalized.

<Figure8. DUBU4 DAG Transaction double payment resolution>

3.2 Transparency and Anonymity

① DUBU4 blockchain supports transparency, anonymity, and both values

a DUBU4-Public

i The DUBU4 public chain is a DAG-based minimum node cross-validation scheme. The nodes of the chain that are connected to the new transaction and the ones of the selected minimum unit among the intersected nodes complete the transaction through quick verification. This approach ensures 100% consensus mechanism between the selected nodes compared to existing POW and POS based blockchains, thus ensuring data transparency and not slowing down

b DUBU4-Private

i In the case of the DUBU4 private chain, it is designed with a focus on combining it with real business, which should provide fast and accurate service rather than focusing on transparent and open data for any public purpose or for all.

ii In the private chain, all the transactions can be managed and verified by the authentication server managed by the chain manager alone, and the transactions can be completed. As a result, compared with the existing methods, the speed is not behind in performing the business logic It does not lag behind iii In addition, the node members in the private chain can view the data of the completed transaction and if necessary, the authentication server alone does not process the transaction. The administrator can simply add and change the method of performing additional verification that a verification member node currently selected in the private chain or the arbitrary minimum node selects the transaction validated by authentication server

3.3 DUBU4 BLOCKCHAIN – CONSENSUS

① Chain Scheme

a Our DAG is a special DAG. In normal use, people mostly link their new units to slightly less recent units, meaning that the DAG grows only in one direction. One can picture it as a thick cord with many interlaced wires inside. This property suggests that we could choose a single chain along child-parent links within the DAG, and then relate all units to this chain. All the units will either lie directly on this chain, which we'll call the main chain, or be reachable from it by a relatively small number of hops along the edges of the graph. It's like a highway with connecting side roads. One way to create a main chain is to develop an algorithm. One way to build a main chain is to develop an algorithm that, given all parents of a unit, selects one of them as the "best parent". The selection algorithm should be based only on knowledge available to the unit in question, i.e. on data contained in the unit itself and all its ancestors. Starting from any tip (a childless unit) of the DAG, we then travel backwards in history along the best parent links. Traveling this way, we build a main chain and eventually arrive at the genesis unit. Note that the main chain built starting from a specific unit will never change as new units are added. This is because on each step we are traveling from child to parent, and an existing unit can never acquire new parents. If we start from another tip, we'll build another main chain. Of note here is that if those two main chains ever intersect while they go back in history, they will both go along the same path after the intersection point. In the worst case, the main chains will intersect only in genesis. Given that the process of unit production is not coordinated among users, however, one might expect to find a class of main chains that do converge not too far from the tip

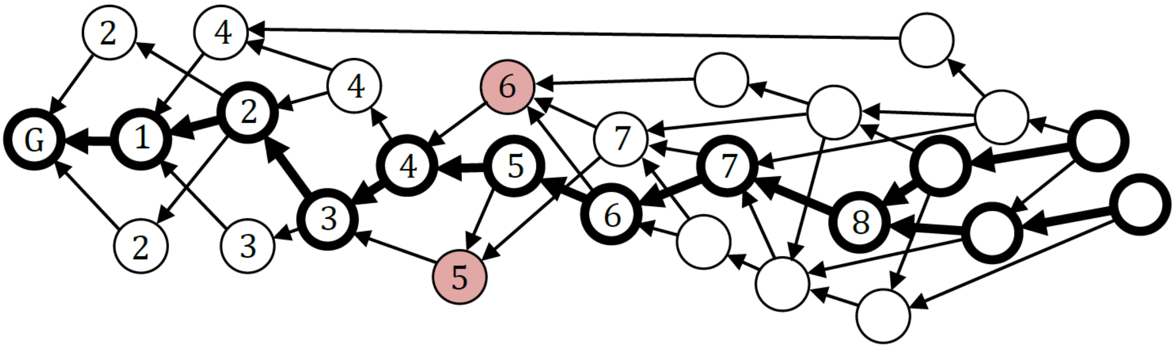


Figure n. Main chains built from different childless units intersect and then go along the same path. Of the two double-spends, the one with the lower main chain index (5) wins, while the other (with MCI=6) is deemed invalid.

Once we have a main chain, we can establish a total order between two conflicting non serial units. Let's first index the units that lie directly on the main chain. The genesis unit has index 0, the next CS unit that is a child of genesis has index 1, and so on traveling forward along the CS we assign indexes to units that lie on the CS. For units that do not lie on the CS, we can find an MC index where this unit is first included (directly or indirectly). In such a way, we can assign an MC index (MCI) to every unit. Then, of the two non-serials, the one that has a lower MCI is considered to come earlier and deemed valid, while the other is invalid. If both non serials happen to have the same MCI, there is tiebreaker rule that the unit with the lower hash value (as represented in base64 encoding) is valid. Note that we keep all versions of the double-spend, including those that eventually lose. Dag Coin was the first published work that suggested storing all conflicting transactions and deciding which one to treat as valid. The MC built from a specific unit tells us what this unit's author thinks about the order of past events, i.e. his point of view about the history. The order then implies which non serial unit to consider valid, as described above. Note that by choosing the best parent among all parents of a given unit, we are simultaneously making a choice among their MCs: the MC of the unit in question will be the MC of its best parent extended forward by one link. Recognizing that many (or even all) parent units might be created by an attacker, and remembering that the choice of best parent is essentially the choice among versions of history, we should require from our best parent selection.

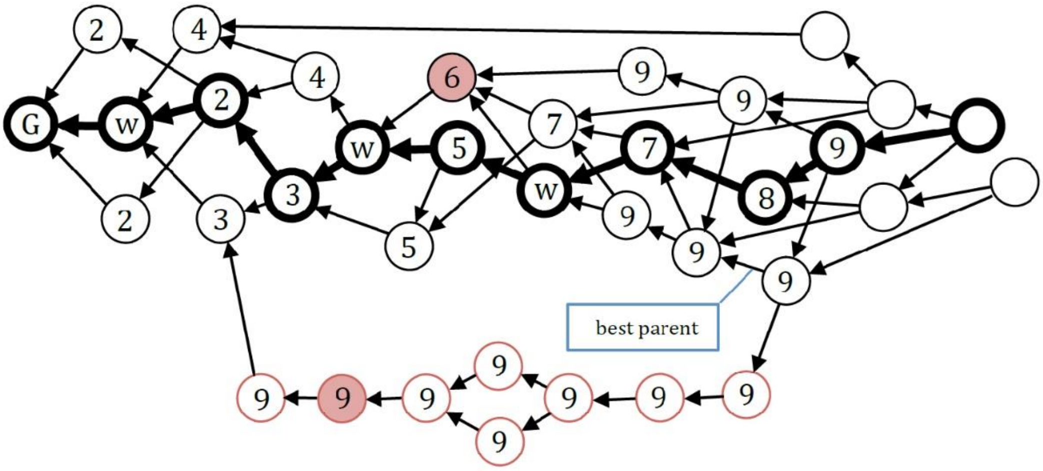
② Witness

"Looking for a “reality test”, observe that some of the participants of our network are non-anonymous reputable people or companies who might have a long established reputation, or they are businesses interested in keeping the network healthy. We’ll call them witnesses. While it is reasonable to expect them to behave honestly, it is also unreasonable to totally trust any single witness. If we know the DUBU4 addresses of several witnesses, and also expect them to post frequently enough, then to measure the reality of a candidate CS one might travel along the CS back in time and count the witness-authored units (if the same witness is encountered more than once, he is not counted again). We would stop traveling as soon as we had encountered the majority of witnesses. We would then measure the length of the longest path on the graph from the point at which we stopped to the genesis. We’ll call this length the level of the unit where we stopped, and the witnessed level of the parent whose CS we are testing. The candidate CS that yields the greater witnessed level is considered more “real”, and the parent bearing this CS is selected as best parent. In case there are several contenders with a maximum witnessed level, we would select the parent whose own level is the lowest. If the tie persists, we would select the parent with the smallest unit hash (in base64 encoding). This algorithm allows the selection of the MC that gravitates to units authored by witnesses, and the witnesses are considered to be representative of reality. If, for example, an attacker forks from the honest part of the network and secretly builds a long chain of his own units (shadow chain), one of them containing a double-spend, and later merges his fork back into the honest DAG, the best parent selection algorithm at the merger point will choose the parent that drives the CS into the honest DAG, as this is where the witnesses were active. The witnesses were not able to post into the shadow chain simply because they didn’t see it before the merger. This selection of CS reflects the order of events as seen by the witnesses and the user who appointed them. After the attack is over, the entire shadow chain will land on the CS at one point, and the double-spend contained in the shadow chain will be deemed invalid because its valid counterpart comes earlier, before the merger point. This example shows why the majority of witnesses has to be trusted to post only serially. The majority should not collude with the attacker and post on his shadow chain. Note that we trust the witnesses only to be signs of reality and to not post non serial units on any shadow chains. We are not giving any of them control over the network or any part thereof. Even for this small duty, it is users who appoint the witnesses and they can change their decisions at any time. The idea of looking at some known entity as a sign of reality is not new. It has long been known, and some companies have engaged in such activity, that to prove that some data existed before a specific date, one can hash the data and publish the hash in some hard-to-modify and widely witnessed media, like printed newspaper. Witnesses in DUBU4 serve the same function as the newspaper. Like newspapers, they are well known and trusted. As for newspapers where trust is limited to trusting them to publish the data they are given, witnesses in DUBU4 are only trusted to post serially, and not much more. Like newspapers, witnesses don't know what's behind the hashes they are witnessing and have few reasons to care. Newspapers are hard to modify (but possible, and in 1984 they do it), while everything produced by witnesses is protected by digital signatures, which makes any modifications impossible. For reliability, we have several witnesses, not just one, and for speed and convenience, these are online. Having decided on a list of witnesses, we can then select best the parent and the corresponding history that best fits the definition of reality as "somewhere where these witnesses live". At the same time, the parents themselves might have different witness lists and consequently different definitions of reality. We want the definitions of reality, and histories that follow from them, to converge around something common. To achieve this, we introduce the following additional protocol rule. The "near-conformity rule": best parents must be selected only among those parents whose witness list differs from the child's witness list by no more than one mutation. This rule ensures that witness lists of neighboring units on the MC are similar enough, therefore their histories mostly agree with one another. The parents whose witness list differs by 0 or 1 mutation will be called compatible (with the unit that includes them directly), while the others are incompatible. Incompatible parents are still permitted, but they have no chance of becoming best parent. If there are no compatible potential parents among childless units (an attacker could flood the network with his units that carry a radically different witness list), one should select parents from older units. The above means that each unit must list its witnesses so that they can be compared. We require that the number of witnesses is exactly 12. This number 12 was selected because: It is sufficiently large to protect against the occasional failures of a few witnesses (they might prove dishonest, or be hacked, or go offline for a long time, or lose their private keys and go offline forever);

i it is sufficiently large to protect against the occasional failures of a few witnesses (they might prove dishonest, or be hacked, or go offline for a long time, or lose their private keys and go offline forever);

ii it is sufficiently small that humans can keep track of all the witnesses to know who is who and change the list when necessary;

iii the one allowed mutation is sufficiently small compared with the 11 unchanged witnesses.



<Figure. n> When an attacker rejoins his shadow DAG into the lit DAG, his units lose competition to become best parent as the choice favors those paths that have more witnesses (marked with w).

③ Light clients

a Light clients do not store the entire dubu4 database. Instead, they download a subset of data they are interested in, such as only transactions where any of the user's addresses are spending or being funded. Light clients connect to full nodes to download the units they are interested in. The light client tells the full node the list of witnesses it trusts (not necessarily the same witnesses it uses to create new units) and the list of its own addresses. The full node searches for units the light client is interested in and constructs a proof chain for each unit in the following way:

i Walk back in time along the CS until the majority of requested witnesses are met. Collect all these CS units.

ii From the last unit in this set (which is also the earliest in time), read the last set.

iii It starts from the last CS and walks backwards in time back to CS until it becomes a block. It meets skiplist. Collect all these blocks.

iv Using the skiplist, jump to an earlier block referenced from the skiplist. This ball also has a skiplist, jump again. Where there are several blocks in skiplist array, always jump by the largest distance possible, so we accelerate jumping first by 10 indexes, then by 100, then by 1000, etc.

v If the next jump by the skiplist would throw us behind the target ball, decelerate by jumping by a smaller distance. Ultimately, leave the skiplist and walk along the CS one index at a time using just parent links. This chain can be trusted because it has witness building units at first. From the light client's point of view, all elements in the chain are displayed either as a parent unit link (witness accumulation), as a last block reference, as a parent block link, or as a skiplist link. At the end of the chain, we have a unit whose presence must be proven.

④ Skiplist

a Some of the blocks contain a skiplist array which enables faster building of proofs for light clients (see below). Only those blocks that lie directly on the CS, and whose CS index is divisible by 10, have a skiplist. The skiplist lists the nearest previous CS blocks whose index has the same or smaller number of zeros at the end. For example, the blocks at CSI 190 has a skiplist that references the block at CSI 180. The block at CSI 3000 has a skiplist that references the block at CSI 2990, 2900, and 2000.

⑤ Multilateral signing

a A unit can be signed by multiple parties. In such instances, the authors array in the unit has two or more elements. This can be useful, for example. if two or more parties want to sign a contract (a plain old dumb contract, not a smart one). They would both sign the same unit that contains a text message (app='text'). They don't have to store the full text of the contract in the public database, and pay for it – a hash would suffice (payload_location='none'), and the parties themselves can store the text privately. Another application of multilateral signing is an exchange of assets. Assume user A wants to send asset X to user B in exchange for asset Y (the native currency 'bytes' is also an asset – the base asset). Then they would compose a unit that contains two payment messages: one payment sends asset X from A to B, the other payment sends asset Y from B to A. They both sign the dual-authored unit and publish it. The exchange is atomic – that is, either both payments execute at the same time or both fail. If one of the payments appears to be a double-spend, the entire unit is rendered invalid and the other payment is also deemed void. This simple construction allows users to exchange assets directly, without trusting their money to any centralized exchanges.

⑥ Address

a Users are identified by their addresses, transaction outputs are sent to addresses, and, like in Bitcoin, it is recommended that users have multiple addresses and avoid reusing them. In some circumstances, however, reuse is normal. For example, witnesses are expected to repeatedly post from the same address. An address represents a definition, which is a Boolean expression (remotely similar to Bitcoin script). When a user signs a unit, he also provides a set of authentifiers (usually ECDSA signatures) which, when applied to the definition, must evaluate it to true in order to prove that this user had the right to sign this unit. We write definitions in JSON. For example, this is the definition for an address that requires one ECDSA signature to sign: ["sig",{"pubkey":"Ald9tkgiUZQQ1djpZgv2ez7xf1ZvYAsTLhudhvn0931w"}] The definition indicates that the owner of the address has a private key whose public counterpart is given in the definition (in base64 encoding), and he will sign all units with this private key. The above definition evaluates to true if the signature given in the corresponding authentifier is valid, or otherwise false. The signature is calculated over all data of the unit except the authentifiers. Given a definition object, the corresponding address is just a hash of the initial definition object plus a checksum. The checksum is added to avoid typing errors. Unlike usual checksum designs, however, the checksum bits are not just appended to the end of the uncheck summed data. Rather, they are inserted into multiple locations inside the data. This design makes it hard to insert long strings of illegal data in fields where an address is expected. The address is written in base32 encoding. The above definition corresponds to address. Example: A2WWHN7755YZVMXCBLMFWRSLKSZJN3FU.

b When an address is funded, the sender of the payment knows and specifies only the address (the check summed hash of the definition) in the payment output. The definition is not revealed and it remains unknown to anyone but the owner until the output is spent. When a user sends his first unit from an address, he must reveal its definition (so as to make signature verification possible) in the authors array:

```
unit: {
    …
    authors: [ {
            address: 'DJ6LV5GPCLMGRW7ZB55IVGJRPDJPOQU6',
            definition: [
                    "sig",
                    {"pubkey":"AsnvZ3w7N1lZGJ+P+bDZU0DgOwJcGJ51bjsWpEqfqB
                    g6"}
            ],
            authentifiers: {
                    r:
                    '3eQPIFiPVLRwBwEzxUR5thqn+zlFfLXUrzAmgemAqOk35UvDpa4h
                    79Fd6TbPbGfb8VMiJzqdNGHCKyAjl786mw=='
            }
        } ],
    …
}
```

c If the user sends a second unit from the same address, he must omit the definition (it is already known on Byteball). He can send the second unit only after the definition becomes stable, i.e. the unit where the definition was revealed must be included in the last ball unit of the second unit. Users can update definitions of their addresses while keeping the old address. For example, to rotate the private key linked to an address, the user needs to post a unit that contains a message such as:

```
unit: {
    …
    messages: [
            …
            {
                    app: "address_definition_change",
                    definition_chash: "I4Z7KFNIYTPHPJ5CA5OFC273JQFSZPOX"
            },
            …
    ],
    …
}
```

d Here, definition_chash indicates the checksummed hash of the new address definition (which is not revealed until later), and the unit itself must be signed by the old private keys. The next unit from this address must: After the change, the address is no longer equal to the checksummed hash of its current definition. Rather, it remains equal to the checksummed hash of its initial definition. The definition change is useful if the user wants to change the key(s) (e.g. when migrating to a new device) while keeping the old address, e.g. if this address already participates in other long-lived definitions (see below).

i include this address_definition_change unit in its last unit, i.e. it must be already stable;

ii new definition in the authors array in the same way as for the first message from an address.

⑦ Delegation to other addresses

a An address can contain reference to another address.

b Delegating signing to another address is useful for building shared control addresses (addresses controlled by several users). This syntax gives the users the flexibility to change definitions of their own component addresses whenever they like, without bothering the other user

```
["and", [
                ["address", "ADDRESS 1 IN BASE32"],
          ["address", "ADDRESS 2 IN BASE32"]
]]
```

3.4 Supported Development with Multi Language

① Unnecessary to learn new language for blockchain development

a Many blockchain technologies support only one kind of development language. However, for the DUBU4 blockchain, all libraries including cores are supported in the languages listed below

i Go

ii Python

iii Java

iv Node.js

v Continuous addition in the future

3.5 GUI Development Tool

① Blockchain that anyone can use

a Most of the blockchain technology is code-based, therefore it's hard to materialize it when an ordinary person who has not studied the programming language has any ideas.

b The DUBU4 blockchain aggregates all libraries including cores into a GUI development tool so that these users can create and retain their own coins and networks without typing a single line of code directly.

① GUI development tool function list

a Main net creation

i Private Network

ii Public Network

b Coin Creation

i Coin naming granted

ii Coin quantity confirmation

iii Coin increase / decrease after coin generation

c Choosing and granting consensus algorithms

i Based on DUBU4 DAG core

ii POW

iii POS

iv DPOS

v POI

vi CA server verification etc.

3.6 Atomic Swap P2P Exchange

① Transaction without fee

a. The DUBU4 block chain opens the Atomic Swap Exchange, which supports more than 30 major coins. All users with 4 coins of DUBU4 and 30 coins that are supported by DUBU4 Atomic Exchange will not be charged any fees through our exchanges, and direct exchanges of coins are possible if the exchange ratio of users is only agreed.

② Based on Hashed Time-locked Contract

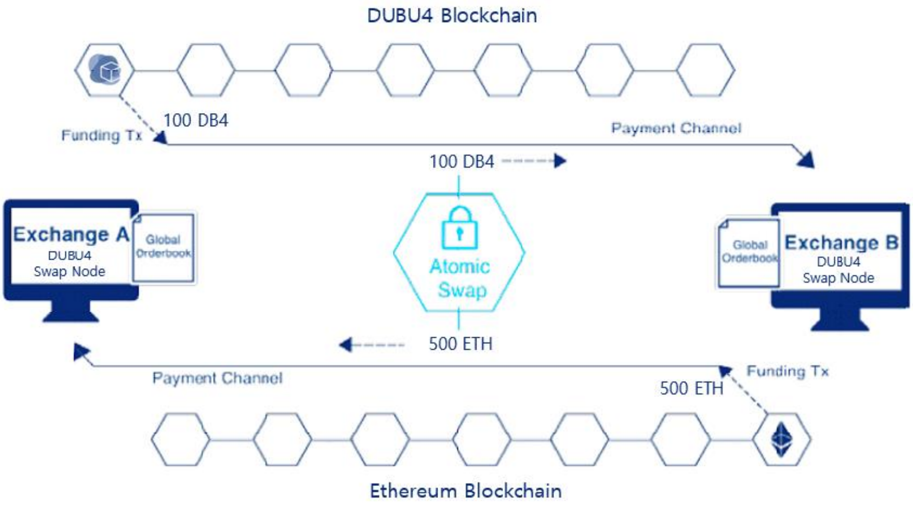
a DUBU4 Atomic Swap requires that the recipient of the transaction acknowledge receipt of payment based on the Hashed Time-locked Contract, which is part of the scripting language used for most existing encryption functions and also the recipient acknowledges the fact all procedures are proof of encryption.

③ Technical description of Hashed Time-locked Contract

a If a trader who owns a coin A and a trader B who owns a coin B, A creates on the A coin block chain that the A coin is transmitted, and B writes on the B coin block chain that it sends the B coin. At this time, if transaction channel A or B is using time-locked technology at the time of transaction, it will use Hash-locks function because of HTLC. In this state, the recipient of the transaction publishes their hash value and finds the public hash value of the coin exchanged. Through this process, coin transactions between traders become possible, even though traders are on two or more different block chains. Additionally, using the HTLC in a coin transaction allows the recipient to confiscate the right to receive a coin for the transaction placed on hold by the transaction recipient. As a result, the recipient can get the money back more effectively for pending transactions.

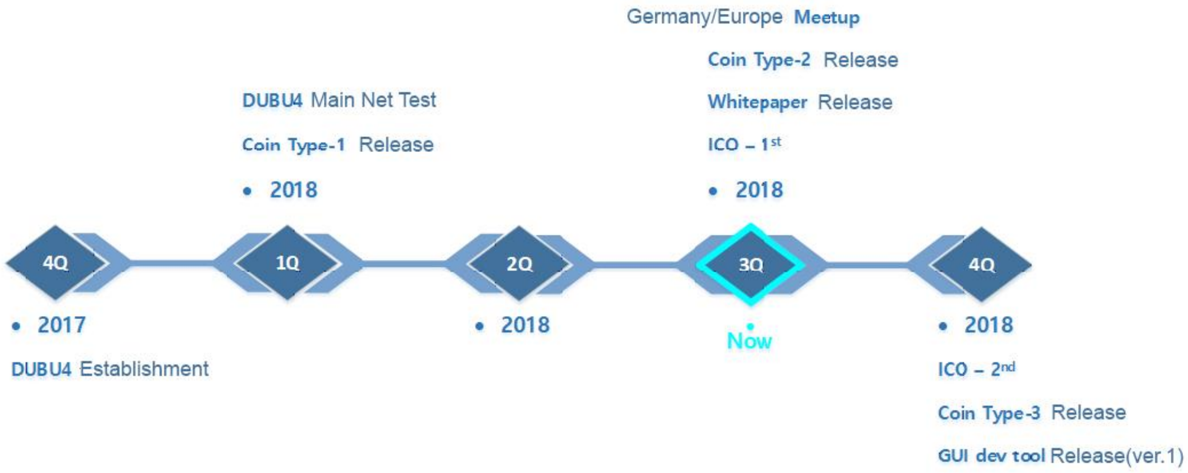
④ Coin List

a DUBU4 A list of coins that can be traded directly on the Atomic Exchange will be released following future whitepaper updates.


DUBU4 Blockchain
100 DB4
Funding Tx
Payment Channel
100 DB4
Exchange A
DUBU4
Swap Node
Global
Orderbook
Atomic
Swap
Global
Orderbook
Exchange B
DUBU4
Swap Node
500 ETH
Payment Channel
Funding Tx
500 ETH
Ethereum Blockchain

<Figure9. DUBU4 Atomic Swap Exchange Structure>

4 Roadmap



<Figure10. DUBU4 Roadmap 2017-2018>

4.1 4Q, 2017 – completed

① Establishment of DUBU4 Foundation

② Establishment and design of core value of DUBU4 block chain

③ Blockchain Based Technology R & D

4.2 1Q, 2018 – Completed

① Coin Type-1 -Release

② DUBU4 Main net (Prototype) Test

4.3 2Q, 2018 – Completed

① Private sale progress (Coin Type-1)

② DUBU4 Core detail R&D

4.4 3Q, 2018 – Progress

① Coin Type-2 -Release

② Whitepaper -Release

③ ICO 1st – in Progress

④ Germany / Europe Meetup in Progress

4.5 4Q, 2018 – Expected

① Coin Type-3 -Release

② ICO 2nd – in Progress

③ GUI dev tool –Release (Version 1)

5 Reference

5.1 Explanation of terminology

① Cryptocurrency: An electronic currency that uses cryptography for secure transactions in a P2P (Peer-to-Peer) network.

② DAG (Directed Acyclic Graph): This is a directional acyclic graph, which means that data is verified and combined in parallel, in the form of directional acyclic graphs, rather than being serially verified or combined, as in a typical blockchain.

③ Transaction: A single transaction occurring within a blockchain.

④ POW (Proof-Of-Work): (P2P: Peer-to-Peer) : A simple way of verifying between participating parties to trust the computational work performed on a network over time or at a cost. Also a blockchain applies information to a random nonce and a hash algorithm in order to obtain a value smaller than the hash of the set size, which proves the completion of additional new block to the blockchain.

⑤ POS (Proof-Of-Stake): In a blockchain technology context, as a proof of having equity in any asset, it is used as a representative example of how to replace POW with POS.

5.2 Technical Reference

[1] Colin LeMahieu, Nano, "Nano's white paper", https://raiblocks.net/media/RaiBlocks_Whitepaper__English.pdf, 2017

[2] Anton Churyumov, "Byteball's white paper", https://byteball.org/byteball.pdf, 2016

[3] Ethereum Foundation, "Ethereum's white paper", https://github.com/ethereum/wiki/wiki/White-Paper, 2014

[4] Satochi Nakamoto, "Bitcoin: A peer-to-peer electronic cash system", http://bitcoin.org/bitcoin.pdf, 2008

[5] Serguei Popov, "The tangle," 2016