Blockchain for modern economic solutions

W H I T E P A P E R

Table of content

1. ExecutiveSummary

DON Token is the cryptocurrency of a distributed ledger which links block-based and blockless blockchain systems

The UTXO-based blockchain system (e.g. Bitcoin [1]) and account-based blockchain system (e.g. Ethereum [2]) has opened the door of a brand-new world for us. Although the impressive success of Bitcoin and Ethereum has certainly proven the value of blockchain technology and its massive potential in the future, we also see some inherent problems in blockchain technology along the way. Since 2015, there have been quite a few highly-promising distributed ledger systems that are not block-based gradually coming into our view, such as DAG (Directed Acyclic Graph) [3]. With no doubt, a decentralized digital world is dawning, and Bitcoin or Ethereum has the potential to become the base currency in a block-based distributed ledger. Nevertheless, despite the ability to be traded unrestrictedly on some centralized exchange platforms, these tokens, due to the fundamental di"erences in the underlying systems, can only circulate within their own blockchains, and would not be able to move freely from blockchain-based to blockless system or vice versa.

Our intention is to create a new decentralized and distributed ledger system that will bridge the gap between blockchain-based or blockless systems, thereby allowing value and information to be circulated freely between di"erent blockchains. In addition, just as Bitcoin serves as the tools of exchange for goods or services in blockchain-based system, we also need a type of asset in the newly invented system that can reflect the value of goods or services objectively. As to the new store of value, we call it "ERD Token"

2. Company

THE DON COMMUNITY

The DON community is a Blockchain solution providing company, transforming clients' business, operating and technology models for the digital era. Our unique industry-based, consultative approach on Blockchain technology helps clients envision, build and run more innovative and efficient businesses. Headquartered in the U.K.

DON Team is expertise in providing Customized blockchain solutions for your business needs. There are 50+ Mainstream clients being served and maintained from 2 years.

Services

Blockchain Frameworks
Blockchain Banking
Blockchain Enterprising
Blockchain Cryptocurrency
Blockchain Hospitality
Blockchain Security

DON procures a good infrastructure and team of Blockchain and business A great combination of technology and business.

3 Introduction

In our vision, DON will create a new platform that can be connected to di"erent blockchains (such as Bitcoin blockchain and Ethereum blockchain), thereby allowing value and information to circulate freely among systems, and redefining the value of blockchain

Below is a schematic diagram of the DON platform.

Hive:Composedof Blockchainand DAGsystems

DON platform is designed to be the sidechain for both blockchain-based and blockless systems, so it can achieve a free flow of value and information between the two. Here, DON is the medium for cross-platform value exchange, while the platform itself is a carrier for cross-platform information interflow.

Based on these design features, DON has taken into account the reading of information from blockchain- based (including UTXO and Account Based) and DAG based distributed ledger at the initial stage of system design.

Addres system

In order to implement another important feature that will be discussed later, DON is designed purposely to have both public and private addresses to be compatible with third party address. Therefore, in the near future, it is expected that people can directly send and receive DON tokens from blockchain to the DAG system.

About Directed Acyclic Graph

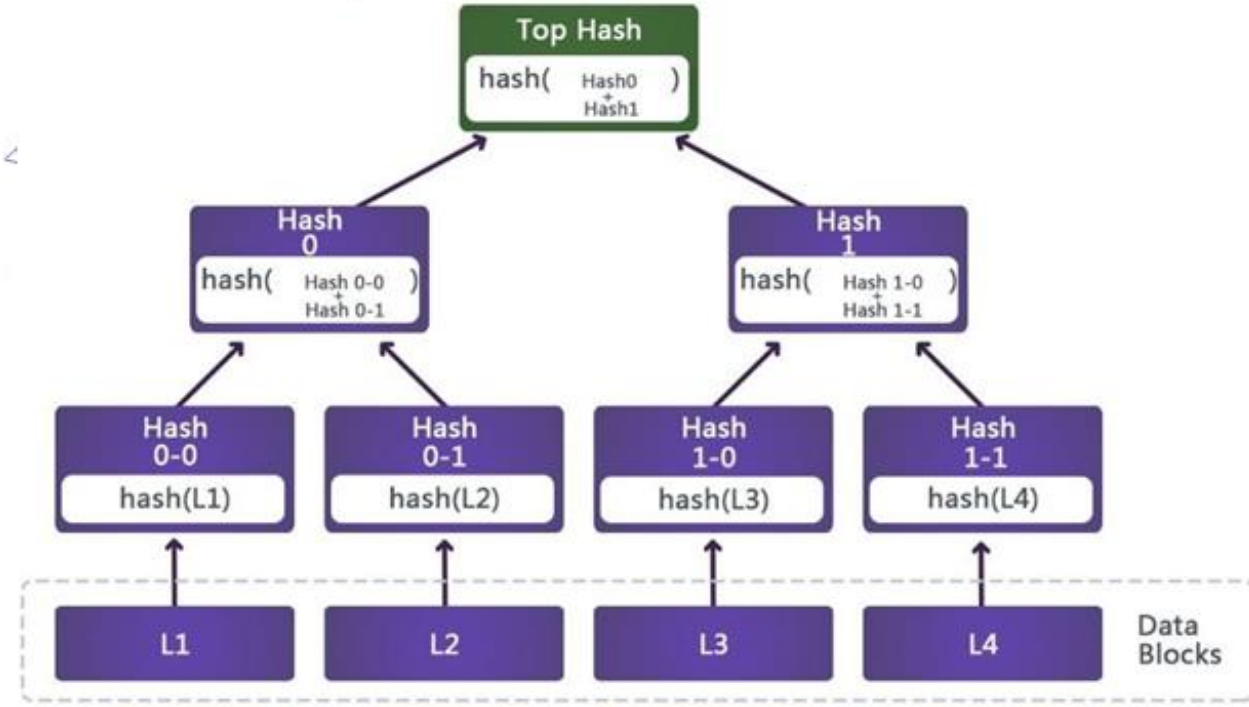
Directed acyclic graph (DAG) is a finite directed graph with no directed cycles. That is, it consists of finitely many vertices and edges, with each edge directed from one vertex to another, such that there is no way to start at any vertex v and follow a consistently-directed sequence of edges that eventually loops back to v again. Since the path from a starting vertex to an ending vertex in a directed graph might not form a cycle, a DAG is not necessarily a tree, but any directed tree is a DAG

Compared to a directed tree, DAG is a special but more general directed graph. Below is a simple illustration of a directed tree, DAG and directed graph. In the Big Data industry, DAG is usually used for Big Data frameworks, such as the execution engine of Hadoop, Storm, and Stark

There is a dependent relationship between each RDD object, which forms a DAG. The DAG scheduler will split the graph into multiple "Stages". The rules for partition are simple: scanning through from back to front, whenever the DAG scheduler encounters a narrow dependence, it will be added into the current Stage, whereas a wide dependence needs to be shu½ed. After completing the division of stages, DAG scheduler will generate a Task based on each stage and submit the TaskSet to TaskScheduler. The TaskScheduler is responsible for the scheduling of specific tasks and execution of tasks on worker nodes.

Recently, with the development of blockchain technology, there are some emerging blockchain systems that used DAG in the underlying data structure, such as IOTA [4]. IOTA's core data structure, called „Tangle', is a DAG that designed to resolve existing issues in the "Internet of Things" (IoT) industry, such as massive data storage and distributed computing, as well as providing a good solution for the micropayment in the IOT industry.

Traditional blockchains (such as Bitcoin and Ethereum) are using the binary tree data structure such as the Merkle tree:



DON Token team attempts to establish a channel between the systems that are based on two completely di"erent data structures so that it can be compatible with current mainstream blockchain technical standards at the bottom level while allowing new blockchain technologies to be able to communicate with current blockchain systems. Although the challenge is undoubtedly great, DON"s technology development team consists of renowned cryptographers from the world"s famous academic institution as well as experts from blockchain, Big Data, and Cloud Computing industry. Therefore, we are confident that with the support of all these experts, the team will overcome the obstacles and meet the original design goals of the system

GCM Technology(Giga Conversion Module) for Autocreation of Nodes.

This is an Inbuilt and custom made technology by the DON Team, this works as Auto-Multiplier or forger of DON tokens when stored in a Wallet. The GCM nodes interact with nodes in another wallet automatically and Generate new Internal Nodes which eventually generate new DON tokens. This is an equation of Time and Hardware modules to electrify or run the software by itself to multiply.

Hierarchy: DAO Governance

The Decentralized Autonomous Organization (DAO) is unexpected, yet the ideal product of the cryptography technological revolution. The root of the Decentralized Autonomous Corporation (DAC) can be traced back to the decentralized organization described by Ori Brafman in "Starfish and Spider" (2007) [11], and "peer production" described by Yochai Benkler in "Web Fortune" (2006) [12]. However, these two concepts are later linked together by cryptocurrency-related technology and gradually entered into cryptocurrency lexicon. In October 2013, Dan Larimer first put forward the idea of Decentralized

Autonomous Corporation (DAC), where he considered Bitcoin as a DAC also.

About DAC

In order to provide a clear definition of DAC, we have summarized the seven features that are necessary to a DAC:

Openness: The design of DAC system is made with a priority for transparency. The principle of openness and transparency is the cornerstone of the entire DAC system. An organization that operates behind closed doors cannot be considered as a DAC. Nowadays, the spirit of open source software has become a typical example of openness.

Decentralization: No centralized individuals or organizations can control the entire DAC. This feature determines self-similarity. The decentralized characteristic of the system ensures the vitality of the DAC system and protects people from corruption and abuse of authority,

Autonomy: Everyone can participate in the DAC system. All participants are either subsidiary or sub-unit of DAC system, which will promote the development of DAC from their own point of view. The spontaneous behavior of the participants guarantees the operation of the DAC.

Value: A DAC system must have to use value and can be put into practical application. For example, several features of the bitcoin system, such as international payment networks, anonymous transactions, tax avoidance, and value storage, have determined the profitability of the Bitcoin DAC system and contributed to improving the value and utility of the coin for coin- holders.

Profitability: DAC participants will receive rewards for contributing to DAC system development, and profitability is determined by the value of the DAC itself.

Self-similarity: Even there are only a few DAC nodes exist, the DAC system can still function and develop normally. The destruction of some unit nodes will not a"ect the development of DAC, which is guaranteed by the decentralization property.

Democracy: Changes in the core protocol of the DAC system require voting from vast majority of units, and thedecentralizationandautonomyfeaturehavedeterminedthatthe DAC mustbeasystemcapableof democratic voting.human participation," just as Stan Larimer said. However, this kind of autonomous organization in the ideal state can also lead to serious consequences if there is no strict control during the system design stage. [13].

For example, in June 2016, the DAO, the largest crowdfunding project in the history of Ethereum blockchain, raised more than $150 million USD worth of ETH. Nevertheless, due to the loopholes in code, the organization was attacked by hackers and lost more than 3.6 million ETH, which worth more $60 million USD at that time. Consequently, the ETH community split with the announcement of new security protocols, resulting in the co-existence of two blockchains: ETC and ETH

In the DON system, 5% of the coins will be sent to a DAO, and all DON holders can determine the use of funds through a real-time dynamic voting system, for example, the development of wallets and other infrastructures, or carrying out marketing campaign and other public relations activities. The DAO is the driving force behind the future advancement of DON community and provides the community with an unfailing supply of vitality. At the same time, the code for DON DAO will go through rigorous audits and

adds necessary human intervention at the initial stage (DON foundation would invite a third party to conduct security audits on the code). This is to protect the DAO from making significant errors in the utilization of funds at an early stage.

Hard: QuantumResistance

Currently, within the blockchain systems represented by Blockchain, SHA-256 hash calculations and ECDSA elliptic curve cryptography serves as the most basic security protection along with the Bitcoin network. However, with the advancement of quantum computer technology, especially within Shaw's algorithm (a typical representative of the quantum algorithm), related operations can be achieved from the index level to the polynomial level in theory. Problems that are difficult for a classical computer in the foreseeable future can certainly be solved by practical quantum computers.

Post-quantum cryptography, also known as quantum-resistant cryptography, is able to resist the attacks by quantum computers. The development of such encryption technology takes a more traditional path, based on difficult problems in specific mathematics fields. Through researching and developing algorithms, the post-quantum secure encryption technology can be applied in the network, and to provide the highest level of datasecurity.

The application of post-quantum cryptography does not rely on any quantum theory phenomenon, but its computational security can defend against any form of quantum attack that is currently known. In 1997, IBM researchers proposed an encryption scheme called Learning With Errors (LWE)[14][15], which means to learn with an error. As it takes a long time to find the nearest lattice, it can resist attacks from the quantum computer.

Ring-LWE-based public key encryption scheme: Related parameter selection and operation rules.

Private Key Generation

In this scheme, the encryption public key is h (x), the decryption private key is f (x) and fp (x).
The selection method is as follows:

$$f(x)\cdot g(x)=0 \bmod q \quad f(x)\cdot fq(x)=1 \bmod q \quad h(x)=fq(x)+1$$

The public key is (h(x) g(x)),and the private key is (f(x) fp(x)).

Encryption proces

In the scheme, the random error polynomial is introduced when encrypting, e(x), is a Gaussian distribution

with the parameter , and the plaintext is converted to the polynomial m(x). The ciphertext is: c(x) = h(x)·m(x) + g(x)·e(x)

Decryption proces

The received ciphertext is c (x), and the steps for decrypting the ciphertext using the private key f (x) and fp (x) are as follows:

(x) = f(x) ·c(x)
= f(x) ·h(x) ·m(x) + f(x) ·g(x)·e(x)
=[f(x)·fq(x)+f(x)]·m(x)+f(x)·g(x)·e(x) mod q(1)
= f (x) · m (x)

fp (x) · a (x) = fp (x) · f (x) · m (x) mod p
= m (x) (2)

In the decryption process of steps (1) and (2), there may be a decryption failure. When the coefficient of step (1) is not in the interval (-q2, q 2) or Step (2) coefficient is not in the interval (-p2, p2), there will be decryption failure. But as long as the selection of the appropriate parameters, the possibility of decryption failure is still very small. We also can use the algorithm similar to NTRU to avoid decryption failure.

DON will develop a Ring-LWE key exchange protocol that works with OpenSSL to achieve post-quantum secure in theblockchain.

. Handy: Limited Blockchain with Unlimited Transaction

The DAG technology itself is not based on blocks. Therefore, it is not subject to the constraints of block validation time (for example, the validation time for Bitcoin and Ethereum is 10 minutes and15 seconds, respectively). Due to the need to take into consideration the interaction between ERD and DAG-based blockchain system, the system has incorporated some of the advantages and strengths of DAG in its design. Thus, the validation time for transactions in the DON system is almost instantaneous. Also, as DAG is not based on blocks, there is no so-called block size limit in DAG. In theory, the amount of transactions that can be accommodated per unit time is fairly large (HTPS, Hyper Transaction Per Second). At the same time, DON needs to account for interaction with block-based blockchain systems. Consequently, it is possible for DON to realize a mass number of transactions per unit time under a limited block volume, thereby truly fulfilling the function of "DON Token".

. LimitedTokenSupply

The total supply of DON is fixed. About 9.9 millions of tokens will be created and will be distributed through the Mobile wallet.
9,90,00,000 Total Supply

20 million (40 %) is for Initial Distribution
2.5 million (5 %) is for Team reserve
2.65 million (53 %) Set to generate in Giga conversion model
1 million (1%) Promotion and Development

The DON token supply at Initial distribution in distributed for the Giga conversion module to run the algorithms to multiply (Auto Generate) .

Development: 2

Initial Distribution: 40

Giga: 53

Team reserve: 5

This technology is so strong that 53 % of the tokens will be generated from this Holding.

4. Development
. Business Model

Phase 1: Distribute & Store tokens

To implement proposed DON code and develop a scalable global currency network it takes and the high volume of nodes and transaction reflection in Hardware devices
The investors will get ERD Token first as a sort of Token holder in a Secure Mobile wallet, which is developed based on the existing mature UTXO model.
The token Holders are made to STORE OR EXCHANGE the tokens from device to Device.

Phase 2: List the DON token

With a IEO (If required) the DON token will be set to list on Top Exchange sites
The DON tokens are visioned to have 54 times more price at the listing phase compared to the Launch phase

The DON tokens can be Exchanged with any other Explorer or Ledger applications with no hassles.

DON Token's open source code can be found under DON's GitHub page - everyone can read and review the source code and check if the total number of tokens issued is consistent with the number of ERD stipulated in the whitepaper.

DON Wallet

Your funds are stored in hot and cold multi-signature addresses on their original chain, managed by a RPPOM consensus mechanism, and only accessible by you.

- **Store Funds securely**
- **Exchange or Transfer funds to a di"erent user and Di"erent currency**
- **Make Utility Payments**
- **Manage ERD tokens Reports and security.**

DON Roadmap Ahead

5 . ProjectRiskand Risk Management

.Regulatory risk

At present, although some governments, such as Japan, hold a positive attitude towards blockchain technology and cryptocurrency and have established a favorable policy to support the growth of the industry, there are still many uncertainties in the regulatory level due to conflicts between the decentralized nature of public blockchain and the policies of existing centralized governments. Governments adverse to the proliferation of the use of cryptocurrencies in local commerce could issue laws and regulations deeming the use of cryptocurrencies a regulated activity. For example, in recent weeks, countries such as China and Korea have issued regulations or statements prohibiting token sales, while other countries like the U.S. have sought to bring the sale of tokens within the regulator control of

securities o"erings. This could result in holders of ERD being unable to use their coins in the future without further regulatory compliance.

The management team will use the following ways to manage the regulatory risk:
The team will set up a separate public relations department that will actively communicate with relevant government authorities and industry practitioners, so as to design and carry out its digital asset issuance, trading, blockchain finance, blockchain applications and other business under an existing legal framework.

Theoperationof DON projectneitherinvolvestransactions usingfiatmoneynorinterfereswiththe exchangebetweenDON andfiatmoney carriedoutbythird-partyexchanges. DON teamfocused only on technology.

.Market risk

The ultimate goal of DON is to achieve the free flow of value and information within the blockchain ecosystem. However, since the blockchain industry is still in its infancy stage of development, the project will face a variety of market tests in the future.

The operation team will use the following ways to manage the market risk:
The DON operation team will attend industry meetings regularly and hold press releases on project progress from time to time to communicate and discuss with relevant developers regarding current market needs and prospects. This can ensure that the project is able to respond to the voices of the community and market.

.Technical risk

The goal of DON is to establish a new set of cross-platform technical standards, which is a very difficult taskintermsoftechnologydevelopment. Therefore, theproject putsa highdemandon top-notch technical talents and requires extensive research involvement and engagement. If these requirements cannot be satisfied, it will definitely a"ect the progress of the project and even eventually lead to the failure of the whole project.

The operation team will use the following ways to manage the technical risk:
The operations team will work closely with top domestic and foreign universities and research institutions to build joint laboratories that focus on the development of innovative blockchain technology. The DON foundation will also regularly allocate funds to support the construction of DON community and carry out in-depth collaboration with other blockchain and crypto communities, so as to ensure that the technical risks of the project are controllable.

.Financial risk

Financial risk refers to the significant loss of investment raised through Initial distribution. For example, hackers or other malicious groups or organizations may attempt to interfere with DON distribution or DON tokensinavarietyofways, including, but notlimited to, malwareattacks, denialofservice attacks, consensus-based attacks, Sybil attacks, smurfing and spoofing, In addition, the team may not be able to complete the development progress within the schedule because of personal and financial problemsand so on.

The operation team will use the following ways to manage financial risk:
All the digital currency raised Initial public sale are stored in a multi-signature wallet with cold storage and managed by the directors of DON Foundation. Using 3/5 multi-signature, the risk of project funds being subject to expropriation and/or theft can be e"ectively reduced.

6. Disclaimer

This whitepaper has been prepared by DON team for the sole purpose of introducing the technical aspects of the DON and its associated platform and underlying blockchain protocol. This document does not constitute any o"er, solicitation, recommendation or invitation for, or in relation to, the securities of any company described herein.

The whitepaper is not an o"ering document or prospectus and is not intended to provide the basis of any investment decision or contract. The information presented in this whitepaper is of a technical engineering nature only and has not been subject to an independent audit, verification or analysis by any professional legal, accounting, engineering or financial advisers. The whitepaper does not purport to include information that a buyer of DON might require to form any purchase decision, and, in particular, does not comprehensively address risks of the DON, which are numerous and significant.

DON(along with its directors, officers, and employees), does not assume any liability or responsibility whatsoever for the accuracy or completeness of the information contained in this whitepaper, or for correcting any errors herein.

The content of this whitepaper is technically challenging and requires a high degree of familiarity with distributed ledger technology in order to comprehend the DON and its associated engineering risks.

Recipients of this document are encouraged to seek external advice and are solely responsible for making their own assessment of the matters herein, including assessment of risks, and consulting their own technical and professional advisers.

WHITE PAPER

www.DONtoken.com