# upload_post_object_v2_013460123

# XDAG: A new DAG-based cryptocurrency

## Introduction

XDAG is a new generation public chain based on Directed Acyclic Graph (DAG) infrastructure, and is the first mineable, pure community-driven DAG+POW project, with the main network launched in January 2018. The maximum XDAG supply is approximately 1.446294144 billion .XDAG has no project sponsor, no ICO, no private placement, no pre-mining, and is developed and maintained by geek enthusiasts from all over the world, which is truly decentralized, efficient, secure and fair. Although XDAG is a DAG project, its transaction model is similar to Bitcoin's UTXO, and the development of the project also has some similarities with Bitcoin's.

**The Legend of XDAG**

XDAG was started in September 2017 by a math professor in a Russian university who used the name of Cheatoshi. Because he was not satified by the cryptocurrency projects at that time, he wanted to make a cryptocurrency project of his own. He chose DAG and used PoW. Cheatoshi spent three months to complete the project but failed on launching in December 2017. After Cheatoshi spent a few days to debug, XDAG network successfully start in January 2018.

On January 5, 2018, Cheatoshi posted the XDAG founding post in the BitcoinTalk forum, claiming to create a fair cryptocurrency system based on DAG technology. At that time, everyone was communicating on bitcointalk, and in February 2018, Cheatoshi open-sourced the project for the community to participate in contributing, after which the community migrated the project to Github.

Then Cheatoshi disappeared and leaved the project was completely transfered to the community to manage. This experience is very similar to that of Satoshi Nakamoto.

Salute to Cheatoshi.

XDAG is the first DAG to support mining (IOTA is not really mining), while there is no pre-mining, no ICO, and is completely community-driven, no sponsor or investors to promote. XDAG is currently being continuously developed and maintained by a group of developers who love blockchain and persist in the ideal of decentralization.

**Current Issues of Decentralized Technology**

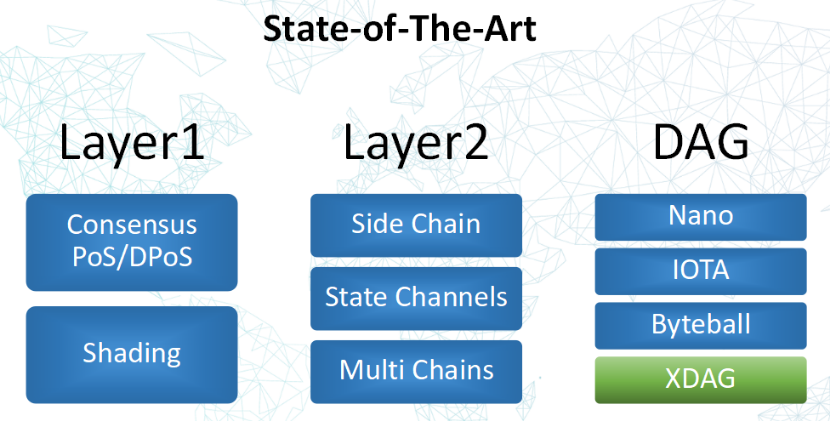
Although the industry has developed over the years, blockchain technology based on blockchain itself has many problems, and these problems are becoming more and more serious with the expansion of scale.

The current problems encountered are mainly in the following two areas.

1. The TPS bottleneck of blockchain itself limits the performance of blockchain technology.

2. The long confirmation time of blockchain also limits the scatibility of blockchain technology.

Although many blockchain developers in the industry are trying to find various technical means to solve these problems, but from the current state of technical development, various attempts have not made breakthrough progress.



The current approaches tried include.

1) Layer 1 (Sharding)

-PoS/DPoS and consensus / Sharding (sharding calculation)

2) Layer 2 (Side Chain)

-Side Chain/ State Channels/ Multi Chains

For the defects of blockchain, whether it is the centralized solution of EOS or the current hot sharding technology, there are still unsolvable problems in side chain technology, which indirectly shows that it will face great difficulties and challenges to expand based on blockchain itself. The technology of DAG appeared as a third option of resolutions.

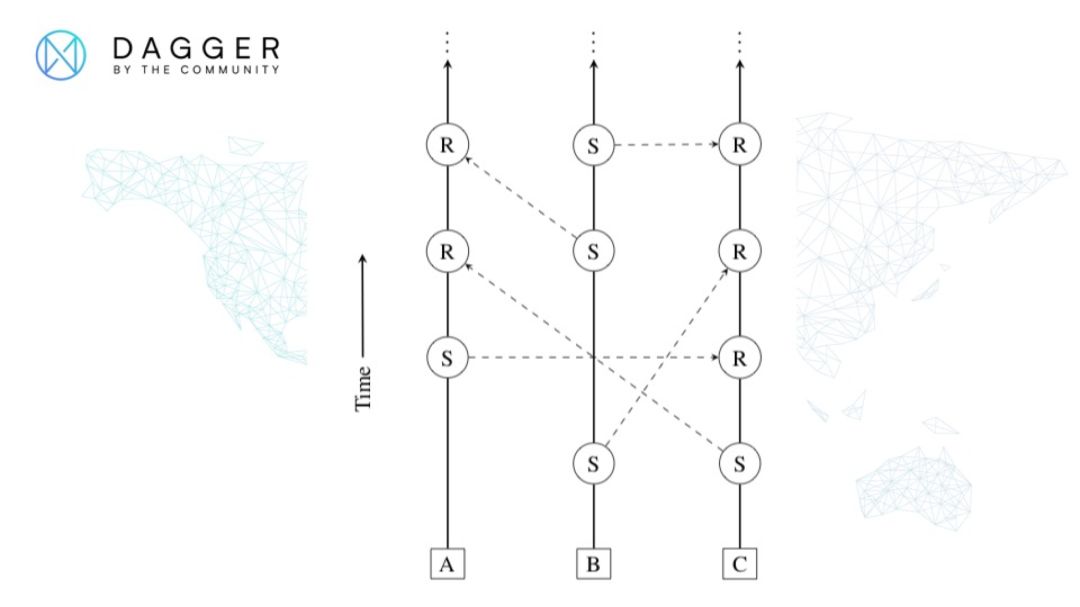
DAG is relatively special, the data structure is different from blockchain, and it is born with high scalability. The most well-known project using DAG technology is IOTA, but IOTA still has the problem of centralization; XDAG has made changes with PoW being adopted, which has been proven to be the optimal consensus scheme, and leaving the work of verifying transactions to miners exclusively, and retaining the original advantages of DAG.

**XDAG Technology**

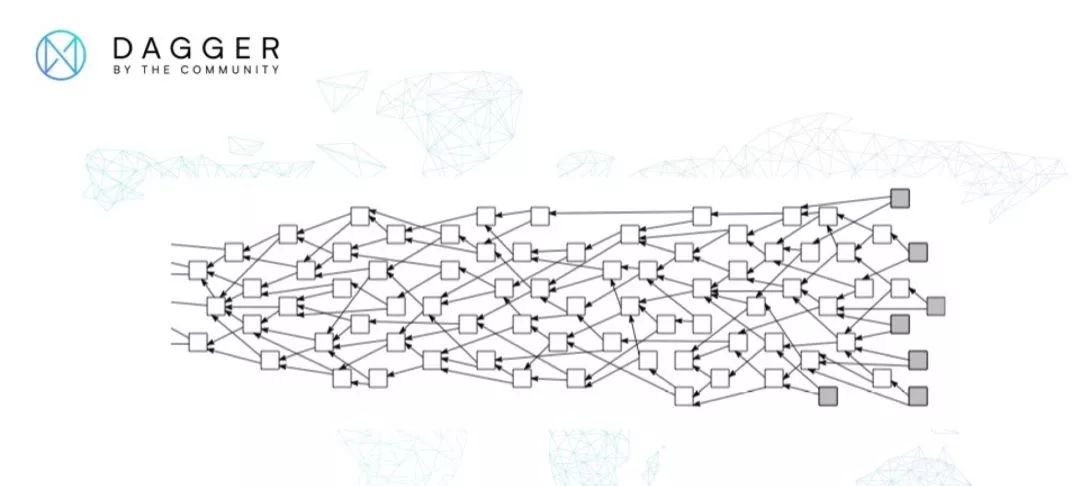
1.Introduced as early as 1736, DAG (Directed Acyclic Graph) is not a newly emerged technology, but a mathematical concept in graph theory and a branch of mathematics. While in computer technology, this digital storage structure has been existence since the early days of computer technology. Theoretically DAG structures are more complex than single-chain structures, but have better scalability.

At present, there are some public chains based on DAG structure in the industry, but each public chain has different implementation routes and application scenarios due to different understanding of DAG technology.

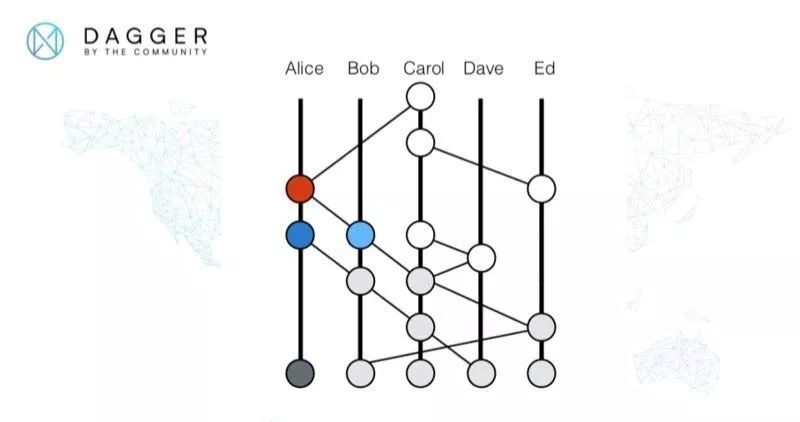
1). This is the way NANO is implemented, the main idea is that each account has its own chain, and different accounts are linked together based on transaction records, thus forming a DAG:



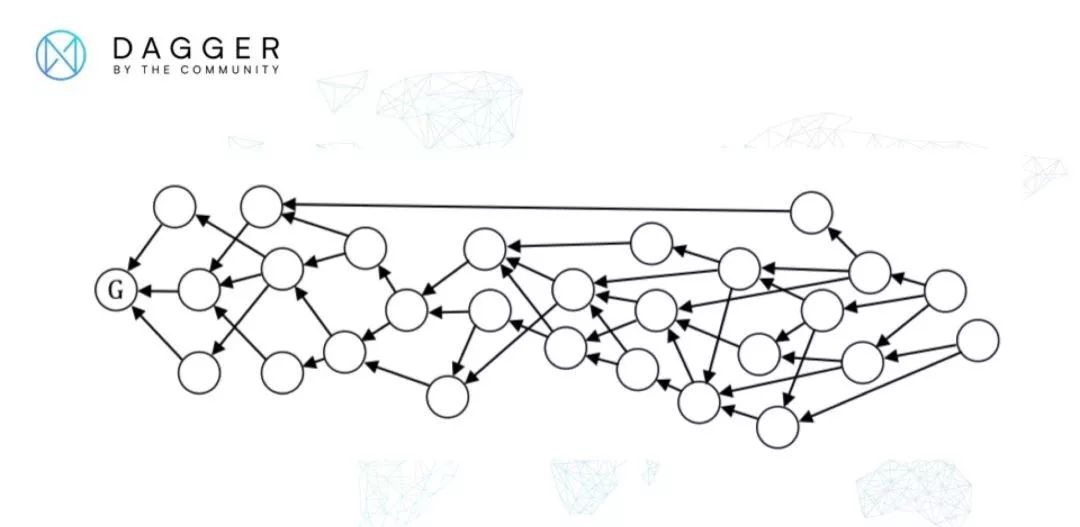
2). This is the DAG of IOTA, and the main idea is to let the user determine the validity of a transaction based on its different heights and weights:



3). This is the DAG of Hashgraph. The main idea is to use the modified gossip algorithm between Nodes to propagate the transaction information to form a sequence in time, thus forming a DAG:

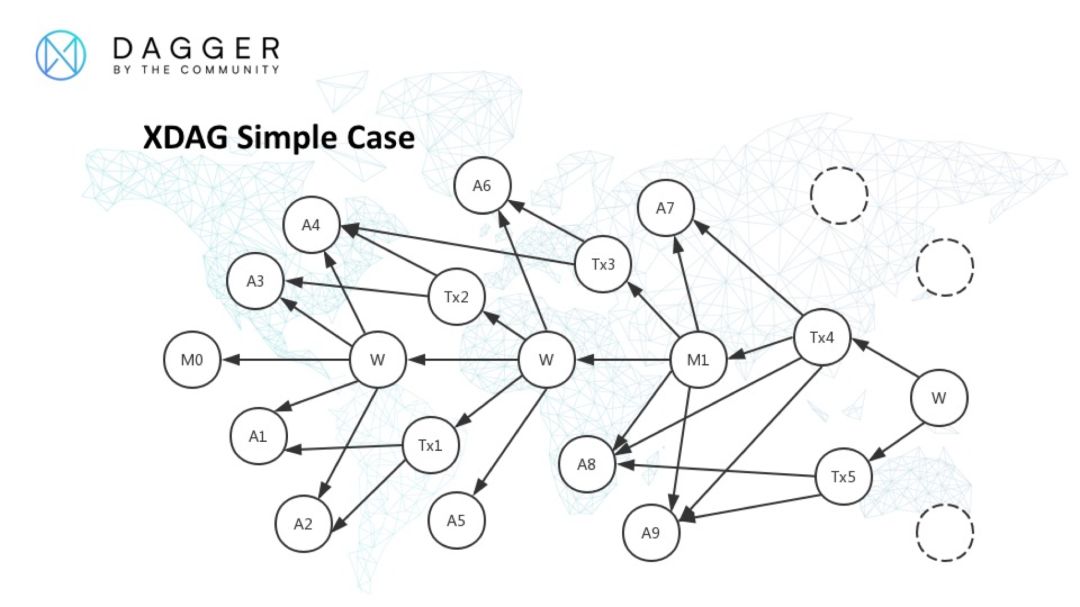


4). This is the DAG of Byteball, and it is based on the idea of using witness Nodes to append witness units to each post-transaction to increase the weight on the branch and thus determine the current master chain in the DAG.



And the above multiple DAG implementations do not address the "impossible triangle" ,which are problems of decentralization, high TPS and low confirmation time.

2. XDAG attempts to redesign the data structure from the bottom of the blockchain technology and adopts another DAG composition, cleverly combining PoW consensus algorithm and DAG technology, and at the same time providing concurrent processing of transactions between different Nodes to improve TPS and reduce confirmation time while ensuring network security and fairness.



A partial DAG composition in XDAG

A=wallet address block, Tx =transaction block, M = main block generated by PoW, W =witness block.

The unique feature of XDAG: Blocks = Transactions = Addresses



The data structure of the block in XDAG is shown in the figure above, and this data structure is used for persistent storage of data.

The block structure is composed by 16 structures named *xdag\_field*, each *xdag\_field* is a structure, which consists of a structure and a union.

The *transport\_header* is used to represent the sequence number during transmission and to hold the address of the next block during post-reception processing.

*Type* is a 64-bit field used to indicate the type of 16 *fields* in a block, which is divided into 16 parts, each part is 4 *bits*, that is, half a byte, and 4 *bits* can indicate 16 *types,* so the *field type* indicates the *type* corresponding to a *field* every 4 *bits*.

*Time* is used to indicate the time of block generation, the format used is 1/1024 seconds, in which one second is expressed as 2^10. It is also used as the starting time point of the request time range when data is exchanged between Nodes.

*Hash* is a 24-byte truncated hashes, usually the truncated hashes of another block.

*Amount* is a quantity value in *Cheato*, used to record the number of XDAGs, *Cheato* is the basic unit in XDAG, 1 XDAG contains 2^32 *Cheato*.

*End\_time* is used to indicate the end time point of the data exchange between Nodes as the request time range. *data* is a 32-byte hashes .

The blocks described above in XDAG are generated completely independently by each Node and each wallet itself without interference from others, thus ensuring the independence of block processing in the basic design, and laying the foundation for the high TPS mentioned subsequently.

3. Technology Advantage of XDAG.

1) XDAG is the first public chain based on DAG to realize the PoW. Combining the high concurrency of DAG with the security and decentralization of PoW to solve the “impossible triangle” problem in the blockchain technology;

2) Block = Transaction = Address.

This unique design ensures that the transfer process will not lose coins due to typing in the wrong address;

3) Low transaction fee and high TPS.

4) XDAG uses unique technology to solve many problems that may exist in the blockchain system, such as double-spending, uncontrollable transaction time, centralization, 34% attacks, and 51% attacks.

5) Some of the experiments currently done in Bitcoin and Ether can be done on XDAG, as the founders have done their own operating systems, so they have been designed with this in mind.

These can be explained as below figures :

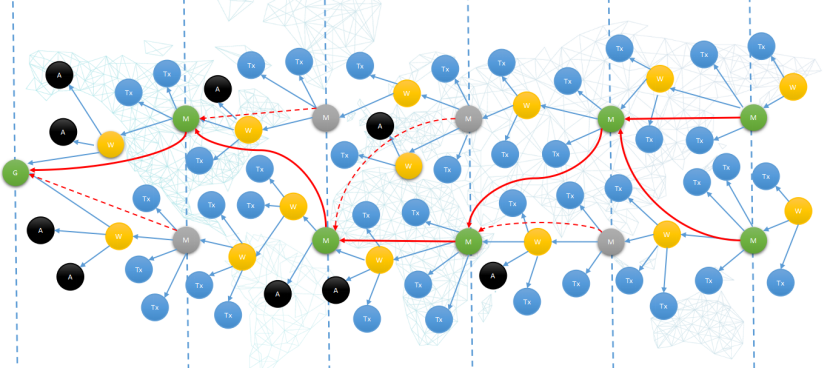


Diagram 1:

There is a concept of main chain in DAG, because the transactions in DAG need a sorting, otherwise it cannot solve the problem of double-spending. XDAG inside the main chain, there is a slice according to the time, each slice will be packaged for transactions, *Green* is the main block on the main chain, Y*ellow* is the witness block, *Blue* is the transfer transaction, *Black* is the address block.

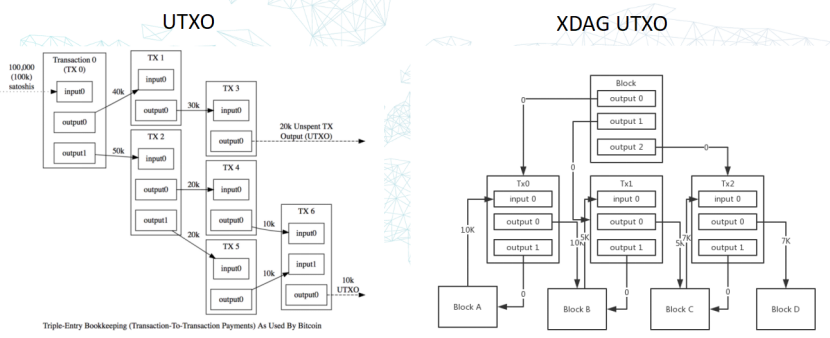


Diagram 2:

XDAG is similar to Bitcoin and is also the model of UTXO. The graphics may not be the same, but the essence is the same, the *Block* in the figure is the connection block mentioned earlier, *Tx0, Tx1, Tx2* are the real transactions, and *Block A - D* are the addresses.

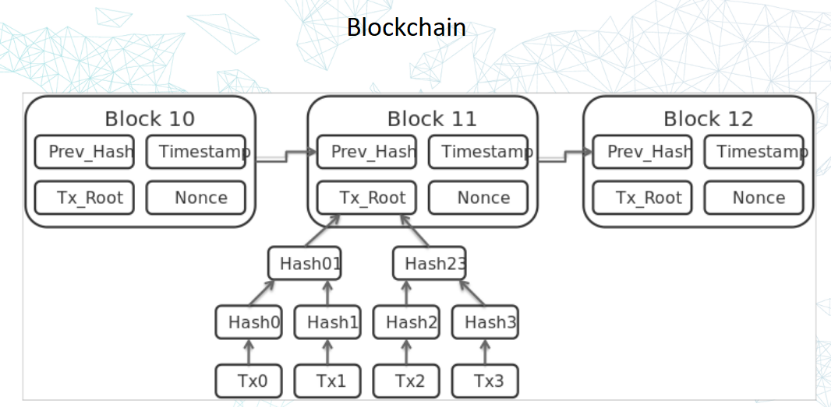


Diagram 3:

From the above figure, there are Merkle trees in the blockchain and a similar structure in XDAG.

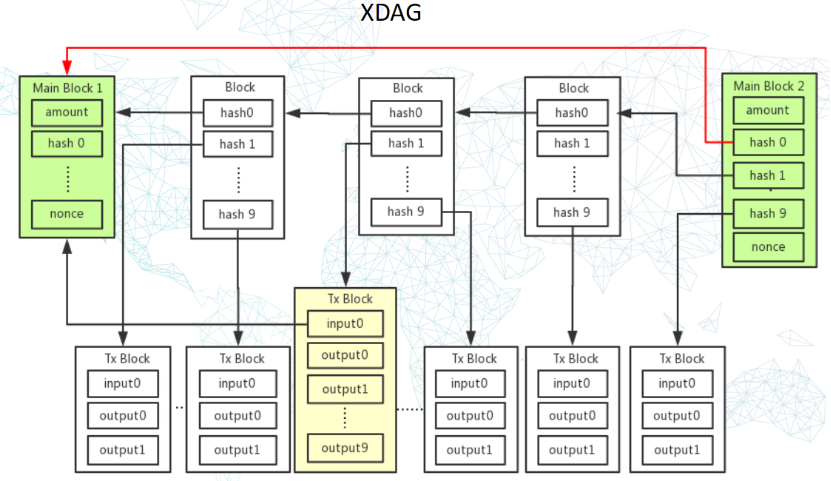


Diagram 4:

The green *Main Block* in the above figure stores the hash of the transaction, similar to the Merkle tree.

The calculation of PoW in XDAG is variable, miners add the received transactions to their own hash calculation, each Node will do the calculation, and finally compete who has the strongest calculation power, and then generate the block of *Main Chain*.

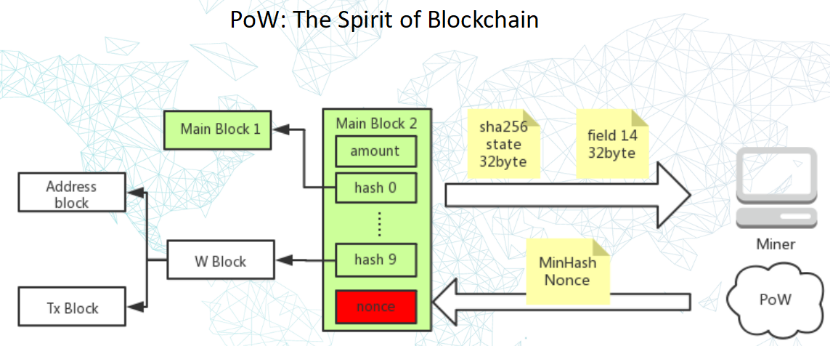


Diagram 5:

It is to do the hash that calculating of the local block/transaction, layer by layer, and finally fill in the new block *(Main Block 2)*, and then do the *sha256* calculation, what *sha256* does is to do iterative calculation and obfuscation. For the sending of the result, only the calculated *sha256* value needs to be sent instead of sending all the transactions, the size is only *32byte*, which will save bandwidth resources, so that the miner only needs to continue to calculate the *sha256* and finally find a minimum hash to get the nonce and determine the new *Main Block* on the *Main Chain* , and in this way the structure of the main chain is formed.

Note: To ensure fairness, the XDAG mining algorithm has been changed from *sha256* to *RandomX* algorithm.

## 4.How to resolve Double Spend.

This can be illustrated in diagrams as below:

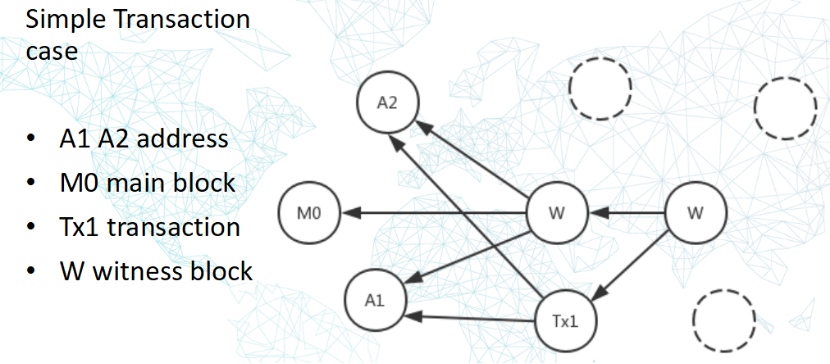


Diagram 1:

If a transaction is generated between A1 and A2, a new connection block is generated to confirm the transaction between them, and the connection block is generated from the miners.

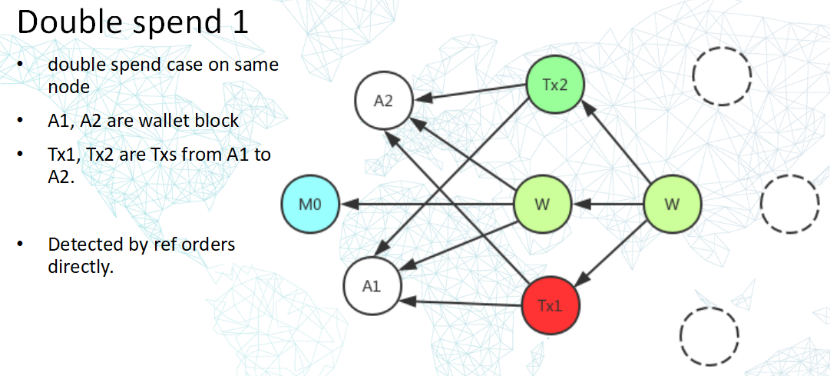


Diagram 2: A typical Double Spend detection

Suppose there are 10 XDAGs at address *A1*, and *A1*'s wallet is maliciously copied twice and two transfers are initiated at the same time, one *Tx1* transfers 5 XDAGs from *A1* to address *A2*, and the other *Tx2* transfers 7 XDAGs from *A1* to address *A2*. The two transfers total 12 XDAGs, which exceeds the original 10 XDAGs for the *A1* address, a typical double spend.

The logic in XDAG detection is that when the Node receives *Tx1* and *Tx2* at the same time, the Node generates a W block that references *Tx1* and *Tx2*, and according to the stable ordering rules *Tx2* will be populated with fields with smaller order numbers when referenced by the *W block*, thus *Tx2* is processed first and *Tx1* is processed later, thus verifying that the *Tx1* spend is a double spend, and thus the internal block will The transaction block pointed to by this hash is marked as rejected, and the transaction block *Tx1* is recorded in the DAG forever and is not deleted.

Because users can choose which Node to send their transactions to for verification, it is assumed here that if both transactions are sent to the same Node, the first transaction referenced by the connection block is a valid transaction, and the second is an invalid transaction, solving the simple double spend problem in this way.

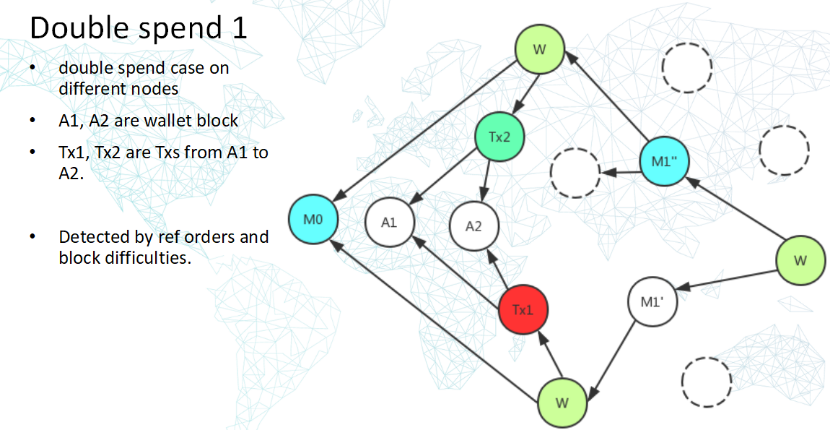


Diagram 3: A more complex Double Spend detection

Suppose the premise is the same as the previous one, and suppose there are 10 XDAGs at address *A1*, and *A1*'s wallet is maliciously copied twice and two transfers are initiated at the same time, one *Tx1* transfers 5 XDAGs from *A1* to address *A2*, and the other *Tx2* transfers 7 XDAGs from *A1* to address *A2.* The two transfers totaled 12 XDAGs, exceeding the original 10 XDAGs at the *A1* address, a typical double spend.

But this time the situation has changed, that is, the person maliciously used technical means to connect the wallet to a different Node, thus creating a double spend detection between different Nodes.

At this point, PoW consensus comes into play, and a master block is generated every 64 seconds in XDAG. By comparing the difficulty of the master block *M1' M1''*, it is determined that *M1''* is more difficult, so *M1 ''* referenced block *Tx2* in sorting priority over *M1'* referenced *Tx1*, so that *Tx1* is detected as a double flower, and thus the transaction block pointed to by this hash is marked as rejected in the internal block, while the transaction block *Tx1* is recorded in the DAG forever and will not be deleted.

If there is a user who wants to cheat and sends these two transactions to different nodes, this time it is necessary to solve this problem through the PoW-generated master block (*M1''*), as you can see from the above figure *M1''* is the master block generated through the miners' PoW arithmetic competition, while *M1'* is not, because the master block takes precedence, in this case, *Tx2,* which is indirectly referenced by *M1''*, is a valid transaction thus solving the Double Spend problem.

5. XDAG supports high TPS.

Why can high TPS be achieved among XDAG? It is because it splits the DAG into multiple localized blocks, so it can achieve a high TPS similar to the effect of sharding computation.

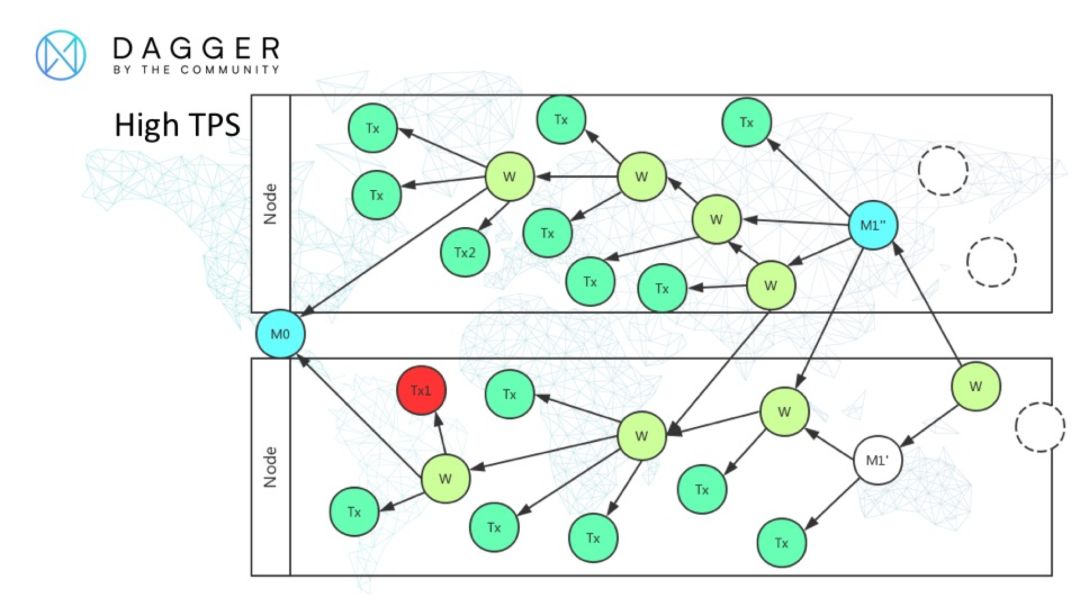


Diagram 1:

The diagram shows a more comprehensive DAG structure of XDAG, where the wallet address blocks in the previous diagrams are omitted for simplicity.

*Node* denotes a different node, *M* denotes the main block mined by PoW, *W* denotes an additional block, which I named witness block, and *Tx* is the transaction block.

Different nodes receive their own transaction blocks separately, and the act of stitching the transaction blocks into the DAG is less coupled with each other, and the connection between them is established through the data interaction between nodes, which enables different nodes to absorb higher concurrency well to achieve high TPS.

At the same time, a master block is generated every 64 seconds through PoW, so that the transaction confirmation time of decentralized public chains is also greatly reduced, and can be confirmed in 1 to 2 minutes in general.

**Advantage of XDAG**

1. XDAG adopts the DAG + PoW method to break through and solve the limitations of the traditional blockchain technology, which can greatly improve the scalability of the blockchain system. XDAG has the advantages of decentralization and high TPS while supporting PoW mining. XDAG network can still have high TPS under the most originalist decentralization like PoW consensus, and the transaction volume can reach several thousand TPS.

Theoretically, the DAG approach is that there can be unlimited trading blocks between *Main Blocks,* but the actual situation still depends on the network transmission speed and the performance of the equipment on the network. The peak transaction volume has once reached several thousand TPS, however, due to the network and hardware conditions, the transaction limit has not been measured.

2. Friendly to blockchain technology. A block in XDAG is also a transaction, and the address generated by the wallet will also generate a transaction in the network: Block = Transaction = Address. Some of the experiments currently done in Bitcoin and ETH can be done on XDAG, because the founders themselves have done the operating system, so they have taken these into account in the design.

3. Fast block generation, fast transfer and no commission. Thanks to the characteristics of the infrastructure DAG technology, XDAG is currently set to generate a block every 64 seconds, the transfer can be about 3 minutes to the account, the fee is zero. This is in the case of PoW decentralization, to achieve a high TPS and fast transfer.

4. XDAG can achieve financial security, no black hole address. All wallet addresses and transaction records in XDAG are blocks, as long as there is a wallet, then the wallet address must exist in the main network; if you try to transfer money to a non-existent address will fail, so there is no problem of transferring to a black hole address.

5. Originality of XDAG. The implantation of DAG+PoW in XDAG is groundbreaking and the earliest (Note: check the time through BitcoinTalk's Genesis post), and the code is original. XDAG provides C language and Java.

6. Turely community driven. No project sponsor, no pre-mining, no 1CO, every XDAG is mined and mined out by miners farely. The community team is made up of enthusiasts from different countries, together driving the evolution of XDAG.

7. ASIC resistance and CPU minging. XDAG adopts RandomX mining algorithm to attract more CPU users to join mining, more fairness.

With these advantages, XDAG can support many decentralized scenario applications, allowing more applications to be ported to XDAG, free from the pain of congestion and high fees of other public chains.

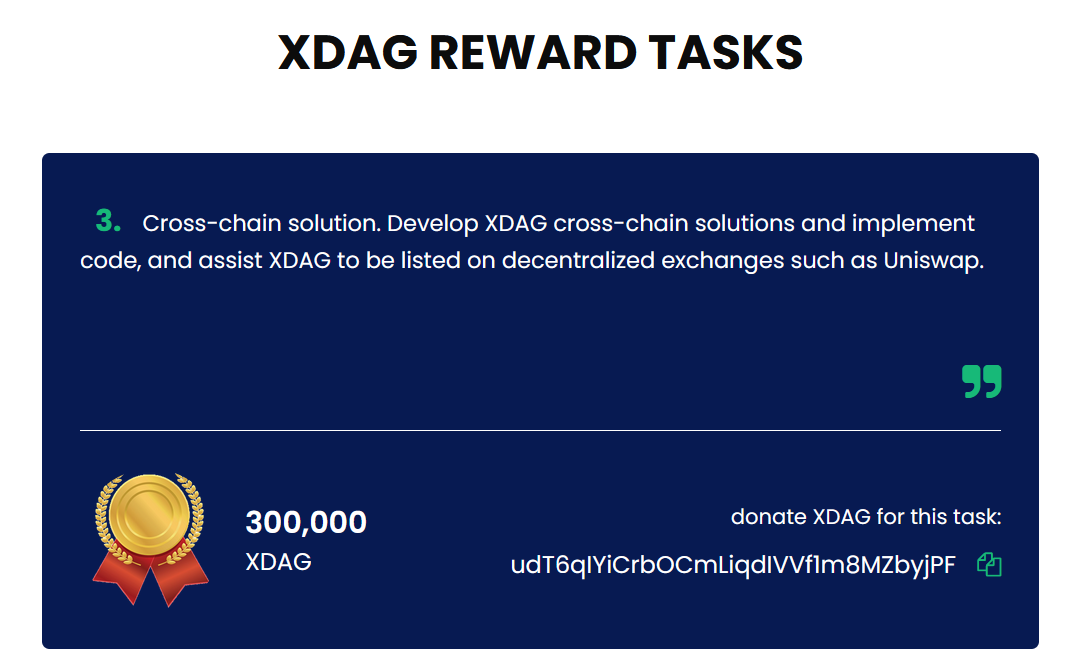
**XDAG Community**

XDAG enthusiasts set up a community autonomy team, from geek free development to orderly advancement, from the Apollo Program to the current Mars Program, XDAG is making rapid progress one step at a time and the community is getting stronger and stronger.

At present, XDAG community autonomous team is comprised of more 20 members from around the world, corresponding to XDAG JAVA/C , PC wallet, Android wallet, IOS wallet, mining algorithm, mining software, network protocols, community website, testnet, community operations and other different work.

The workload is still relatively large for a autonomous community, we need more XDAG enthusiasts to join us. At present, the community has established a community proposal mechanism (https://trello.com/b/nlSBXa2d/xps) and developer incentive mechanism, you can check the community website https://xdag.io/ , where there is a "Reward Task" to attract more developers to the community. Anyone can suggest improvements on XPS and sponsor the development costs.

Here's an example:



## XDAG Links

Official Website： xdag.io

Bitcointalk：https://bitcointalk.org/index.php?topic=2552368.0

XDAG Whitepaper：https://github.com/XDagger/xdag/blob/master/WhitePaper.md

Github：<https://github.com/XDagger>

Blockchain Explorer：https://explorer.xdag.io/

Exchanges： coinex.com

## Welcome to XDAG Community

Discord：<https://discord.gg/Nf72gd9>

Telegram：<https://t.me/dagger_cryptocurrency>

Tweeter：<https://twitter.com/XDAG_Community>

Wechat：xdag\_dev