Bityuan Whitepaper

A simple, stable and scalable blockchain network

V2.0

June, 2018

Content

Abstract

Bityuan aims to build a simple, stable and scalable blockchain network. The design of the entire system is based on the principle of 'simplicity'. Bityuan supports payment, C2C trading, Dapp development and business use cases. Additionally, it ensures the security of digital assets with wallet recovery function. From a technological perspective, Bityuan integrates parachains on its main chain such that anyone can launch a token-based blockchain project on the Bityuan network, and no coding is needed in the whole process.

Bityuan also provides a decentralized exchange environment where non-native tokens can be exchanged via Bityuan's native token in an anonymous and secure manner. Outside of the Bityuan ecosystem, atomic cross-chain trading is designed to allow Bityuan to communicate with other public chains in the blockchain space.

We wish to build a sharing and prosperous ecosystem where blockchain is truly open, transparent, and equal to everyone. By adopting the token-incentive mechanism, we encourage more to join our community and contribute to the ecosystem. In this way, we can build and maintain a highly secure and multi-layer blockchain ecosystem, and let the technology advancement guide us towards the future.

1. Mission & Aim

It is generally believed that the distributed ledger and token-incentive timestamp system, represented by Bitcoin, will be the pillar of modern finance in the future. For an emerging technology, it will accept wide adoptions and public recognition only when it enables technological upgrades and performance optimization, thus obtaining widely business applications and becoming a disruptive technology. The mission for Bityuan is to achieve decentralized governance, allowing participants to formulate relevant rules, and have sufficient development funds to mobilize the power of the entire community and promote the development of Bityuan.

The core of Bityuan is just as stable as Bitcoin's. Furthermore, Bityuan is equipped with a flexible and efficient scalability. Developers can build powerful decentralized applications (Dapp) and design multi-chain ecosystems on the Bityuan platform, to jointly maintain the development of the Bityuan network. Whoever makes contributions to the Bityuan community and ecosystem will be rewarded with Bityuan coin - BTY.

Bityuan aims to build a simple, stable and scalable blockchain token system, and the design of the entire system is based on a principle of 'simplicity'. Nevertheless, the architecture of the Bityuan network empowers functionalities including but not limited to: i) Quick and safe payment; ii) Anonymous trading; iii) Atomic cross-chain trading. Additionally, a combination of off-line wallet and wallet recovery function safeguards the security of crypto assets in the Bityuan network. Ongoing blockchain projects with classifications of points, games, prepayment are built on the Bityuan platform, improving its diversity.

2. Use Cases

2.1 Digital Asset

Assets that exist in the form of electronic data are called digital assets. The use of blockchain technology enables digital assets to have characteristics of decentralization, trust-less and traceability. Bityuan mainly implements the function of asset digitization.

Users can register assets on the Bityuan main chain to achieve asset digitization. Some non-liquid assets, such as real estate, gold, commodities, points, debt notes, etc., can be digitized and securitized to increase liquidity such that transfer becomes

seamlessly and boundarylessly.

2.2 Mining

In addition to the functions of payment and storage, the PC version of the BTY Wallet introduced by Bityuan has mining mechanism. The BTY holders lock a portion of the BTY tokens in exchange for tickets. Bityuan blockchain network designs an innovative PoS algorithm and is expected to deploy 1 million synchronous nodes worldwide, including about 30,000 mining nodes. The block time is about 15 seconds, with each block producing 30 BTYs, of which 18 BTYs are collected by the miners and 12 BTYs enter into development funds. In the current version, every 10,000 BTYs can be locked in exchange for one ticket. Ticket holders will participate in the mining of new blocks. The average time for each ticket to be selected is five days. With more tickets in the lottery system for a single participant, the chance to be selected to mine the next block increases accordingly, which will lead to a larger production of BTY over a fixed time span.

2.3 Payment

Bityuan blockchain system has experienced a few upgrades and is now featuring with the characteristics of high performance and low latency, which gives it a great competitive edge in the payment and clearing industry. In the mean time, Bityuan main chain is set up with bridges to facilitate token transfer. Bityuan strives to become a reliable medium for global asset transactions, and most of the user's fees can be reduced.

2.4 Wallet Recovery

The Bityuan's default wallet recovery function solves the problem of private key loss. A personal wallet featuring wallet recovery function is equipped with a master private key and a back up private key. If the master private key is lost, you can retrieve your own crypto assets by using the back up private key (self-stored or kept by a trusted institution/person). Wallet recovery does not mean transferring the digital assets instantly, but it takes some time for the action to be effective. Therefore, if the back up private key is misused, the owner will be notified immediately and use the master private key to transfer the digital assets to another secure wallet, preventing unnecessary loss.

2.5 Blockchain Explorer

Users can view all the relevant information in the blockchain through the Bityuan blockchain explorer, including the block throughput, the transactions in each block, the history of token issuance and token transfers, mining production records, account balance, etc.

2.6 Business Application

Bityuan network has a unique ecosystem where users can receive, store and transact digital assets on different chains seamlessly.

The tokens on the Bityuan blockchain ecosystem can represent anything that is valuable and tradable. It can be used in many industries, such as royalty points, prepaid cards, games, gambling, real estate, commodities, smart clearing, etc.

3. Technology Advancement

3.1 Proof-of-Stake (PoS)

PoS stands for Proof-of-Stake, is a type of algorithm by which the blockchain network aims to achieve distributed consensus through staking wealth or other combination of random selection. BTY holders participate in the decision making process by voting mechanism. The Bityuan's PoS algorithm incorporates self-innovations, which solves some of the mining security issues and the mining can be done as securely as the conventional PoW algorithm.

Under the PoS consensus mechanism, mining does not consume a large amount of physical utilities, which shortens the time that nodes require to reach consensus. On average, every block is created every 15 seconds in the Bityuan blockchain network, and the transaction throughout can be 100 TPS, which is a moderately high performance among the many public blockchains, and has commercial-level applications.

3.2 One-click Token

'One-click token' is a buzzword which describes an act of issuing a token through the

Bityuan network, because of the convenience and simplicity, the whole process is almost as if one click is needed to complete the process.

Anyone can fill in a customized application form to issue a token on the Bityuan network. After approval, the issued token can be launched and begins circulating on the Bityuan network. The property of the token issued with 'one-click' is called non-native token (Bityuan's native token is BTY).

No programming code is required during the token issuance process and the security resources of the issued token is provided by the Bityuan main network. Therefore, to issue a token on Bityuan network is easy and secure, anyone who even has little idea of the concept blockchain or cryptocurrency can do that. The many tokens issued on the blockchain network will facilitate the respective projects and make the Bityuan ecosystem prosperous.

The advantages of 'one-click token' powered by Bityuan network is classified in below:

A) Simplicity

As long as the idea behind the token is an improvement to the Bityuan network in terms of its diversity, culture integrity and so on, then the application for launch the token and the project will definitely get approval. The process is simple, with no developers of blockchain expertise needed.

B) Secure

Since the consensus mechanism is provided by the main blockchain of the Bityuan network, security is promised. Additionally, upgrade and maintenance is supplied by the main network as well.

C) Unique

The name ticker of the issued token is unique.

D) Ecosystem

The tokens will have the space for independent development with no fear of collision. In the mean time, tokens can be interoperable and transferable through the Bityuan main chain.

3.3 Anonymous C2C trading

Once the BTY wallet is set up, users can conduct transaction in the Bityuan network in a peer-to-peer manner. Every wallet is a transaction node in the network, users of the network can trade without a trusted third party (i.e.exchange). The features are in below:

I) Anonymity

The C2C trading in Bityuan network is anonymous. Since the majority of the exchanges in the marketplace is centralized with a strict KYC process and personal data is kept by the exchange, so the risk associated with personal privacy is high. Bityuan wallet is deployed on the blockchain with a feature of anonymity.

II) Decentralization

The conventional crypto exchange is centralized, therefore users must conduct transaction through platform and are 'forced' to have confidence in the venue provider to behave morally. With that being said, traders still bear the risk of exchange being hacked and personal assets getting stolen. In the Bityuan network, however, personal data are stored securely in the distributed network nodes, traders transact seamlessly without relying on a trusted third party.

III) Non-native token exchange

All tokens issued on the Bityuan blockchain network are non-native tokens, which are possible to be exchanged through BTY, instead of exchanges.

3.4 Parachain

Three key words to know about parachain: scalable, efficient and secure. When compared to sharding scheme, parachain is proposed to be easier to scale and more intuitive, powered with more functionalities; it is not merely a decentralized application but is empowered with its own blockchain ecosystem; it is also more efficient and easier compared to cross-chain trading.

3.4.1 Background

The majority of the blockchain systems are composed of two essential components: consensus and state machine. The consensus component provides the security for the blockchain network, is the fundamental which differentiates blockchain system from a conventional software system. Whereas, the state machine supplies various functions to support the blockchain system. Most of the blockchain networks currently adopt one of the three main consensus mechanisms: PoW, PoS and DPoS. As to the state machine, the situation is different, every chain is embedded with a distinctive state machine because every chain is designed to serve a particular function. The nature of parachain is to share the consensus mechanism - 'network security' with the main network, and a blockchain developer will just need to build a state machine to fulfill the promise that the parachain is designed to make.

3.4.2 Why Parachain?

Outsiders may think that the security of blockchain network can be ensured if a handful of super nodes are established, or to add some mining mechanisms on top of that. As a matter of fact, the most recent 51% attack to a blockchain network with PoW consensus mechanism tells the many of us that PoW is not absolutely safe. As to DPoS mechanism, the relative smaller number of nodes will induce a higher probability for conspiracy among validators (nodes), the intuition behind DPoS was in fact to improve blockchain performance with sacrifice of network security - a tradeoff between performance and security. As we may probably notice by now, a blockchain network security is not supported by just a few nodes, it requires contributions from a dedicated technical team to maintain and a proactive involvement of community members to increase the size of nodes throughout the whole network, thus the security of the network. The resources that committed to maintain the security of the network is enormous, and since every public blockchain is isolated, the security resources from one network can not be reused to secure another network. A parachain is designed to share the consensus mechanism of the

main chain and therefore the security of the main chain.

3.4.2 What is Parachain?

Parachain (Parallel Blockchain) is a simple and scalable blockchain whose 'security' is provided by the main chain as it adheres to the consensus mechanism of the main chain. The relationship between a parachain and its main chain can be independent but also interdependent. A parachain can have its super nodes and state machine, but its security is supplied by the main chain, the transaction data and hash data on the parachain will be eventually kept on the main chain.

The main chain will ensure the security for its parachain, it also serves as a bridge to connect parachains for cross-chain interoperability, in this way the parachains and the main chain form a complete ecosystem. The best example can be seen in the league of royalty points where every business organization will have its own blockchain to issue its own royalty points, but the points are highly iliquid and not interoperable, just like the traditional point market. The existing problem in the point market is that points issued by a business entity can not be used in other business entities. The introduction of parachain can solve this problem, if every business organization incorporates a parachain to issue points individually and, through the main chain, they can exchange their points. For a singular blockchain, the ecosystem is difficult to set up and developed. For a muti-chain blockchain with many parachains, the security resources are shared and security is reinforced, but more importantly the parachains are connected and interactive.

3.4.4 The Nature of Parachain

One of the key notion for parachains are that they function independently, however they are connected among each others through the Bityuan main chain. There is a clear boundary among the parachains such that they all can process transactions at once without conflicting with other parachains.

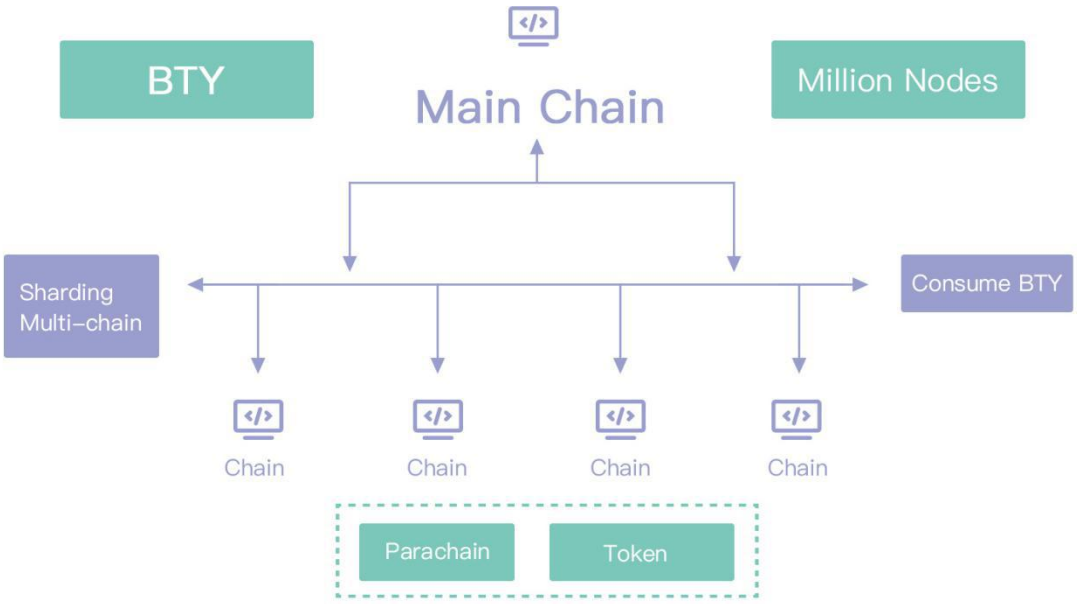
Conventionally, transaction is validated by each node before they are put into the block. Suppose now there are 10 parachains inherently different but are all attached to Bityuan main chain, the great thing about this is that these 10 parachains can execute transactions inter-dependently and simultaneously without fear of collision, which improves the 'transaction per second' magnitude by 10 times. Perhaps an analogy would offer a better insight, suppose initially there is one road connecting point A and B with a traffic capacity 2,000 per hour. Now, the government decides to add 10 more roads connecting point A and B, which enables the traffic capacity to increase 10 times.

Parachains are attached to Bityuan main chain, sharing the security resource from the security pool provided by Bityuan main network, without the need to provide its own. Decentralized applications can be implemented on parachains, which is desirable. Because this enables developers who do not have much blockchain knowledge, to build use-cases on top of parachain. This is also what Bityuan aims to do - allowing more to build blockchain applications with the least obstacles.

Every parachain can define its own functionality. When a bug is detected, the main network can easily implement upgrade to overly the bugged parachain, without inflicting the main chain.

Another pain point for blockchain in general is that the data contained in a blockchain is in a serial of events, therefore it is obligatory to download all the data to be able to validate the authenticity of the blockchain. Whereas, to validate a parachain, it is enough to just download the data which is relevant with this particular parachain.

Being a parallel chain in the Bityuan network, a parachain is incorporated with a independent wallet and a blockchain explorer. On top of that, a parachain can launch various blockchain projects within its own realm. Additionally, smart contracts can be created and executed. The more applications are built in the Bityuan network, the more frequent will cross-chain trading be taken place, which leads to the prosperity of the ecosystem.



3.5 DEX: Decentralized Exchange

The centralized trading faces regulatory hurdles as it is required to meet institutional legal and compliance criteria. Traders, inevitably, have to comply with regulations set by the trading service providers and trade with commission fees.

Bityuan's DEX trading pattern (Decentralized Exchange) will provide two convenient and secure solutions to this problem: BTC Relay and Hash Locking.

3.5.1 BTC Relay

BTC Relay is a method with the idea to incorporate a Bitcoin Simplified Payment Verification on Bityuan network.

Here is a insight of Simplified Payment Verification given by the mysterious Mr. Satoshi Nakamoto:

It is possible to verify payments without running a full network node. A user only needs to keep a copy of the block headers of the longest proof-of-work chain, which he can get by querying network nodes until he's convinced he has the longest chain, and obtain the Merkle branch linking the transaction to the block it's timestamped in. He can't check the transaction for himself, but by linking it to a place in the chain, he can see that network node has accepted it, and blocks added after it further confirm the network has accepted it. (Nakamoto, 2009)

BTC Relay is implemented by copying block headers in bitcoin blockchain to Bityuan blockchain, though it is not possible to verify the transaction, by linking it to a place in bitcoin blockchain, it is possible to confirm that bitcoin network node has accepted it. In this way, any willing parties can transact anonymously without a third party, and the whole transaction process will be done within 6 hours.

3.5.2 Hash Locking

Alternatively, Bityuan DEX proposes Hash Locking to complete an atomic cross-chain trading.

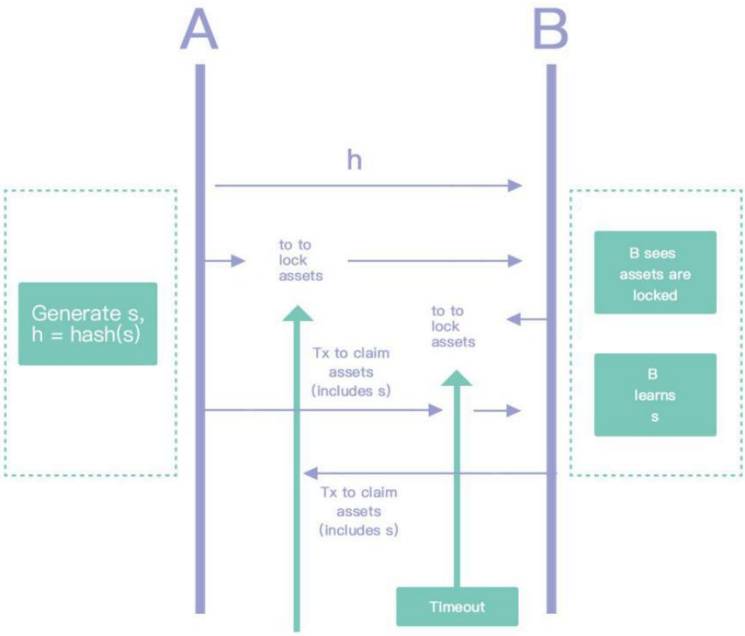
Atomic cross-chain trading refers to an approach where at least two parties own coins in separate cryptocurrencies, and want to exchange them without having to trust a third party. Between two parties, they agree on an exchange rate of the two cryptocurrencies and confirm to complete the trade.

Atomic cross-chain trading on Bityuan network is performed by using scripting languages to build smart contracts that will supply an asset transaction between two separate blockchain network securely, and with no third party involved.

Hash locking originates from the HTLC (Hashed Time Lock Contract) of the Lightning Network. If A owns 1 bitcoin and wants to transact with B with 20,000 Bityuan that he has, they will perform the following:

1) A generates a random number **s**, and calculates h = hash(s) and sends **h** to B;
2) A generates a HTLC. The take lock is set to be 2 hours for instance. If B finds the random number **s** within 2 hours, then A's bitcoin will be taken by B or otherwise A gets his bitcoin back. Note: both A and B know **h** but A has the key to the contract **s**;
3) At the same time, B deploys a smart contract on Ethereum platform, the one who provides an **s** that will have the hash of **h** will unlock the contract and take the 20,000 Bityuan away;
4) A takes away 20,000 Bityuan by providing the correct **s**;
5) B gets to know **s** when A providing the correct **s** to take the Bityuan, B can unlock HTLC and takes the bitcoin.

When the two parties agree on an exchange rate, their assets will be temporarily stored in a special place. Two ways to move away the coins, one is to provide the correct **s** which can lead to the per-calculated **h** with the hash algorithm, two is the time over-dues before the correct **s** is provided, and thus the coins will be back to each.



A provides the correct random number **s** to take the Bityuan away from B, because the blockchain network is transparent, so B can naturally find out what the random number **s** is, to take A's bitcoin.

Note that the smart contract is set to be in between party A and B exclusively, no third party can participate the trading, therefore when A broadcasts the number **s** to the whole network, no one else can take the coins away even though they all know what the number **s** is. The time lock on the smart contracts are different, the time lock A sets on his smart contract has to be longer than B's so that B will have enough time to take A's coins.

For future reference, Bityuan team will develop a handful of tools to utilize the atomic cross-chain process, in a way that the DEX can be also executed on a mobile end.

In conclusion, both BTC Relay and Hash Locking will make atomic cross-chain trading possible. Nevertheless, their differences are summarized in the following table:

Bityuan is more than just a simple, stable and scalable blockchain network. It promotes decentralized exchange with the method of BTC Relay and Hash Locking.

4. Governance

4.1 Issuance Mechanism

The native token in Bityuan network is BTY. It was created in early 2014 and adopted a self-innovative PoS algorithm. Currently, it has a circulation of about 320 million. Bityuan generates a new block in every 15 seconds, one block contains 30 BTY, of which 18 are collected by miners and 12 are allocated to the Development Foundation. The annual mining output is approximately 63 million. The minimum unit of Bityuan is 10^{-8} BTY. Every 10,000 BTY can buy a ticket for mining, and honest node mines through the ticket. The more tickets, the higher probability of mining a block. Malicious nodes that attempt to fork Bityuan, or any malicious activities that the system can detect, may be punished and will lose 20% of the funds. Mining must be carried out with the standard wallet published by Bityuan Foundation. Any modification of the mining behavior, if it is automatically determined as malicious by the system, will cause huge losses to the miners.

4.2 Development Foundation

Bityuan has always been committed to solving blockchain governance problems in an

autonomous manner. Community volunteers formulate community operation rules. Decentralized decision-making can build Bityuan into an autonomous and decentralized cryptocurrency while allowing all participants to get rewarded according to the efforts that has been put.

The Bityuan Development Foundation is established under the Bityuan Foundation, which acquires its primary source of funds through mining of BTY. The funds can be used to support the development, operation, and ecological development of Bityuan network, part of the funds are given as an incentives to Bityuan developers and council members or other purpose related. In addition, part of it will be used for tax reduction and public welfare activities.

The Bityuan Foundation will publicize the use of the Bityuan Development Fund in related channels and communities.

4.3 Roadmap

- May 2018

Bityuan launches on its main blockchain network, with an upper limit of TPS of 100.
Main functions: transferring, mining, parallel child chain (with its own independent wallet and service, child chain consensus security is provided by the main chain), wallet recovery, one-key token, hash locking.

- September 2018

The Bityuan achieves the function of atomic across-chain interoperable with Bitcoin (BTC Relay), and the decentralization exchange and transaction with Bitcoin. For example, after sending Bitcoin to a certain address, Bityuan or the token on Bityuan can be automatically sent to that person.

- November 2018

Launch a private transaction function to achieve completely anonymous transactions.

- February 2019

Bityuan launches a blockchain proposal mechanism and the Development Foundation will be used completely transparent.

5. Conclusion

The main purpose of the Bityuan network is to design a system that can be easily self-renewed, so as to gradually surpass Bitcoin, which is not yet in place. The

ultimate goal of Bityuan is to form an integrated development platform where all industries can store data and conduct transactions. It can pay, accept, store a variety of cryptocurrencies, support wallet recovery, mortgage payment, cross-chain coin transactions, PoS environmental mining, etc., and has a high degree of scalability.

We wish to build a sharing and prosperous ecosystem where blockchain is truly open, transparent, and equal to everyone. By adopting the token-incentives mechanism, we encourage more to join our community and contribute to the ecosystem, jointly build and maintain a highly secure and multi-layer blockchain ecosystem, and let the technology advancement guide us towards the future.