Bitvote.one

# Bitvote Whitepaper

# Table of Contents

# 1.0 Introduction

## 1.1 Background

Born in the wake of the global economic crisis, Bitcoin was a protest by Mr. Satoshi Nakamoto against the endless QE policy of a centralized monetary issuance system. In the traditional financial system, the national credit system and banking institutions controlled the issuance and circulation of money, which granted their power to exploit the people through the currency without any restraint. The point-to-point currency system proposed by Satoshi is a transformation of the traditional centralized system. Without interference of a centralized "supernode", all transactions are broadcasted to all network nodes, and become tamper-resistant after all the nodes confirm. In this way, a complete credit system can be established without the endorsement of third-party credit agencies.

The "miners" play an important role in this credit system. Miners can compete to solve math problems, and the winner would get bitcoins as rewards. Obviously, the more miners join, the safer and more trustworthy this system is. In the early days, only a handful of geeks were using their PCs for mining, and the processors could easily do the job due to low difficulty. However, with the rise of bitcoin prices, in order to obtain generous rewards, methods of increasing computing power began to be researched. Video card mining, FPGA mining, and ASCI mining were successively introduced. At the moment, the ASIC miner has replaced previous CPU mining with specialized chips that make SHA256 computation time faster and more efficiently.

Satoshi's vision of "one-CPU-one-vote" has been replaced by "one-ASIC-one-vote." Nowadays, the mining factory is often a huge warehouse filled with ASIC miners that operate 14/7. If the situation continues, the problem of centralization can happen again, which makes it difficult for ordinary bitcoin holders and enthusiasts to be involved in decision-making process of the community about which direction the entire community should go.

## 1.2 Bitvote overview

Bitvote's goal is to get digital currecy back to the state when all community members have an equal chance to participate, whether you are a miner or an investor. In the Bitvote ecosystem, more community members can participate in the development of the whole community by expressing their own feelings and putting forward their own ideas, thereby solving the problem of congestion in BTC transaction while realizing the vision of democratic autonomous community.

Bitvote has implemented replay protection to increase the security of BTV (name of

token issued) and tamper-resistance of voting results. In addition, the block size has been increased from 1 MB to 8 MB with Segwit support, which greatly improves the transaction speed and solves the issue of high concurrency. At the same time, the lightning network has been integrated to solve the problem of congestion, enabling BTV to be used for high frequency small transactions. BTV also uses a block mark voting system that prevents one party from abusing and controlling the system and ensuring that the user who owns the BTV has the right to speak. Other than the features above, BTV has also incorporated efficient smart contract that allow users to build applications and issue digital asset on BTV, making BTV a functional benchmark for value.

# 2.0 BTC status quo

## 2.1 BTC status quo

Voting has been used as a relatively fair multiplayer decision-making method since ancient times, and with the development of science and technology, voting can not only be conducted offline but also online with ease. However, since the data on centralized server is controlled by service providers, the authenticity of the voting results cannot be guaranteed and often is questioned. The fairness of voting is in name only.

In bitcoin's PoW (proof of work) system, the more mining machines you own, the higher computing power you have, the more likely you will get the right to create a block. In Chapter 4 of the Bitcoin white paper, Satoshi made the following statement about mining: The PoW mechanism also addresses the problem of identifying who is the majority in a collective vote. However, If the way to decide who is the majority is based on IP addresses, and each IP address has one vote, then the mechanism would fall if someone has the power to allocate a large number of IP addresses. The essence of PoW mechanism is exactly one CPU-ONE-VOTE.

In the bitcoin system, the emergence of large-scale mining factories has been regarded as a deviation from the original intention of bitcoin, as average participant do not have the voting right under existing circumstance. Currently, the voting power is concentrated in the hands of mining pools with a large amount of computing power, which runs counter to the concept of decentralization. Therefore, a change to the system would meet the needs and serve the long term interests of Bitcoin as well other cryptocurrency.

Bitvote is created to solve the problem of trust in the voting process. By using CryptoNight algorithms, Bitvote aims to implement Satoshi's original intention of ONE-CPU-ONE-VOTE on bitcoin. In general, Bitvote has set up a new digital currency experimental autonomous community, which can be applied to notarization, decision-making, scientific management and many other aspects in the future (Especially the AB-share management system that became popular all over the world, that is, the same-share-with-different-rights system). Bitvote will provide high-quality solutions to many large enterprises in the future. It will also guarantee fairness in the election of the government and organizations and improve the social credit system through decentralization.

# 3.0 Forking plan

## 3.1 How to get bitvote?

To get free Bitvote, you need to have BTC on block height when taking a snapshot. If you hold BTC, you will automatically get the same amount of bitvote at the same address, and you can use the same private key. Backup is also very important, your private key and mnemonic can help you recover your wallet. However, if you have BTC on the exchange or custody service provider, you do not need to access the private key. What you need to do is to make sure that the provider will support Bitvote. If you are unsure if your custody service provider will support bitvote, we recommend that you transfer your BTC to a service that supports Bitvote.

## 3.2 Hard fork

As a set of distributed ledger, modification to Bitcoin's code is done through a fork, which can be further categorized into soft and hard fork. The code itself is a consensus of the bitcoin network, so all BTC full nodes need to be run and perform the same consensus rules; nodes that implement different consensus rules are not part of the bitcoin network.

If a miner finds a new block that follows the bitcoin consensus rules and broadcasts it to the entire network to validate it, all the full nodes on the network will accept the block and all the transactions it contains. When the miners found that the block does not meet the bitcoin consensus rule, and the previous node does not accept the block, then the new block that has been mined would become a hard fork.

before the 478558th block, bitcoin and bitcoin cash nodes still follow the same consensus rules and accept the same block. But starting from that block, the new consensus rule for bitcoin comes into effect, and bitcoin full nodes refuse to use bitcoin cash ledger and the blocks from bitcoin cash nodes. This time, miners continue to use the bitcoin account, a direct result of the network forked.

Bitvote has hard-forked bitcoin by implementing a new consensus rule (estimated January 21, 2018, CET) with a projected height of 505050. The new rule will take effect in the 505051th block, a total of 21 million, out of the block for 2 minutes, 4 million bifurcation after digging, each reward 12.5 BTV. From this block, Bitvote Miners will begin to intervene to create a new branch of the BTC blockchain. This new branch retains the same historical deals and equity distributions on the blockchain, and of course if you hold BTC you will automatically get the same amount of Bitvote.

## 3.3 Affiliated exchange


## 3.4 Affiliated mining pool


## 3.5 Affiliated wallet

# 4.0 Technical feature

## 4.1 DAO decentralized autonomous organization

Bitvote uses DAO's organizational structure to support the idea of balanced distribution of voting rights. DAO, known as Decentralized Autonomous Organizations, is a combination of computer code, blockchain technology, smart contracts, and people. The founders of DAO can set out the basic rules for doing business. DAO has several stakeholders who can obtain relevant rights and have their own tokens. Essentially, all of these stakeholders want to increase the value of tokens to improve their status in the organization

DAO differs from the organizational relationship of a traditional corporate unit in that DAO's token holders (i.e. shareholders), instead of board of directors and managers, can decide on the development of community organizations. They have the right to vote "yes", "no" or "abstain" on any proposal the organization faces,

DAO's rules of operation allow efficiency rather than position to be the priority when doing transactions. Most importantly, in the DAOs on the Blockchain, we are no longer hired as employees, but get contracts on a project basis. For example, the community members can vote to decide whether to deploy Segwit, and it is immediately implemented after the proposal is passed.

Using DAO's organizational structure, Bitvote uses a block mark voting system to get the development team work with miners to prevent the risk of fork and to establish mutual trust among users without endorsement from a third party. With larger blocks and throughput to process transaction data, Bitvote can easily solve the problem of congestion in bitcoin network. Bitvote can be seen as a self-evolving version of BTC. Its stronger scalability can make bitcoin become much better in the future.

## 4.2 Mixed Consensus Mechanism PoW + PoS

Disagreements can occur in the community, and voting rights are created on the basis of PoW. If a consensus cannot be reached, that is, miners support different parties, a new token can be “forked off” from the original blockchain. However, the miners account for only a small portion of the entire BTC community, and most of the rest are investors. This is not conducive to the development and stabilization of BTC.

Bitvote adopts the hybrid consensus mechanism of PoW + PoS. Both users and miners who own Bitvote can vote and jointly participate in the major decisions of the BTV community. They can influence pre-programmed updates

on the blockchain, including Segwit, block scalability and more. If these updates are widely accepted, the blockchain will automatically be updated without intervention of developers.

Bitvote implemented the voting results of community members in a smoother way. The voting results were recorded on the blockchain and executed automatically, so as to resolve possible disagreements among all parties in the community and promote the healthy development of the community. PoW is mainly designed to prevent the system from being attacked by hackers or DDoS and ensure that information can be transmitted in a safer way without third party endorsement. However, the work of PoW system is mainly based on miners, the math problem need to be solved will become more and more difficult, and the cost of PoW system and the mining fee each transaction needs to pay to motivate miners to confirm transactions will become higher and higher.

The rise in transaction costs can result in heavy transaction congestion, reducing user experience for Bitcoin users. In addition, the concentration of computing power in a few pools will increase the risk of a 51% attack.

PoS (Proof of Stake) can solve the problem of PoW in resource consumption, but simply relying on PoS will lead to a solidification of class, because people who have more tokens are likely to get more tokens. Therefore, the adoption of PoW + PoS hybrid consensus mechanism can prevent PoS from distributing more shares to early investors, and the security guarantee provided by PoW mechanism can ensure the safe operation of the system.

Bitvote uses this hybrid consensus system to strike a balance between miners and users. general, miners who operate the infrastructure have considerable influence in the network, while users have relatively little influence. Bitvote allows users to directly influence the project without the need to buy expensive mining hardware, thereby creating a more harmonious and sophisticated cryptocurrency ecosystem.

## 4.3 MIMBLEWIMBLE

Bitcoin uses the blockchain's public database to hold all the transaction data, but the person who really wants to check the status of the system has to download all the data and traced each transaction. At the same time, most of these trades do not affect its final real state (they destroy one previous trades each time an output is created).

However, the entire blockchain must be fully validated to confirm the final status. In addition, these transactions are "cryptographically atomic", and it is clear what outputs go into every transaction and what emerges. The "transaction graph" can leak a lot of information and is subjected to analysis by many companies whose business model is to monitor and control the lower classes. This makes it very non-private and even dangerous for people to use.

Greg Maxwell discovered to encrypt the amounts, so that the graph of the transaction is faceless but still allow validation that the sums are correct. Dr Maxwell also produced CoinJoin, a system for Bitcoin users to combine interactively transactions, confusing the transaction graph. Nicolas van Saberhagen has developed a system to blind the transaction entries, goes much further to cloud the transaction graph (as well as not needed the user interaction) [3]. Later, Shen Noether combined the two approaches to obtain "confidential transactions" of Maxwell AND thedarkening of van Saberhagen.These solutions are very good and would make Bitcoin very safe to use. But the problem of too much data is made even worse. Confidential transactions require multi-kilobyte proofs on every output, and van Saberhagen signaturesrequire every output to be stored for ever, since it is not possible to tell when they are truly spent.

Dr. Yuan Horas Mouton fixed this by making transactions freely mergeable, but he needed to
use pairing-based cryptography, which is potentially slower and more difficult to trust. He called this "one-way aggregate signatures" (OWAS).

OWAS had the good idea to combine the transactions in blocks. We can combine across blocks (perhaps with some glue data) so that when the outputs are created and destroyed, it is the same as if they never existed. Then, to validate the entire chain, users only need to know when money is entered into the system (new money in each block as in Bitcoin or Monero or peg-ins for sidechains) and final unspent outputs, the rest can be removed and forgotten. Then we can have Confidential Transactions to hide the amounts and OWAS to blur the transaction graph, and use LESS space than Bitcoin to allow users to fully verify the blockchain. And also imagine that we must not pairing-based cryptography or new hypotheses, just regular discrete logarithms signatures like Bitcoin.

This technique can be used to prevent the blockchain from revealing the information of all users, so the inventor of the technology called it Mimblewimble (Curse of Silence, from Harry Potter).

## 4.4 Block mark voting

Due to the concentration of computing power caused by ASIC miner, the rights mechanism in PoW consensus has no longer had equal representation. How to establish a functional, autonomous community so that the disagreements can be resolved more democratically is a problem that every blockchain need to consider. BTV's use of block marking rights separate bid voting scheme made it possible for voters to reach a consensus when there is disagreement in the community and to prevent the differentiation between developer team and miners.

Bitvote separated the voting rights from the marking rights. Before the announcement of major events in the community, all community users can participate in the auction to obtain the block marking right. Marking rights are used for signing the vote, and the options each user have are "support", "oppose" and "abstain". The blocks that are signed are valid blocks, and the direction of community development is determined according to the voting results.

The following are the possible situations that can help during the vote:

1. If more than 90% of all the votes in the BTV are "abstain", the parliamentary vote will continue to be valid for the next BTV.
2. If all non-abstention votes within the BTV fail to meet the 75% majority threshold, the parliamentary vote will continue to be valid for the next BTV.
3. If 75% of all non-abstention votes in the BTV support the proposal ("support"), the proposal is confirmed as locked and the consensus would be changed after the vote has been passed.
4. If 75% of all non-abstention votes in the BTV oppose the agenda ("oppose"), the proposal will fail and the change to consensus will never be initiated.
5. If a proposal expires before reaching 75%, the proposal will expire and the change to the consensus will never be initiated.

Latest Blocks

| Height | Relayed By | Size(B) | Reward | Time | Block Hash | Block Version |
|---|---|---|---|---|---|---|
| 505,663 | BTC.com | 1,019,900 | 13.59041420 BTC | 20 minutes ago | 000000000000000000624683bea23b273278897b851b587795c9ae3470d3805c | Abstain Kral |
| 505,662 | F2Pool | 1,066,941 | 12.90831001 BTC | 23 minutes ago | 000000000000000000790be43c50c6379200787f4683bca0ec4778021f9203fc | Abstain Kral |
| 505,661 | BTC.com | 1,021,889 | 13.04461853 BTC | 24 minutes ago | 000000000000000000004229c213c7d5c986ba68973f32db793b32d8172d050ec | Abstain Kral |
| 505,660 | SlushPool | 1,006,360 | 13.11658520 BTC | 27 minutes ago | 000000000000000003ac554a00850993ef9196ef1b6b06ba67712fe18d1a46f | Oppose Bob |
| 505,659 | ViaBTC | 1,015,803 | 13.27285318 BTC | 29 minutes ago | 000000000000000006b624a43e551ddb1e63c1632c57ca97514a422cce4d122 | Oppose Bob |
| 505,658 | Bitcoin.com | 1,031,776 | 13.85783714 BTC | 31 minutes ago | 000000000000000000639975ef74cc059f7f7fdd7e772472ba6fb6b93a54fff3 | Oppose Bob |
| 505,657 | SlushPool | 1,004,109 | 12.84493959 BTC | 38 minutes ago | 000000000000000000033d72d1322f9f1911ae503a0b8c7b4ae4a30b93c703f95 | Support Alice |
| 505,656 | AntPool | 1,002,338 | 12.88202985 BTC | 39 minutes ago | 000000000000000000094247a0f21ba1966fc936c3e4fe042ecca997b366d7fc | Support Alice |
| 505,655 | ViaBTC | 1,003,017 | 12.81072518 BTC | 40 minutes ago | 000000000000000000019ef0693531100a7495eec38cbf9ac99e092a48d3662f2 | Support Alice |
| 505,654 | BTC.TOP | 1,021,226 | 13.85320046 BTC | 41 minutes ago | 000000000000000000001a1593a86a60a7a88d195c7061961956be6294a000a01f | Oppose Jack |

## 4.5 CPU mining algorithm

In bitcoin, the mining algorithm is SHA256. Also, the difficulty of the network would be adjusted every 2016 blocks (about two weeks), in order to keep the average interval between blocks around 10 minutes. If the average time between blocks is less than 10 minutes, the network difficulty will increase; if the average time exceeds 10 minutes, the network difficulty will be redueced

Bitvote uses CryptoNight algorithm. By using such an algorithm for mining, it can avoid the emergence of large-scale professional mining machines, thereby solving the problem of over-centralized computing power. The distribute of computing power on Bitvote network is balanced, and the network difficulty has been adjusted to be align with the goal of 2-minute intervals.

## 4.6 Block time acceleration

The block time for Bitcoin is 10 minutes, and each block has 1M of storage space. If the amount of transactions has exceed the amount of data that can be stored on the blockchain, those transaction data with higher transaction fee will be put into the blocks first, and the rest have to queue up and wait for the next work. That is to say, the capacity of the block and the block time would affect the speed the transaction being confirmed.

Compared to bitcoin, Bitvote has a 2-minute block time that shortens transaction confirmation time, improves transaction efficiency, and reduces transaction fees.

## 4.7 Block scalability

The Bitcoin blockchain is a global, distributed, public ledger with limited capacity. With the boom of bitcoin, the number of transaction conducted on bitcoin blockchain will become higher and higher. However, the limited block size will make low-value transactions (such as sending 1 cent) never be able to be recorded in blocks because low-value transactions cannot pay for expensive network fees.

Bitvote, on the other hand, uses large blocks (8M) that can accommodate more transactions. Even when a large amount of transactions need to be processed, the 8M block would allow Bitvote to pack all the transactions and get them recorded in the blocks. In addition, with a 2-minute block time, Bitvote can easily handle transaction data, and every user can enjoy the great convenience and benefits of Bitvote.

## 4.8 Replay protection

Replay attack is one of the most commonly used attacks by computer hackers. It occurs when the attacker sends a message already received by a target host to cheat the system. Replay attack is mainly used in the authentication process - undermining the correctness of authentication - so as to achieve the purpose of multiple fraud. If the recipient can effectively identify and refuse to replay the information, there will be no replay attack vulnerability, and the possibility of being attacked can also be avoid.

Because of the previous attack against Ethereum, it was not uncommon for replay attacks to be discussed widely before the birth of the BCH, and everyone was worried that such events would persist on both the BCH and BTC chains. Learning from the event on Ethereum, Bitvote developers have set up replay protection in advance - they added SIGHASH_FORKID (0x40) to the transaction data signature after the BCH fork, which will make the transaction data on both chains no longer compatible with each other. In this way, the possibility of the replay being recognized has been reduced to zero, thereby securing the system against replay attack

The risk of replay attacks is inherent in every hard fork. Therefore, Bitvote will provide technical protection for users after the fork to prevent loss of funds arising from user accounts being attacked.

## 4.9 BTV Foundation

The Bitvote Foundation is a non-profit organization that promotes the construction of the Bitvote community and maintains and facilitates the development of the Bitvote community. The BTV Foundation manages 20% of mining output and uses it to promote platform construction and research, development and education in basic level to better serve Bitvote and the decentralized technology ecosystem. The mission of the BTV Foundation is to complete the development of new applications and technologies under an open, decentralized framework, support the application of relevant technologies and protocols of BTV, and promote the development of autonomous community for digital currency .

## 4.10 Related technologies

**Smart contracts**: Smart contracts allow users to write custom behaviors and use them for blockchain without having to do more than one predefined action. By using smart contracts, users have the flexibility to extend their customized complex trading options and financial contracts. At the same time, users can limit and dynamically control expansion capabilities without having to modify or upgrade the code.

Smart contracts allow users to register customized contract bytecodes in the blockchain and invoke transactions in the BTV chain. Contract bytecode is executed in Turing

completion contract bytecode virtual machine. Developers can write smart contracts in a programming language and compile them into contract bytecode with reasonable syntax and apply them in the blockchain.

**Lightning Network**: The purpose of lightning network is to carry out off-chain transaction in a safe way. It is essentially a mechanism that uses hash time to lock smart contract to conduct a 0 confirmation transaction safely. By setting a "smart contract", the user can conduct unconfirmed transactions on the lightning network as securely as trading gold (or as bitcoin).

**SegWit**: If the block size is not enough, a simple solution is to scale it up to 1M. However, this would require a hard fork, and many people may disagree with it and are concerned that something will go wrong. Yet, another option is to reduce the size of data in a single transaction that plunges into this 1M block, which will allow for more transactions. SegWit is the way to put more transactions into the same 1M space. This would break the 1M block limit so it can accommodate more transactions.

**Zero Knowledge Proof**: Zero Knowledge Proof (known as "zk-SNARK") is the core technology to realize the anonymous nature of Zcash. "Zero Knowledge Proof" is defined as, the prover is able to convince the verifier that a certain assertion is correct without providing the verifier with any useful information. Thereal application is that the user is able to prove the money he has spent is less than his account balance without telling anyone his account balance and the spending. Therefore, the recipient can receive the transfer even without his public address being recorded.

**Quantum Resistance**: In the current blockchain system represented by Bitcoin, the SHA-256 hash calculation and the ECDSA elliptic curve cryptogram constitute the most basic security. Nevertheless, with the advancement in quantum computer, the existing algorithms cannot resist quantum attacks, which put a risk to user information and personal assets.
Post-quantum cryptography, also known as quantum-resistant cryptography, is a cryptosystem that is thought to be resistant to quantum computer attacks. Quantum-resistant algorithms, if successfully deployed, will provide stronger protection for private property and have a profound impact on the entire cryptocurrency.

**Cross-Chain Transaction**: Cross-link technology is the key to realizing value network. It is a solution that saves alliance chain from a separate and isolated islands and a bridge for expansion and connection of block chain to the outside world. Technically, blockchain is a decentralized database and distributed ledger; Commercially, it is a value network. In this value network, the more effective nodes are connected and the wider the distribution, the greater the possible value stackup. Blockchain is the core infrastructure of value network. Blockchain applications should not only be limited to alliance chain, which constrain the value in a small circle. We need cross-link technology to build highways for value network by facilitating the connection and expansion of different blockchains.

# 5.0 Milestone

## 5.1 Development Plan

Development Plan

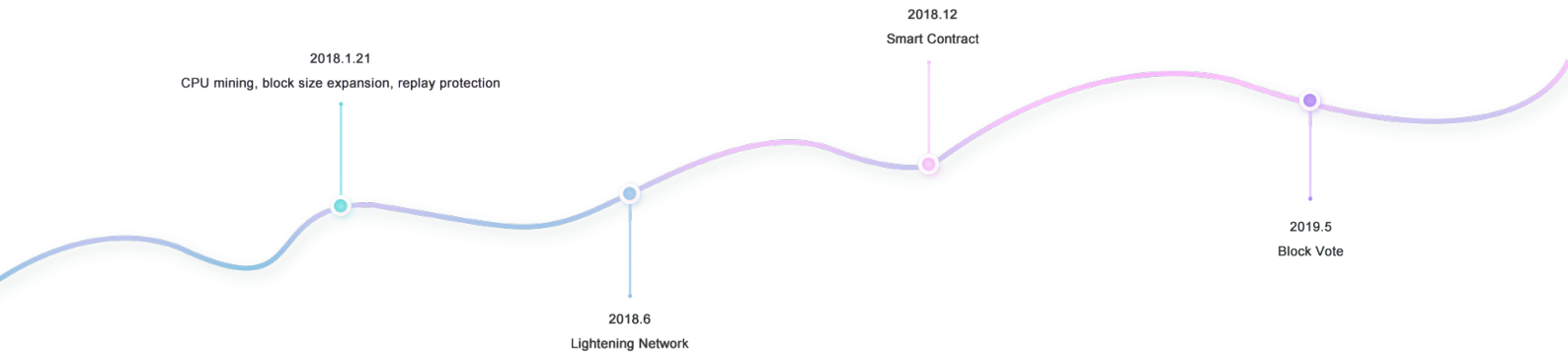
January 21, 2018: Fork planned for 505050 block height

January 21, 2018: Support CPU mining, scalability, replay protection

June 2018: Lightning Network

December 2018: Smart Contract

May 2019: Block Mark Voting System



# 6.0 Risk warning

## 6.1 Monetary regulatory risk

Governments are still designing public policies on the regulation of cryptocurrencies as a form of settlement. Governments who do not favor the use of cryptocurrencies in local commerce may release laws and regulations that prescribe the use of cryptocurrencies as a regulated activity. This may result in BTV holders unable to use their BTV in the future without further advancement of compliance by BTV.

## 6.2 Tax risk

The use of BTV as a settlement currency may or may not be subject to local income tax, capital gain tax, value added tax or other forms of taxation. This uncertainty in tax legislation may cause unforeseeable future tax consequences for merchants and customers on the use of BTV as a settlement currency or transaction token and the capital gains of BTV tokens.

## 6.3 Capital controls risk

Many jurisdictions, such as China, exercise strict controls over cross-border capital movements. The BTV holder may be subject to these requirements and / or to the enforceability of such provisions at any time. This will make BTV's move from local jurisdiction to overseas exchanges an illegal activity that will subject BTV users to government fines or other regulatory sanctions.

## 6.4 CTF and AML Regulations

The United States has introduced a series of provisions to combat terrorist financing and money laundering. Many other countries have enacted similar laws to control the capital flows of these illicit activities. The use of cryptocurrency by some criminals can violate these rules. The illegal use of any BTV can seriously affect the international reputation of the BTV network. In such circumstances, it is conceivable that this could lead to censorship by CTFs and AML regulators and could result in significant damage to the distribution and circulation of tokens and BTV tokens in the Bitvote ecosystem.

## 6.5 Blockchain risk

Hackers or other malicious groups or organizations may attempt to interfere with the BTV in a variety of ways, including but not limited to malware attacks, denial of service attacks, consensus-based attacks, Sybil attacks, smurf attacks and electronic scams. In addtion, becauseof the rapid

advances in technology, BTVs can become out-dated. The regulatory status of cryptocurrencies, digital assets and blockchain technology remains unclear or ambiguous in many jurisdictions. It is hard to predict how the government will manage these technologies and whether the government authorities will make any changes to the existing laws, regulations and / or rules that affect cryptocurrencies, digital assets, blockchain technology and their applications. Such changes can have a negative impact on BTV in a variety of ways, including, for example, determining that tokens are regulated financial instruments that require registration. If a government act makes it illegal or continuing the project not viable commercially, the company may stop the distribution the BTV and the development of the project or stop the operation of the project in this jurisdiction.

# 7.0 Contact

## 7.1 Contact

**Official website :** http://www.bitvote.one/

**Media cooperation :** media@bitvote.one

**Customer service** :support@bitvote.one

**Twitter** :bitvote.one

**Reddit** :bitcoinvote

**Sina Weibo :** bitcoinvote

**Wechat subscription account :** bitvote


Bitvote.one