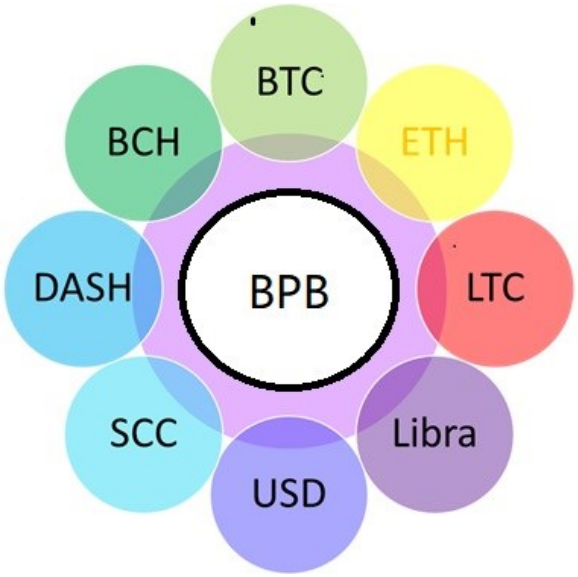
MacroSQL Stable Fiat Coin Technology

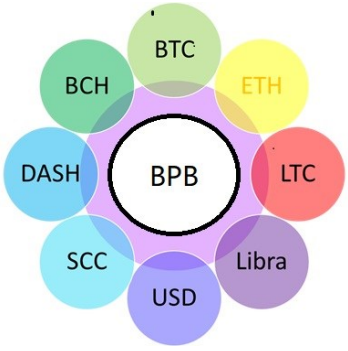


High Security + High Throughput

National Stable/Fiat Bitcoin

Stable coin has characters of open verification, low cost, 24x7, offline, globalization and centralized management, will be beneficial to decrease the financial cost... and likely to dominate future monetary system.

But existing crypto systems such as bitcoin/Ethereum, still lack the high reliability, security, transaction speed that are mandatory for national stable coin. The Byzantine generals' problem is a long-standing problem of distributed data consistency. Research papers on the subject began in 1982. In 2009, Bitcoin became the first digital currency in the world that successfully solve the problem of distributed data consistency by utilizing ECDSA cryptography and the asymmetric SHA256. The approach of Bitcoin is more rigorous than that of other digital currencies. In particular, it has avoided the huge security weakness brought by gigantic virtual machine. The flexible smart contract of Ethereum is based. However, Bitcoin still faces a few major problems: slow transaction speed, two wallets can potentially produce same address, and 51% computing power attack, irreversible on errors. These mean that none of the current digital currencies are 100% reliable while no sovereign currency or commercial currency can afford any error.



MacroSQL is a leading cluster database company in Silicon valley, California, with solid experience in financial transaction. MacroSQL Stable Coin (**MSC**) technology is designed to address the problems listed above. MSC has the following characteristics:

1. **Retail payment support**: The three-tier blockchain can achieve 3 million transactions per second while scalable, enough to support national and global payment into the future.
2. **100% Security**: It solves the 51% computing power attack, address overlapping, Ethereum's VM vulnerability, resistant to hacker attacks. It is 100% bullet proof that is required by national and commercial banking.
3. **Publicly Verifiable:** Because MSC transaction is publicly verifiable via blockchain browser, while Alipay and Wechat transaction are not publicly verifiable.
4. **Anonymity** : It has 3-tier architecture. Level 1 of MSC is built on top of Bitcoin. Level 2, 3 adding more acceleration and check. The flexible 3-tier architecture can be modified modularly and avoid collateral damage. Its anonymity and decentralization can be fine-tuned for specific countries.
5. **Multi Channel**: It can connect to various blockchains and commercial bank interfaces, conduct bank-level security transactions and commercial retail payment via secure multisig.
6. **Error Correct/Prevention**: MSC's error prevention and correction are partially located in layer 2 & 3. address can be blacklisted. There is a lot of flexibility to add more error prevention logic in layer 2 & 3 as time goes by.

Security Challenges:

At the beginning of this article, we said that the current blockchains do not completely solve the security of Byzantine generals' problem. Bitcoin still faces the problem of 51% computing power tampering with blocks. Not only that, because the blockchain transaction data is irreversible and there is no personal identity information as customers in banks, it is almost impossible to recover it after the digital currency is stolen. Crypto currency has become the heaven for hackers. And even employees of a company can pretend to send bitcoin to wrong address by mistake. Hackers can apply to become employees, and employees may become hackers because of greed; Mobile phone chips and memory are hardware without ECC fault tolerance. Mobile phones can be stolen, broken, flooded; computers and mobile phones can be attacked by Trojan horses, viruses and hackers. There are Trojan horses and viruses on 90% of computers and phones, and tens of thousands of people lost their digital wealth. Also, hash algorithms are vulnerable to quantum computers attacks……all these problems need to be solved within the blockchain ecosystem. In fact, many existing blockchains and trading platforms are very crude, very unreliable and are hacked frequently. In business, supervisors are absolutely afraid of taking any risk listed above. How to solve these problems is the key for the wide adoption of blockchain in the commercial and financial fields.

From the fact that Ethereum and smart contracts have been breached more than 50 times; the fact that most trading platforms and wallets are even more often hacked, it is clear that the current blockchain and trading platforms have serious shortcomings. Because the irreversibleness and non-identity of receiver, the security requirements of customer accounts need to be hundreds of times more robust than existing banking system and exchange, and more resistant to malicious behaviors.

Smart contracts and the Lightning Network are design at the cost of sacrificing its security. The smart contract code is dynamically interpreted by the virtual machine. This dynamic interpretation is highly flexible but it introduces security issues. First of all, the code of this kind of virtual machine is gigantic, which is "non-deterministic" and hard to guarantee security of every line of code; it is difficult to be flawless. Since the birth of Ethereum, more than 50 major hackings have happened. Bitcoin has never been compromised and is very safe. Therefore, it is ideal if one can solve the weaknesses of Bitcoin while utilizing its advantages.

Performance Challenges:

Big performance problems of crypto come from its linear general ledger structure, and a large amount of computation for encryption and decryption. These two aspects make it difficult for the blockchain to be fast in operations such as classification, statistics and search. It is slow because it has to linearly traverse billions of historical transactions while decrypting and parsing, and the length of each block and transaction are both not identical and cannot jump transactions or blocks.

MacroSQL Architecture Improvements:

MacroSQL is the leading real-time cluster database company in Silicon Valley, USA. Blockchain is also a simple distributed cluster database, thus MacroSQL's cluster DB technology is perfectly suit for improving blockchain.

MSC uses 3-layer architecture: the bottom layer is an improved Bitcoin network. Layers 2 and 3 are acceleration, security and reliability layers. The third layer of MSC also includes payment, banking and interfaces; These three layers are fully interoperable.

The second layer uses MacroSQL real-time cluster database to achieve real-time data consistency, which simplifies the processing of synchronization and data correctness, and engineers can focus more on the verification of data logic. Data ACID is handed over to the MacroSQL cluster database to deal with. The second and third layers have various checks via machine learning, credit learning and confirmation mechanisms, as well as security features such as deep freezing, PKI/RSA public and private key security and other functions. High-digit PKI is more effective against quantum computers than ECDSA/hash.

Not only can the second and third layers of the blockchain monitor the correctness of the system, the second and third layers also complement the deficiencies of the Bitcoin's code check; jointly complete data correctness monitoring and credit monitoring. Adding 2, 3 layers of software to collaboratively enhance the data consistency of the entire system, so as to make full use of all the advantages of the Bitcoin network. At the same time, it enhances automatic audit and supervision logic code to strengthen the maliciousness resistance and correctness of the network. Considering the second and third layers as the extension and enhancement of the underlying blockchain data validation system. They collaborated to overcome the weakness of current blockchain systems.

Tier-3 is an enhanced banking, payment, management system on top of blockchain, it serves to enhance security and functionality of national stable coins. Tier-3 has multi-level intelligence learning, address reputation, RSA key authentication, and multiple PKI security lines of defense. With one-way encrypted information, multi-signature multisig authorization, even if a hacker breaks in or steals account, they may not get multiple authorizations. Large and business customers can choose the high security level settings, and can customize the design and choose which kinds of defense lines to use. There is also 3-layered firewall and an IDS, which is an online IP packet monitoring system developed by MacroSQL. Because hackers and employees can intermix. So online IPS monitoring is necessary.

An open blockchain system actually requires much higher security than banks. We believe that the security, reliability, and fault tolerance of a blockchain system are far more important than any other things. If asset security is not guaranteed, the Byzantine loophole is not resolved, and the wallet is not resistant to disasters, there will be no possibility of widespread commercial application.

This three-tier structure can fully combine and enhance the existing advantages of the Bitcoin blockchain, cluster database and banking system. Our framework solved most of weakness of existing crypto system, it is secure, has high throughput and can be customizable. We are looking forward to cooperate and assist central banks in different countries/organizations to implement successful national fiat stable coins.

Dave Liu

CEO, MacroSQL Technology

dliu@macrosql.com