Bitsing

Preface

Following the framework proposed by BitTribe on how a peer-to-peer monetary system may be built, a group of architects, who have participated in drafting the BitTribe guidelines, join their efforts again to build Bitsing, a public blockchain implementing the idea of BitTribe, in the hope that it may serve as the first of its kind in providing the world with a peer-to-peer monetary system.

I. Understanding “BitTribe: A Peer-to-Peer Monetary System”

In the paper “BitTribe: A Peer-to-Peer Monetary System”, a purely peer-to-peer monetary system is proposed. In this system, money issuance is no longer controlled by one institution or a small number of people, rather the right of money issuance lies in the hands of all participants. In addition, the quantity of the money supplied will be determined according to its demand on the market. In this system, the privileges and benefits of money issuance no longer belong to those "closest to the money printing machine", but are truly shared by all the average people.

A money needs to be backed by faith, which in turn may come from an asset of value such as gold, or from our belief that the money issuer is willing and able to issue the right amount such that the price levels will stay stable. The Bitcoin system designed by Satoshi Nakamoto, for example, is backed by the faith based on the consensus of all the participants in a decentralized system. However, Bitcoin does not feature stability due to its inherent design and it is similar to gold, more suitable to be an asset rather than a money.

The paper “BitTribe: A Peer-to-Peer Monetary System” is based on the original vision of Satoshi Nakamoto and the experience accumulated from the practice of Bitcoin system in the last ten years. Furthermore, it proposes an operable mechanism of a new monetary system. It can be simply described as a process similar to Bitcoin by which miners acquire cryptoassets through mining, and then collateralize their cryptoassets to the Reserve Bank to issue currency for circulation, thereby completing the money issuance process. What needs to be explained is that the Reserve Bank is not a centralized institution, but just a set of smart contracts coded into the system. The Reserve Bank by itself cannot determine the quantity of money in circulation. The cryptoasset collaterals of all miners or all participants within the system and a consensus based smart contract Money Issuance Protocol are the true determinants of the quantity of cryptocurrency in circulation. This is a decentralized process of money issuance purely based on demand and supply of market. Because the miners obtain cryptocurrency through collateralized cryptoassets, they can deposit cryptocurrency into commercial banks within the same blockchain community (i.e., a group of smart contracts acting as commercial banks) or directly lend to others in demand to earn interest. Therefore, the interest rate of borrowing and lending, which fluctuates with the demand of money on the market,

will directly affect the behavior of the miners to collateralize the cryptoassets. When the rate of interest goes up, the amount of the collateralized cryptoassets increases, the money supply on the market goes up, and vice versa. This leads to a dynamic balance of monetary supply and demand.

From the above analysis of this decentralized process of currency issuance, it can be found that it also relies on an important factor: the decentralization of mining process of cryptoassets. In Bitcoin system, Satoshi Nakamoto proposed mining based on proof-of-work or PoW. However, because Bitcoin uses competitive mining, i.e., the first miner finds the "golden nonce" receives exclusive rewards, it led to the emergence of giant mining pools. Consequently, the hash power of Bitcoin network has gradually concentrated to top five mining pools. An ordinary individual miner cannot mine Bitcoin without joining a giant mining pool, which seriously violates Satoshi Nakamoto's original vision. In BitTribe paper, it proposes a new proof mechanism, decentralized Proof-of-Work, dPoW, in which Proof-of-Work algorithm and Verifiable Random Function (VRF) are combined to optimize the mining process from competitive mining to cooperative mining. Thus, everyone who participates in the mining process can benefit from their work, which encourages everyone to participate mining. At the same time, the mining machine contributing the hash rate and the miner's identity are bound to ensure that a miner can only hold a limited number of mining devices. This binding will prevent concentration of hash power to achieve much more even distribution of cryptoassets through mining.

The core value of BitTribe is to propose a new peer-to-peer monetary system which can be the foundation of future digital economy, and to provide the technical solution of the key problems involved. The core guidelines of the paper, like those in the Satoshi Nakamoto's paper ten years ago, can guide the development of a new social experiment.

II. Overview of the Bitsing blockchain

Bitsing is a blockchain that fully follows the ideas of BitTribe paper, which aims to establish a new monetary system and the necessary infrastructural services for the future digital world.

Bitsing will follow the principles of no institution, no external financing and no pre-mining. No institution means that Bitsing will be like Bitcoin system, which is fully owned by the participants and will not be controlled by a centralized organization. No external financing means that Bitsing is funded by the project development team's own investment with no external private or public offerings. No pre-mining means that the limited amount of cryptoassets could be obtained by the project development team only through mining after launch, rather than through pre-allocation.

Construction of Bitsing includes a monetary system based on asset collaterals, a public ledger, a Reserve Bank and commercial banking system and a decentralized crypto identity system.

-- Monetary system based on asset collaterals. The monetary system realized by Bitsing is based on the mechanism of mined cryptoasset and the circulating cryptocurrency issued through cryptoasset collateral, and using Oracle machine (an agent that finds and verifies outside

occurrences and submits this information to a blockchain to be used by smart contracts) to determine the borrowing interest rate and adjust the issuance of money.

-- Public ledger. The public ledger of Bitsing will adopt a fully decentralized dPoW consensus algorithm by sharing mining hash power to ensure the decentralization of the mining nodes and making the public ledger more secure, credible and stable, and at the same time ensure a fair initial distribution of mined cryptoassets.

-- Reserve Bank and Commercial Bank system. Functions of Reserve Bank and Commercial Banks can be implemented with a set of smart contracts and algorithms. Reserve Bank is responsible for accepting cryptoasset backed collaterals and issuing cryptocurrency for circulation. Commercial banks accept cryptocurrency deposits to provide financial instruments to support the development of the token economy.

-- Decentralized crypto identity system. The non-tamperable and secure nature of blockchain provide a new world identity to each native resident. This system will continue to provide support for governance in the new crypto world.

Bitsing will adopt a new approach to address the following four key issues:

The first issue is the cryptoasset allocation of Bitsing. A total of 21 million cryptoassets will be issued. The project development team can attain up to 4.9%, all through mining efforts after launch. As a result, the project development team will provide necessary mining power at startup (similar to bitcoin startup), and maintain the operation of Bitsing when the number of participants is insufficient while accumulating the targeted percentage of cryptoassets through mining efforts. The project development team's mining devices will exit the network’s mining reward system after mining 4.9% of cryptoassets. The rest of the cryptoassets will be mined by other miners in Bitsing.

The second issue is reducing energy consumption. The huge energy consumption has been another focus of Bitcoin's criticism. However, in Bitsing, because collaborative mining algorithm and dPoW are used, the mining difficulty value can be calculated according to an upper limit of hash rate. Therefore, in Bitsing, the direction of development of mining chip is to reduce the electricity consumption.

The third issue is the community building of Bitsing. Bitsing will build its own digital autonomous community, i.e., Bitsing tribe It will be built by its evangelists and believers based on common culture, shared value and vision. Bitsing tribe will uphold the core concept of equality, freedom and justice, and carry out governance through a bottom-up multi-stakeholder governance model.

The fourth issue is the development of Bitsing. The source code of Bitsing will be all open source. The future development of Bitsing will be guided by the Bitsing tribe residents. Of course, Bitsing tribe also welcomes other digital tribes or communities to participate in the construction and governance of Bitsing.

In memory of Satoshi Nakamoto's original Bitcoin paper published 10 years ago, we would like to celebrate it with proposed Bitsing, and look forward to building a brilliant new digital world built on consensus, and heading for a higher dimensional digital civilization.