SAT White Paper

Date: 2020-01-13

Abstract

The SAT: The return of the King of digital currency.

SAT is not a new currency，it is a rebirth of Bitcoin after 12 years of Bitcoin and the original intention of Satoshi Nakamoto. The requirement of growing Bitcoin application！

The 12 year of Bitcoin has three times halving, this is calling his original intention and demand！

As Satoshi expected. In the past, 20,000 BTC only can get a pizza, but nowadays, a BTC can buy 20,000 pizza and it could get 200,000 pizza in the future！

The purpose of Bitcoin is for circulation and transaction, it should not be a collection on the shelf. Satoshi's white paper already told that sat as the smallest unit will become a new currency.

With the progress of society and the development of science and technology, history repeat and repeat in an ascending spiral！The development of decentralization should not leading by centered thoughts and methods in this world. In the decentralized digital world, the consensus of digital should be the only rule.

What is monetary? It means the currency with value and used for transaction and circulation.，Financial is the result of the development of human history, not related to any political party or form of economy. Every war of financial is caused by humanity, not technology.

Sat is the smallest unit in Bitcoin named after Satoshi，and is his original intention. The BTC is a treasure in his mind, but the SAT is the real currency for transactions。

SAT is stablecoin of Bitcoin，is the only decentralized token coin in Markets. As a stablecoin, its value should be pegged to Fiat Money or digital

currency? How can history go backward? Since it has progressed to the era of digital currency then it should leave the world controlled by fiat money.

Now is the calling of Bitcoin. The original design of Satoshi makes the SAT today. SAT is birth for Bitcoin after 3 times of halving.

Base on SAT, we all the royalty craftsmen to making the real digital world come true.

Seeding of SAT, building the digital world with ecological industry chains of finance, medical care, agriculture, industry, commerce！ These are the achievements of each generation.

Take the SAT as a pledge, we proclaim private property should be sacred and inviolable. Defend the ownership of personal property and the right of making profits or disposal! We pledge to protect people property and oppose undocumented crimes！

In the name of SAT, we against rigid society, believe that God rewards the diligent！We believe digital is the solution and asking for the right of decentralization!

Chapter I. Introduction

a. Summary

Sat is the abbreviation of Satoshi and the smallest unit of Bitcoin. SAT is not a new digital currency, it is the son of Bitcoin.

Bitcoin has valued over 40,000 dollars, which shows that Bitcoin has obtained more and more people's approval. Bitcoins as a representative of digital currencies, but it behaves more similarly a symbolize than a transaction currency now. Twenty thousand Bitcoin to get a pizza just like yesterday, but now you can get 20,000 pizzas using a bitcoin.

The rising value of Bitcoin makes it not suitable for daily transactions, decimals could cause misunderstandings, Its inconvenient for the transaction.

Thanks for Satoshi leave 8 decimals for Bitcoin, it is the original unit of Bitcoin, just like dollars and cents. A transaction requires proper unit, Bitcoin also requires its own token coin. SAT is the best token coin of Bitcoin and every decentralized digital currency.

Digital currency is historical progress. Stablecoin accelerates the development of digital currencies. But there have many stablecoins that are centralized and make for fiat currency. History should not go back, those coins are created in the transitional period. The real stablecoin is decentralized and serves all decentralized digital currencies. SAT is the best stablecoin since it is from Bitcoins' smallest unit.

b. Idea

1) SAT is not a new coin is born from the smallest unit of Bitcoin, the return of Bitcoin.
2) SAT is the world's first decentralized digital stablecoin. It is a stablecoin for Bitcoin and all centralized digital currencies.
3) SAT is the transaction version of Bitcoin, has more quantity and the faster transaction to satisfy the realistic requirements of transactions.

Chapter II. SAT Distribution Statement

a. Parameter

1) Symbol

   i. Name：SAT

   ii. Unit：SAT

   iii. Icon：

2) Founder：Satoshi and his followers

3) Quantity：21,000,000,000

4) Smallest unit：0.00000001 SAT

5) Block generation time：2.5 minutes

6) The initial block reward: 12,500 SAT

7) Block reward halving every 840,000 blocks.

8) Algorithm: SHA-256

9) Synchronized Bitcoin on January 13th

10) Initial rate：BTC：SAT=1：1,000

11) Divide to 1:1,000 when a Bitcoin over 1 million

Chapter III. SAT Technical Description

SAT as the son of Bitcoin, continued its characteristic and did not change any main technical to keep the original intention of Satoshi.

a. SAT Architecture

Based on the peer-to-peer distributed network architecture, it works with a different type of nodes. A full SAT node includes route, blockchain data, miner, and wallet. Each node is joined to the SAT P2P network as a route to discover nodes and keep connected. Every node participates to verify blocks and disseminate.

b. SAT Wallet

Wallet includes:

1) Private Key: the 32 bytes（256bits）random string from SHA-256 which is the wallet password of every holder.
2) Public Key: created with a private key that is public and acts as the account number of wallet holder.
3) Wallet Address: It is a 160 bytes base58 string created from a public key after a hash of SHA-256 and RIPEMD-160. Holder could have almost 2^161address to receive SAT. The P2PKH address prefix is ‘S’ and the P2SH address prefix is ‘T’。
4) Support SegWit(Segregated Witness) address. This technic is the important standard for Bitcoins’upgrade, it could lower transactions fee and process times. But Segwit only supports when 95% of Bitcoin nodes updated, SAT support in begging and the prefix is sat.

c. Transaction

Using SAT wallet to doing SAT receive and payment. In Bitcoin, miner calculates and create blocks around every 10 minutes to publish transactions, but it is too long for nowadays, especially user

would like to check transaction result faster. To speed up the block generate time, SAT's block time spacing is around 2.5 minutes.

The following are the steps of the trading network:

1) The new transaction will be broadcast to all nodes.
2) Each miner node tries to find a HASH value that meets the current block difficulty requirements.
3) When a node finds a HASH value that meets the current difficulty, it will broadcast the block to all nodes.
4) The node will accept the block when all transactions in the block are valid and have not been spent.
5) Node uses the current block hash as the new block's previous block hash to join the new block in the chain。

The node will always consider the longest chain to be correct and expand it. If two nodes broadcast two new blocks of different versions at the same time, some nodes may receive one of the blocks first. At this time, the node will process the first received block, but also save another branch chain to prevent it from becoming the longest chain. When the next block is found and one of the chains becomes a longer chain, the nodes that originally worked on the other branch chain will switch to the longer chain. New transactions do not have to be broadcast to all nodes, as long as these transactions are broadcast to enough nodes, these transactions will be integrated into a block soon. Block broadcasting also allows for message loss. If a node does not receive a block, when the node receives the next block, it will know that it missed a block and will generate a request for the missing block.

d. Incentives

In SAT, blocks generate every 2.5 minutes, the miner who creates the blocks first could earn the block reward to incentivize people to maintain nodes to support SAT networks. This provides a method of currency

circulation without a central authority to issue currency. Realistic miner spends time and resources to mine golds, in SAT system miner consumed own resources include time and power to do calculations using CPU, GPU, and ASIC devices, this is proof-of-work.

Every 840,000 blocks — or approximately four years — SAT cuts block subsidy in half. The purpose is to reach an equilibrium of supply and demand and incentive transaction fees as block rewards after reach 21 billion SAT released to avoid inflation.

The reward mechanism also helps to encourage nodes to remain honest. A greedy attacker can have more CPU power than all honest nodes. Then the attacker will be facing the below choices: double-spending attacks to swindle previous payments or generate new currency through honest proof-of-work. Attackers will find that it is more advantageous to follow the rules. Complying with the rules allows the attacker to have more SATs than destroying the legality of the system and their own property.

1) Proof-of-Work

There are many encryption algorithms nowadays. SAT adheres to the spirit of Bitcoin and Satoshi Nakamoto's original intention. SAT continues using the SHA-256 hash algorithm. On average, as the number of leading 0 bits increases, the amount of work required will increase exponentially, and only one hash operation is required for block verification.

In the timestamp network, by increasing the nonce value of the block, until the block hash value equal to the number of leading 0 bits and the nonce value is found. Once the computing power meets the requirements of the proof of work, the block cannot be changed unless the calculation is done again. When the block after a block is connected to the chain, all the workload after the block needs to be completed to change the block.

Proof of work also solves the problem of majority representation. The

majority is represented by the longest chain because the longest chain has the largest proof of work. If most of the CPU computing power is controlled by honest nodes, this honest chain will grow the fastest and surpass any competitor's chain. To modify the previous block, the attacker must re-complete the proof of the workload of the block and all subsequent blocks, and catch up with and exceed the workload of honest nodes. We will explain later that the chance of a slower attacker catching up will exponentially decrease as subsequent blocks increase.

In order to solve the problem of increasing hardware speed and nodes number in the network would not be stable, the difficulty of proof of work is determined by the average number of blocks generated per hour. The SAT will update the difficulty once a day to ensure that blocks are generated in an average of 2.5 minutes. If the speed of block generation becomes faster, the difficulty will increase accordingly.

e. Update and Maintenance

   SAT keeps maintenance by SAT dev team, Bitcoin dev team, and the communities which would like to makes digital currency better. Everythings are volunteer and decentralized. See more information on https://www.satcoin.org.

Chapter IV. Positioning and Prospecting of SAT

a. the present situation of stablecoin

Before discussing stablecoin, what is the stable meaning? Stablecoin corresponds to fiat money or legal tender in traditional financial concepts. The stability of fiat money is about purchasing power and the important index is the inflation rate. As the world-first currency, the value of the US dollar is related to inflation the keep floating rate of inflation between 2% every year. Most fiat money in the world related its value to the US dollar and the inflation of each country.

Then people created centralized stablecoin as the bridge of fiat money and digital currency which relate its values to fiat money. This is one of the solutions, but compare to finding a solution in decentralized digital currency focus on fiat money will push the history going back.

b. SAT is the world's first decentralized digital stablecoin. It is a stablecoin for Bitcoin and all centralized digital currencies.

1) SAT is the smallest unit of Bitcoin
2) SAT is the token coin of Bitcoin
3) SAT is the token coin of centralized digital currencies

c. Decentralize stablecoin is the historical progress

Stablecoin is created to solve the transaction problem between digital currency and fiat money. But the solution should consider decentralized digital currency, not fiat money.

SAT is the first decentralized digital stable currency, as the Bitcoin 12 years ago. We expected SAT to grow and solve the problem of transaction time, and leading digital financial popularize.

Chapter V. Quantity of SAT

SAT as a practical token of Bitcoin, synchronize the released quantity of Bitcoin. After a consensus of the development team and participate development community, the quantity of SAT will have allocation below:

The quantity of SAT is 21 billion and each block reward started from 12,500 but since Bitcoin has third-time halving. For synchronizing, the genesis block reward will have 87.5 % of SAT. Compare to other digital currencies even people could mine from the beginning, but there a lot of digital currencies with no actual value now. We decide to synchronize Bitcoin quantity and use this 87.5% to create application value for SAT.

For those people who doubt this pre-mine is unfair, we declare the 87.5% SAT of genesis block will separate into 3 public wallet addresses under the supervise of SAT community and use to hedge, development plan and guarantee of exchange, etc. To maintain the value of the SAT, the community only pays SAT from public wallets which would help the future of SAT.

Allocation of the quantity of SAT

<table>
<tr><th>Proportion</th><th>Quantité</th><th>Proportion</th><th>La description</th></tr>
<tr><td>Inédit
12.5%</td><td>2.625 billion SAT
SAT block reward</td><td>12.5%</td><td>The reward for miners who runs on the SAT network.</td></tr>
<tr><td rowspan="3">Publié
87.5%</td><td rowspan="3">18.375 billion SAT</td><td>12.5%</td><td>• SAT maintenance and upgrade.
• Reward to financial partners which cooperate in begging.
• Reward to entity partners which cooperate in begging.
• The reward of promotion.
• Digital currency solutions.
• sponsored Digital currency conference.
• Digital currency exchange cooperation.</td></tr>
<tr><td>25%</td><td>End-device construction includes ATM, POS, smart banks and mobile phones, etc.</td></tr>
<tr><td>50%</td><td>Freeze for 4 years, then use for building a decentralized digital city includes blockchain infrastructure development</td></tr>
</table>

			center, lab, entertainment, and blockchain AI medical center, etc.

The rule of unfreezing and releasing 50% of SAT: After 4 years, base on the demand for development of the SAT. The first year will not release over 10% which is 2.1 billion to the world, and the second year will not over 15% which is 3.15 billion of SAT.

Chapter VI. Ecosystem of SAT

a. Software

1. Develop SAT online real-time trading system, to solve the trading bottleneck of digital currency
2. Develop SAT online boutique store, archive real-time shopping of boutique using digital currency
3. Develop wallet anti-tracking system to protect users right and safety
4. Develop decentralize digital currency exchange, makes the SAT, Bitcoin and all digital currencies could transaction any time anywhere

b. Hardware

1. SAT real-time transaction ATM
2. SAT mobile phone with building wallet
3. Unified hardware system

c. Products

1. SAT ATMs
2. SAT mobile phones
3. SAT POS machines
4. Financial AI system with non-profit organizations

d. Business

1. SAT online Europe boutique store
2. SAT online Japan boutique store
3. SAT online China boutique store
4. World-first online travel service with digital currency
5. Asia-first online real estate investment service with digital currency

e. Ecosystems

    1. Integrate the financial end-device, makes mobile phones, POSs, ATMs to work together in real-time for SAT
    2. Organize the Europe and Asia trading system and create Europe and Asia joint online boutique store
    3. Organize the Europe and Africa Industry system, to achieve production and sales in the world without borders
    4. Organize the global investment system, to achieve investment and profit globally without borders

Chapter VII. Five-Year Plan of SAT

Years	Events/Plans
2021	• The born of SAT • SAT on four digital currency exchange • SAT in online games • Over 20,000 wallet holder • Over 100 million value of transactions • The first year of SAT, focus on digital currency education • The value of the SAT around 0.001 to 0.01 cents
2022	• Joined to ATM Ecosystem • Over 100,000 wallet holder • SAT on more than eight main digital currency exchanges • Creating a decentralized digital currency exchange • The year of development, focus on related Ecosystem • The value of the SAT around 0.005 to 0.05 cents
2023	• Joined to Mobile phone system • Over 300,000 wallet holder • SAT works with mobile phones, ATMs, currency exchanges • The year of growing, focus on financial hardware Ecosystem • The value of the SAT around 0.01 to 0.1 cents
2024	• Build a digital city • Over 1 million wallet holder • Being a Bitcoin and all digital currencies' stablecoin • Makes 10 thousand transactions of entity products • The value of the SAT around 0.05 to 0.5 cents
2025	• Build the digital kingdom • Works with bank system let the SAT could use any time, everywhere • Expand the production of SAT mobile phones and ATMs • Over 2 million wallet holder • Makes 200 thousand transactions of entity products • SAT touch 1 dollar
2026~	It's a long journey SAT will keep growing and write its own history