Sound Money Coin: A Sound Money and Store of Value

Saifedeous von Mises
saifedous@soundmoneycoin.io
www.soundmoneycoin.io

Abstract. Government-controlled fiat money is the most devastating force in the Universe. By constantly printing money out of thin air, governments inflate the money supply which leads to high time preference in the population, world wars, Justin Bieber, the breeding of inexcusable aberrations like the Sphinx and Pekingese, and ultimately the demise of mankind. The decentralized finance ecosystem that is emerging on the Ethereum blockchain offers the potential to solve this problem but lacks a trustless reserve currency. Sound Money Coin is a sound money and a secure store of value. Its monetary policy is encoded into an Ethereum smart contract and therefore fundamentally immutable. If Bitcoin is gold, then Sound Money Coin is Dwarven lodenstone hardened for 1,000 years in the flames of Mordor.

1. Introduction

Several cryptocurrencies, most notably Bitcoin (BTC), claim to be a sound money. However, in Bitcoin, the inflation rate is indirectly determined by the block reward which is specified in the code of the Bitcoin node software. As per the Bitcoin whitepaper [1], the block reward is halved every 210,000 blocks. This leads some to claim that Bitcoin is to be considered "sound money" because presumably no more than 21,000,000 BTC can ever be generated.

The elephant in the room is that Bitcoin's issuance policy is mutable and could be changed by social consensus in the future: All it takes is some influential figureheads manipulating the Bitcoin memeplex to manipulate users into installing an upgrade.

If there is widespread consensus amongst a large number of developers, users and miners that the issuance policy should be changed, then the issuance rate *will* be changed. This may not happen in the near future. But what if in 10, 30 or even 100 years, it turns out that block rewards are too low to keep the Bitcoin blockchain secure? There goes your 21,000,000 max supply, here comes raving inflation. Professor Ammous calls this the *easy money trap:* anything used as a store of value will have its supply increased, and anything whose supply can be easily increased will destroy the wealth of those who used it as a store of value [2].

Thus, as much as the Bitcoin community may claim it, Bitcoin is NOT a sound money. For something to be a sound money its monetary policy must not be subject to any form of governance. What's needed is an eternally immutable monetary policy that is immune against social consensus. Sound Money achieves this property as its emission rate and max cap are encoded into an Ethereum smart contract. There is no way to change or update the code of the smart contract, ever. Thus, code is law and the danger of governance, by whatever group, is eliminated.

2. Immutability

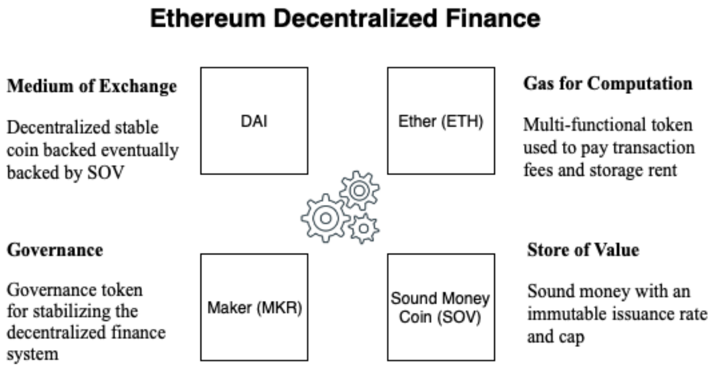
Sound Money Coin is defined as:

The ERC20 token at address 0x010589b7c33034b802f7dba2c88cc9cec0f46673 on the Ethereum main net.

It not possible to "fork" Sound Money Coin: If, say, Craig Wright were to deploy another smart contract at a different contract address, then that is *something else than Sound Money Coin by definition*. Sound Money Coin will always be Sound Money Coin in the same way that the moon will always be the moon. In Bitcoin however, both block rewards and hard cap can be changed via Nakamoto consensus. Thus, Sound Money Coin is harder currency than Bitcoin.

2. Role in Decentralized Finance

Decentralized finance lacks a reliable store of value. Ethereum's native currency Ether functions as gas paid for computation. This causes a hideous dilemma: If ETH price increases too much, using the Ethereum blockchain becomes prohibitively expensive. The missing piece is a digital asset that functions as a store of value for the decentralized finance infrastructure.


Ethereum Decentralized Finance
Medium of Exchange
Decentralized stable coin backed eventually backed by SOV
DAI
Ether (ETH)
Gas for Computation
Multi-functional token used to pay transaction fees and storage rent
Governance
Governance token for stabilizing the decentralized finance system
Maker (MKR)
Sound Money Coin (SOV)
Store of Value
Sound money with an immutable issuance rate and cap

Sound Money Coin decouples the store of value use case from Ether. It can function as a reliable "reserve currency" that is not influenced by monetary policy of the Ethereum developer team, who has shown to make frequent changes to block rewards and other key factors in an ad-hoc fashion.

3. Mining

The rules are simple: 0.05 SOV can be minted once per Ethereum block by calling the mint function in the Sound Money Coin smart contract. Minting SOV is free except for the Ethereum transaction fee. To add the property of scarcity, we propose setting a max cap on the total amount ever to be minted.

Converting to Solidity code...

```
uint256 constant public MINING_REWARD = 5000000;
uint256 constant public DEV_FUND = 100000;
uint256 constant public MAX_SUPPLY = 2100000000000000;

function mint() public {

     uint256 blockNumber = block.number;
     require(blockNumber > lastMinedAt);
     require(totalSupply() < MAX_SUPPLY);

     lastMinedAt = blockNumber;

          _mint(msg.sender, MINING_REWARD);
          _mint(treasury, DEV_FUND);
       }
```

Minting is not resource intensive but the cost of production manifests itself in gas fees. If there are competing transactions, Ethereum miners will be more likely to prioritize the transaction with the highest gas price (however, it depends on the algorithm that determines the order of transactions in blocks). If user A calls the mint function with as gas price of 2 Gwei and user B sets gas price to 4 Gwei, user A's transaction will likely end up in the block after user B's transaction and user B will receive the coins. Economically, the cost of minting 1 Sound Money Coin is given by the total gas fees effort and effort spent of all users competing for that coin.

At the same time, the transaction fees paid by all minters goes to the miner who added the Ethereum block to the blockchain (or, in proof-of-stake, to the node who generated the block). The miner therefore earns ETH amount equal to the value of the SOV minted. This somewhat disincentivizes miners from cheating, as they are already earning the high gas fees paid by minters. However, it is still possible, and even desired behavior, for miners to cheat eventually to take load off the Ethereum network (see below).

3. Danger of Clogging the Ethereum Network

As Sound Money Coin rises in fiat value an increasing number of actors will attempt to mint new coins. Currently, the Ethereum network only supports 15 transactions per second. Consequently, if minting SOV becomes too popular, Ethereum blocks could be soon be completely filled with SOV minting transactions.

In practice however this is unlikely to happen: Spamming transactions with a low gas price will always fail due to some minters using optimal strategies. Transactions are often sorted by gas price by default, but there are also other things that influence the order. If, say, the address somehow plays a role in sorting, a minter may get an advantage by minting only from sscertain addresses (e.g. those that start with "0x00"). A minter could also try to outsmart others by monitoring the mempool and trying to optimize the gas price and moment at which the transaction is broadcast. The gas price minters are willing to pay is another factor. It is expected that over time, only the most sophisticated minters, who are also willing to pay a high gas price, will compete for new SOV. An equilibrium should emerge between cost of minting SOV and price at which it trades on the market.

If it turns out that Sound Money Coin mining transactions *do* clog the network, there is a simple solution: Large Ethereum mining pools could announce to intentionally insert their own SOV minting transactions first in every block they mine. From that point on, transactions by regular users are bound to fail and incentives to spam the network vanish. Sound Money Coin generated this way could then be distributed to miners as a secondary block reward.

4. Inflation Rate

Sound Money Coin's monetary policy is intentionally simple: 0.05 SOV are generated with each minting transaction. The rate of generating SOV Coin is tied to the rate of Ethereum block generation. This is similar to the constant emission rate used by Grin [3].

Assuming that Ethereum block times stay constant, the first four years of Sound Money Coin emission rate are identical to the first four years of Bitcoin emission. Yearly inflation will tend towards zero over time.

```
- Year 1: 100%
- Year 5: 20%
- Year 10: 10%
- Year 15: 6.7%
- Year 20: 5%
- Year 25: 4%
- Year 30: 3.3
```

5. Conclusion

SOV Coin is the apex predator of value. Over time, it will become the world’s reserve currency. By 2035, once the Ethereum blockchain has become be the basis of the world’s financial infrastructure, SOV Coin will assume the role of a global reserve currency.

It’ll be commonplace for banks and governments to buy SOV Coin reserves. Eventually however even the world’s most backwards central banks will grudgingly buy SOV Coin. Soon after, we will see the end of wars, the-emergence of beautiful science and art, and the crafting of spaceships that fly us to the furthest corners of the Universe.

References

[1] S. Nakamoto, "Bitcoin Whitepaper", https://bitcoin.org/bitcoin.pdf, 2008

[2] S. Ammous, "The Bitcoin Standard: The Decentralized Alternative to Central Banking", Wiley, 2018

[3] https://github.com/mimblewimble/docs/wiki/Monetary-Policy