Memecoin: A Peer-to-Peer Meme Cash System

Satoshi Nakamemo
$MEMECOIN

Abstract. A purely peer-to-peer version of developer trust would allow holders to buy a memecoin without fearing that its creator will sell. Locks and vesting schedules provide part of the solution, but the main benefits are lost if a date, a third party or a contract still decides when the developer may sell. We propose a solution to the selling-developer problem using the oldest proof in crypto: a wallet that does not move. The developer holds 5% of the supply in a single public wallet and never moves it. The network timestamps that wallet in every block, forming an ever-growing record that cannot be changed without everyone seeing it. The longest record not only serves as proof of the commitment, but proof that it came from the developer's own choice, as it did for Satoshi. As long as the wallet does not move, the record keeps growing, and it outpaces any promise. The system itself requires minimal structure. Holders can check the wallet at will, leave and come back, accepting the longest record as proof of what happened while they were gone.

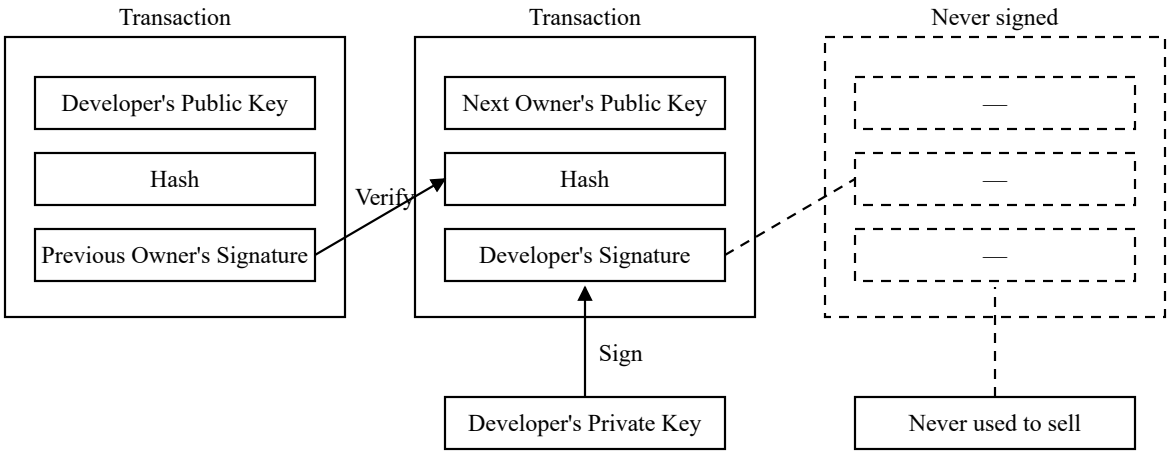
1. Introduction

Commerce in memecoins has come to rely almost exclusively on developers serving as trusted third parties. While the system works well enough for most launches, it still suffers from the inherent weaknesses of the trust-based model. A developer who holds supply can sell it at any moment, and buyers have no way to know when. With the possibility of a sale, the need for trust spreads. Holders must be wary of the developer, watching the developer's wallet and pricing in a risk that never goes away.

What is needed is a commitment based on public proof instead of trust, allowing any holder to check the developer without asking anyone. There is a precedent. In 2009 the creator of Bitcoin mined the first blocks alone and accumulated, by one well-known estimate, around one million coins [2], roughly 5% of the 21 million that will ever exist. His coins were never locked. He simply never moved them. In this paper, we propose to follow the same rule: the developer of $MEMECOIN holds 5% of the supply in one public wallet and never moves it, recorded by the network for anyone to verify.

2. Transactions

We define a memecoin as a chain of digital signatures. Each owner transfers the coin to the next by digitally signing a transfer to the public key of the next owner. A holder can verify the signatures to verify the chain of ownership.

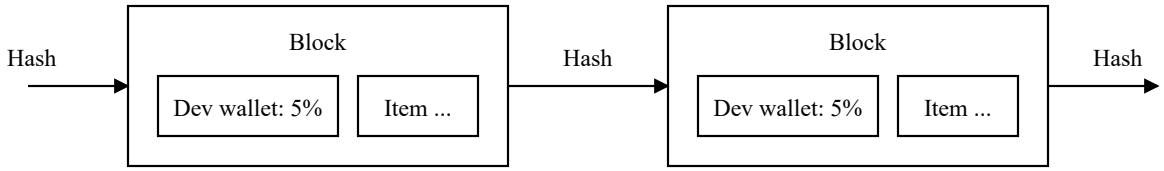


The problem, of course, is that the holder cannot verify that one particular owner, the developer, will not sign a transfer to the market tomorrow. A common solution is to introduce a trusted arrangement: a promise, a vesting service, or a lock that expires on a date. The problem with these solutions is that the fate of every holder depends on the arrangement, and most arrangements end.

We need a way for holders to know that the developer has not sold. For our purposes, the earliest record is the one that counts, so we do not care about promises of future behaviour. The only way to confirm the absence of a sale is to be aware of all transfers out of the developer's wallet. To accomplish this without a trusted party, the developer's wallet must be publicly announced, and we need a system for holders to agree on a single history of what that wallet did. Solana already provides that history.

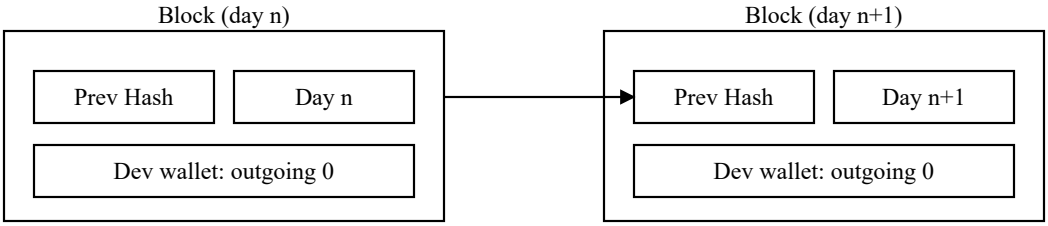
3. Timestamp Server

The solution we propose begins with a timestamp server. The network takes a hash of a block of items to be timestamped and widely publishes the hash. The timestamp proves that the data must have existed at the time. Each block includes the previous hash, forming a chain, with each additional block reinforcing the ones before it. Every block therefore records the balance of the developer's wallet at that moment.



4. Proof-of-Holding

To implement the commitment on a peer-to-peer basis, Bitcoin uses proof-of-work, which makes its history expensive to rewrite. $MEMECOIN relies on a simpler property of the same idea: a public chain cannot be rewritten without everyone seeing it. Once a block has recorded the developer's wallet as unmoved, that record cannot be changed. As later blocks are chained after it, the work to change it would include redoing all the blocks after it.



We call the result Proof-of-Holding. A lock proves that a developer cannot sell until a date. Proof-of-Holding proves that the developer has not sold, every day, with no end date. It is not a guarantee about the future, and we do not present it as one. It is a record that grows with every block, and the longer it grows, the more it is worth to the developer to keep it growing.

5. Network

The steps to run the network are as follows:

1. The token is created on pump.fun on Solana, with a fixed supply of 1,000,000,000.
2. The developer's wallet address, holding 5% of the supply, is broadcast to all holders.
3. The official pair is announced: $MEMECOIN against Bitcoin on Solana (cbBTC).
4. Each holder can check the developer's wallet in any block.
5. Holders accept the commitment only if the wallet shows no outgoing transfer.
6. Holders express their acceptance by holding, and keep checking in the next block.

Holders always consider the longest record to be the correct one and keep working on extending it. If the wallet ever moved, every holder would see the same transfer in the same block, and the record would end there for everyone.

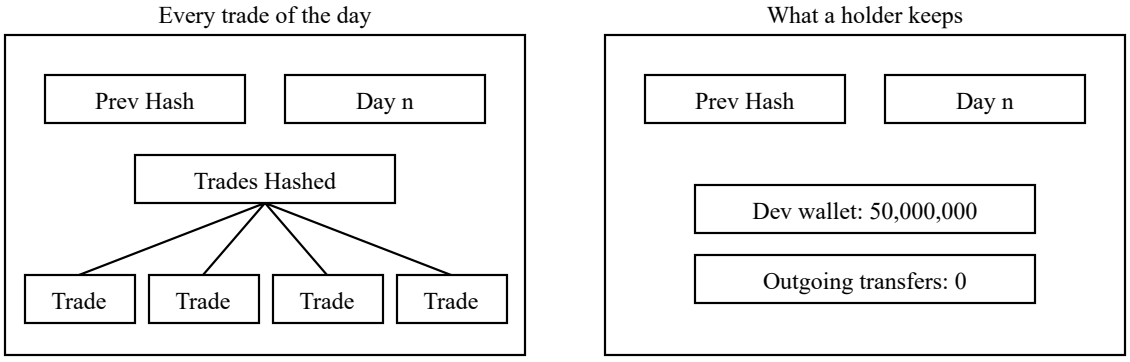
6. Incentive

By convention, a developer's incentive is to sell the developer's bag. In Bitcoin, the first transaction in a block rewards the node that creates it, which gives nodes an incentive to support the network. In $MEMECOIN, the developer's reward is the record itself: the wallet becomes part of the story the longer it stays still, as Satoshi's did.

The incentive may also help encourage the developer to stay honest. A developer who could sell 5% ought to find it more valuable to play by the rule than to break it in public, where every holder would see it and the record could never be restored.

7. Reclaiming Disk Space

Once the latest transaction in a coin is buried under enough blocks, the spent transactions before it can be discarded to save disk space. The same applies to a holder's attention. A memecoin can produce a great many trades a day, and none of them need to be followed to verify the commitment. Everything a holder needs reduces to two numbers about one wallet: its balance and its count of outgoing transfers.

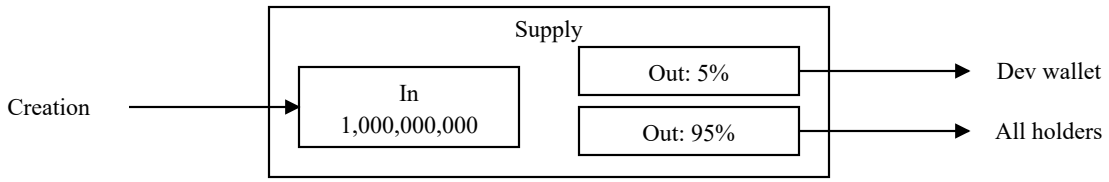


8. Simplified Holding Verification

It is possible to verify the commitment without running a full network node. A holder only needs a block explorer and the published address of the developer's wallet. Two checks are enough: the wallet still holds 50,000,000 $MEMECOIN, and its history shows no outgoing transfer of the token. If both hold, the holder has verified the commitment as well as anyone could. As such, the verification is reliable as long as the explorer reflects the network, and holders who want more certainty can check several explorers or run their own node.

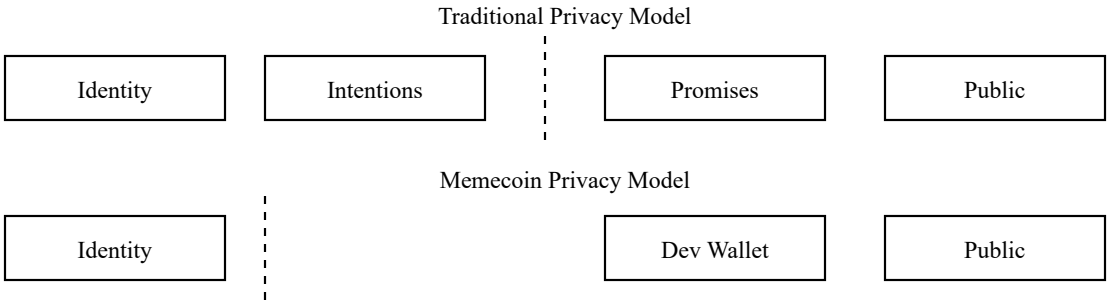
9. Combining and Splitting Value

Although it would be possible to spread the developer's allocation across many wallets, that would make it unwieldy to verify. To keep the commitment checkable in one look, the developer's 5% is held in a single wallet and is not split. The supply itself is fixed at creation and divides as follows:



10. Privacy

The traditional model achieves a level of privacy by keeping the developer's identity public and the developer's intentions private. We do the opposite. Privacy is maintained by keeping the developer anonymous, as Satoshi was, while the developer's wallet is completely public. The public can see that 5% sits still, but without information linking the wallet to anyone. This is similar to the level of information released by stock exchanges, where the time and size of trades are made public, but without telling who the parties were. The mascot, a hooded figure with no face, is drawn from this model.



11. Calculations

We compare the developer allocation of $MEMECOIN with the one it is modelled on. Bitcoin's supply is capped at 21,000,000 coins; the supply of $MEMECOIN is fixed at 1,000,000,000. Satoshi never published his addresses, so his share can only be estimated [2].

```
#include <stdio.h>

int main()
{
    double satoshi  = 1000000.0  / 21000000.0;    /* estimate [2] */
    double memecoin = 50000000.0 / 1000000000.0;  /* exact        */

    printf("Satoshi   %.1f%%\n", satoshi  * 100.0);
    printf("Memecoin  %.1f%%\n", memecoin * 100.0);
    return 0;
}
```

Running the program, we get:

```
Satoshi   4.8%
Memecoin  5.0%
```

The second figure is exact, because the developer's wallet is published. In that respect $MEMECOIN is easier to verify than the original.

12. Conclusion

We have proposed a system for developer commitment without relying on trust. We started with the usual framework of a memecoin, which provides strong ownership through signatures but is incomplete without a way to know whether the developer will sell. To solve this, we chose the rule Satoshi followed: one public wallet holding 5%, never moved, recorded by every block and checkable by anyone. Holders work all at once with little coordination. They do not need to be identified, and they can leave and rejoin at will, accepting the longest record as proof of what happened while they were gone. Satoshi never sold. Neither will we, and you can watch.

References

[1] S. Nakamoto, "Bitcoin: A Peer-to-Peer Electronic Cash System," https://bitcoin.org/bitcoin.pdf, 2008.

[2] S. D. Lerner, "The Well Deserved Fortune of Satoshi Nakamoto, Bitcoin creator, Visionary and Genius," https://bitslog.com/2013/04/17/the-well-deserved-fortune-of-satoshi-nakamoto/, 2013.

$MEMECOIN is a memecoin with no intrinsic value. The developer's commitment not to move the 5% is public, not a technical lock. It is not affiliated with Satoshi Nakamoto or the Bitcoin project. Nothing in this paper is financial advice.