MimbleWimbleCoin White Paper

Good Money for the Information Age

MWC Fact Sheet

- Total Supply: 20,000,000.
- Proof of Work Consensus Algorithm: C31.
- Source Code: Open source.
- Base layer: Mimblewimble.
- Every transaction uses CoinJoin and Confidential Transactions.

MWC Team's Mission

What does good digital money look like? Good money in the Information Age is scarce, censorship resistant, extensible, durable, indestructible, salable, portable, fungible, private and divisible. Good money.

The mission of the MWC developer team is to match and exceed every other good in the market with regard to these ten monetary characteristics in order to produce a good that is the superior qualitative money.

In order to most effectively harness the power of human action, all aspects of the MWC monetary product from creation to distribution and development will hold as the primary purpose or aim to establish greater monetary sovereignty for the buyers and holders in the least costly and most profitable way.

Summary

Bitcoin set the standard of what digital money could be, but, unfortunately lacks a few of the key characteristics of good money. Released seven years after Bitcoin, MimbleWimble technology was created to solve these privacy and fungibility deficiencies while also providing greater network scalability.

All MWC transactions on the base layer use Greg Maxwell's CoinJoin with his Confidential Transactions and signature aggregation. Therefore, all transactions keep all data about the sender, receiver and amount private and each MWC is fungible because it does not have a unique transaction history recorded on a public ledger like legacy blockchain technology does.

In the 2018 paper titled Aggregate Cash System: A Cryptographic Investigation of Mimblewimble, Fuchsbauer, et. al. concluded, "In this paper, we provide a provable-security analysis for Mimblewimble. We give a precise syntax and formal security definitions for an abstraction of Mimblewimble that we call an aggregate cash system. We then formally prove the security of Mimblewimble in this definitional framework. Our results imply in particular that two natural instantiations (with Pedersen commitments and Schnorr or BLS signatures) are provably secure against inflation and coin theft under standard assumptions."

The MWC development team seeks to innovate both technologically and economically in order to bring out all of the MimbleWimble protocol benefits. The MWC team has already created a fully functional GUI wallet, developed a method for secure offline cold storage of MWC, completed a MWC/BTC atomic swap on testnet and is investigating multi-sig transactions and Lightning Network.

There are many potential places development resources can be allocated. They will be chosen based on market needs. Highest priority will be given to requests that primarily benefit and come from the buyers and holders of last resort.
While the MWC Team will carefully consider all opinions; they realize the most important arbiter of success for this monetary product will be the aggregated decisions of the market as found in the orderbook.

The MWC network was launched in November 2019 and has functioned flawlessly with 100% uptime. The MWC Team considers the protocol ossified and currently sees no need for a future hard or soft fork unless a defensive action were required to protect the network.

Mimblewimble: Disruptive Innovation
On July 19th, 2016 the pseudonymous “Tom Elvis Jedusor” rocked the Bitcoin developer community by releasing the “MimbleWimble” white paper which proposed a blockchain architecture with several significant advantages over Bitcoin.

Andrew Poelstra's 2016 San Fran BitDevs presentation on Mimblewimble sent shockwaves through the Bitcoin developer community. Mimblewimble provides an approximate 3x scalability improvement over legacy blockchain technology plus other benefits. Unfortunately, incorporating Mimblewimble into Bitcoin would be a difficult and invasive task as it may require a hard fork. Alternatively, it may be incorporated into Bitcoin as a sidechain or extension blocks.

Three main properties of MWC transactions increase their privacy. All transactions on the base layer are CoinJoined with Confidential Transactions and signature aggregation. Consequently, there are no addresses, transaction amounts or intermediary inputs and outputs in blocks and all transactions are indistinguishable from one another. Unless you are a transaction participant then all inputs and outputs look like random pieces of data on the blockchain.

In 2016 Bitcoin Core developer Peter Wuille said,

> Introducing Mimblewimble into Bitcoin in a backwards-compatible way would be a difficult exercise. It may not be impossible, but it would be hard. I think the way if people were experimenting with this, I would expect it to be an experimental separate chain or sidechain. In a sidechain we would not introduce a new crypto-currency but it would be a separate chain. There are some downsides to Mimblewimble. In particular, it does not have a scripting language...a scripting language is very neat to play with, but it has a privacy downside. Mimblewimble takes this to the other side where you have very good privacy but at the expense of no other features any more.

Fortunately, there has been significant research done since then and with Mimblewimble these types of smart contracts and applications are possible: Multi-Signature transactions, time locks, atomic swaps, and hashed time-locked contracts which are the building block of payment channels and Lightning Network.

MWC: Alpha Stage

The MWC project was announced in February 2019 with an airdrop to Bitcoin holders. Registration took place between April 20, 2019 and July 19, 2019. More than 148,000 BTC registered in thousands of addresses with a value greater than $1.2B. The MWC airdrop was one of the most anticipated and largest airdrops ever.

MWC mainnet launched in November 2019. In the genesis block, 10,000,000 MWC were created to establish the initial stock.

Immediately, developers received 2,000,000 MWC in exchange for their pre-alpha stage efforts from February to November 2019.

In December 2019 MWC, about 5,400,000 of 6,000,000 MWC were distributed to airdrop recipients. This method was chosen to result in having a highly sophisticated self-selected user base with significant financial resources.

Affirmative action was required to claim and there was a deadline strictly imposed. Consequently, a large base of highly sophisticated, economically incentivized and financially powerful holders could be quickly amassed without large inflationary costs incurred by buyers like with Bitcoin, and, unlike Bitcoin Cash and other forks there would be no significant supply overhang from initially uninterested or hostile parties. The airdrop recipients freely received a hedge against Mimblewimble technology.

The creation of the initial stock did not necessarily create any material value. Like with gold, Bitcoin and every other financially substantive asset, the market capitalization would need to be attained through the market process of buyers and sellers. The airdrop distribution began on December 2, 2019 with a total value of less than $1.35m at about $0.00-0.25 per MWC.

There was anticipation that some airdrop recipients would sell their freely received MWC. Trading data from Hotbit, the sole exchange listing MWC, from December to February showed millions of MWC of volume with wildly fluctuating prices.

MWC: Beta Stage

In early April 2020, MWC went through a phase transition with the successful deployment of a hard fork. This resulted in two major changes: (1) a proof of work change so that around November 2020 MWC would solely use the C31 algorithm and (2) an emission rate change.

In order to reduce the store of value costs for holders, a week after the hard fork the block reward was reduced by 75% and continues to rapidly harden. The stock-to-flow ratio will be greater than 60 in February 2021 and more than 100 in February 2022.

The MWC HODL Program is a financial innovation designed as a security feature and to further lesson the economic costs of buyers and holders. There are 2,000,000 MWC in a verifiable escrow wallet allocated for the HODL program.

The primary purpose of the HODL Program is to act as a very important check and balance on the possibility of a hidden inflation bug being abused. This would manifest itself as more MWC being registered than are supposed to exist under the consensus rules.

For example, if someone were able to find and abuse a hidden inflation bug and then attempt to financially profit by selling on an exchange then it is likely that, eventually, a buyer would withdraw the coins and register them in the HODL Program. Because the GRIN supply is created solely through mining, therefore, it is not possible to check for hidden inflation using this type of economic incentive.

MWC: Future Stages

The MWC monetary product is in an experimental stage and will remain so until at least the unclaimed airdrop funds and HODL Program have been completed and the initial stock is fully distributed. Consequently, MWC is experimental and risky.

The MWC Team considers the protocol ossified and currently sees no need for a future hard or soft fork unless a defensive action were required to protect the network. As an open source project it has been found that there are many developers interested in and contributing towards making MWC more usable.

As the MWC network continues performing flawlessly according to the consensus rules the market may generate more trust and confidence in MWC's ability to help them solve problems they face. Month by month and year by year the orderbook will be the arbiter of opinions.

Contact

Email: info@mwc.mw
Twitter: @M_W_Coin