MimbleWimbleCoin White Paper

Good Money for the Information Age

MWC Fact Sheet

- Supply Cap: 20.0 million.
- Source Code: Open source.
- Base layer: Mimblewimble.
- Every transaction uses CoinJoin and Confidential Transactions.
- Proof of Work Algorithm: Cuckoo Cycle Proof of Work.
- MWC forked from the Grin code base.
- HODL program – MWC wallets with zero negative balance movements overstipulated time periods receive MWC. Further details forthcoming.

Lifetime Distribution

- 50% - 10,000,000 MWC - Proof of Work mined.
- 50% - 10,000,000 MWC - Created in the genesis block.
- 7,400,037.409531322 MWC have been distributed and are circulating.
- 2,599,962.590468680 MWC are currently held in verifiable escrow wallets.
- 2,000,000 MWC for the HODL program.
- 599,962.590468680 MWC unclaimed from the airdrop program.

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.

MWC Team's Mission

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.

Summary

Bitcoin set the standard of what digital money could be, but, unfortunately lacks a few of the key characteristics of good money. MimbleWimble technology, released 7 years after Bitcoin was, was created to solve these privacy and fungibility deficiencies while also providing better network scalability.

All MWC transactions on the base layer use Greg Maxwell's Coin Join 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."

Disruptive Innovation

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.

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.

MWC transactions and block format transactions can be merged when an output is directly spent by the input of another and this can happen without being broadcast to the

network. It is as if when Alice sends MWC to Bob and then Bob sends MWC to Carol then Bob was never involved and his transaction is actually never seen on the blockchain. All these features and yet the whole blockchain can be stored, downloaded and fully verified in just a few gigabytes or less.

The MWC development team seeks to innovate and bring out all of the MimbleWimble protocol benefits. The 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 working on multi-sig transactions and Lightning Network.
GRIN miners can easily point the grin-miner binary to a MWC full node and it just works. The only difference needed is to run a MWC full node instead of a GRIN full node. Note that usually, if miners use a Nvidia 1080Ti or 2080Ti or a 8GB GPU then they may want to learn how to set the miner to C31 for significantly more profitability.

Mimblewimble
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:

No addresses. Impossible for an observer who is not a participant in a transaction to determine a sender, receiver or amounts. Increased privacy and fungibility.

Transactions combined such that, in contrast to Bitcoin, the entire history of all transactions is not required to validate transactions. Increased scalability.
MimbleWimble does not allow the full Bitcoin scripting language. However, this "drawback" has been largely mitigated through cryptographic technology advancements. Multi-signature, atomic swaps, time locks, and Lightning Network are all possible on a MimbleWimble-based blockchain.

Shortly after the pseudonymous MimbleWimble white paper was released, Blockstream mathematician Andrew Poelstra took interest in the paper, and wrote his own modified version. Since then, the crypto development community has had time to digest these papers, and it is now widely understood that MimbleWimble has significant long-term potential.

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.
According to Bitcoin core developer Peter Wuille, "Introducing MimbleWimble into Bitcoin in a backwards-compatible way would be a difficult exercise. It may not be impossible, but it would be hard. Unlike Bitcoin, MimbleWimble does not have a scripting language – which is neat to play with, but has a privacy downside. MimbleWimble, (conversely), has very good privacy at the expense of no other features."

Given that Bitcoin cannot easily incorporate MimbleWimble, there have been multiple proposals for alternative blockchains utilizing MimbleWimble – most notably, the Grin and Beam. While these are interesting projects, the stock-to-flow ratios of both are too low. Grin has infinite supply and S2F of about 1.08 and the corporate coin Beam has a lifetime supply cap of 263 million and S2F of about 2.1.

The MWC team considers the store-of-value standpoint extremely important and therefore with many potential places to allocate development resources they will be chosen based on market needs with highest priority given to requests that will primarily benefit and come from the buyers and hodlers of last resort.

In addition to a fixed, limited supply, MWC seeks to optimize the potential return for holders by using the targeted airdrop model to reward proactive Bitcoin holders, via a process similar to Stellar, Bitcoin Rhodium, Bitcore and several other projects. In the initial airdrop to Bitcoin holders, about 5.4m of 6m coins were claimed. The 600,000 unclaimed coins have been moved to verifiable escrow wallets and will be either burned, added to the HODL Program or distributed in future airdrop(s).

The MWC HODL Program rewards MWC holders who, during stipulated periods of time, have zero negative movements from their MWC wallets. There are two million coins in a verifiable escrow wallet allocated for the HODL program.

Contact

Email: info@mwc.mw
Twitter: @M_W_Coin