MimbleWimbleCoin (MWC) White Paper - Jan 31st, 2019

Summary:

On July 19th, 2016 the pseudonymous "Tom Elvis Jedusor" rocked the Bitcoin developer community by releasing the "MimbleWimble" white paper [1]. This paper proposed a blockchain with several advantages over Bitcoin:

1. No addresses, so it is impossible for an observer who is not a participant in a transaction to determine who is sending and receiving coins

2. Transaction amounts encrypted, so it is impossible for an observer who is not a participant in a transaction to determine the amounts being transacted

3. Transactions combined such that, in contrast to Bitcoin, the entire history of all transactions is not required to validate transactions

The long and the short of it is, these features provide potential fixes to Bitcoin's greatest problems: scalability, privacy, and fungibility.

MimbleWimble doesn't allow the full Bitcoin scripting language, but this "drawback" has been largely mitigated through cryptographic technology advancements. To wit, multi-signature, atomic swaps, time locks, and Lightning Network are all possible on a MimbleWimble-based blockchain. [3]

Shortly after the pseudonymous MimbleWimble white paper was released, Blockstream mathematician Andrew Polestra took interest in the paper - and wrote up his own modified version of the white paper [2]. Since then, the development community has had time to digest these papers...and it is now widely understood that there are a lot of great concepts in MimbleWimble. Unfortunately, these changes cannot easily be implemented into Bitcoin in a backwards compatible way because MimbleWimble is too different.

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 recently launched Grin [4] and Beam [5] chains. While these are interesting projects, Grin has infinite supply; whilst Beam is a corporate coin, with a lifetime supply cap of 263 million. We consider these features fatal flaws from a store-of-value standpoint – and thus, introduce “MimbleWimbleCoin,” or MWC.

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 Bitcoin Rhodium’s [6]. In this model, any Bitcoin holder who can prove ownership, via the registration of public, non-zero balance BTC keys, is eligible for the airdrop. Moreover, the MWC HODLing Program rewards holders who, during stipulated periods of time, have zero negative movements from their MWC wallets.

We believe the airdrop distribution method - of a MimbleWimbleCoin with a low, fixed lifetime cap and in-kind dividend; will give Bitcoin holders, and those who acquire MWC in the secondary market, the potential to be a superior store of value to Grin and Beam. Moreover, given MimbleWimble’s technological potential, we believe MWC has amongst the highest upside potential in the crypto universe.

The airdrop registration will begin April 20, 2019, and end on the snapshot date of July 19, 2019; i.e., three years from the day the original MimbleWimble white paper was disseminated. Further details will be made available when available.

MWC Fact Sheet:

- Airdrop registration begins: April 20, 2019
- Airdrop registration ends / Snapshot date: July 19, 2019
- Supply Cap: 20.0 million
- POW Algorithm: Cuckoo Cycle POW
- Pre-Mine: 2.0 million MWC (50% Public Relations/Marketing, 50% Development)

- Each Bitcoin UTXO can register for the Airdrop, with the exact ratio of MWC/BTC determined by the amount of Bitcoin UTXO's registered – so that ultimately, exactly 6.0 million MWC, or 30% of the lifetime supply, are distributed.
- MWC will be forked from the Grin code base, with modifications to the supply function and stipulations for the airdrop.
- MWC HODL program (details forthcoming) – an in-kind crypto-dividend rewarding MWC wallets with zero negative balance movements over TBD stipulated periods of time
- Source code: Open source
- How to Participate: Details regarding air drop registration will be forthcoming.

Lifetime Distribution:

50% POW Mining	10.0 million MWC
30% Airdrop	6.0 million MWC
10% Development and PR	2.0 million MWC
10% MWC HODL program	2.0 million MWC

Sources:

1 - https://download.wpsoftware.net/bitcoin/wizardry/mimblewimble.txt

2 - https://download.wpsoftware.net/bitcoin/wizardry/mimblewimble.pdf

3 - https://github.com/mimblewimble/grin/blob/master/doc/grin4bitcoiners.md

4 - https://grin-tech.org/

5 - https://www.beam.mw/

6 - https://www.bitcoinrh.org/

MimbleWimbleCoin (MWC) White Paper - Jan 31st, 2019

mwc.mw