Bitcoin Zero

Yushi Zhao

November 14, 2017

1 Introduction

In short, Bitcoin Zero is designed to bring zk-SNARK (Zero-Knowledge Succinct Non-Interactive Argument of Knowledge) back to Bitcoin. The journey of 'zero' started from zerocoin (Miers et al., 2013) a cryptographic extension to Bitcoin including utilizing non-interactive zero-knowledge proofs; Then, zerocash (Sasson et al., 2014) formulated and constructed decentralized anonymous payment schemes. After a few technical modification `https://github.com/zcash/zips/raw/master/protocol/protocol.pdf`, Zcash as an implementation of zerocash has finally been available for general use. Now that zk-SNARK is widely accepted, Ethereum for example, users of Bitcoin may want to enjoy the same protection too. So, here comes the Bitcoin Zero. To achieve such a goal, addition to zk-SNARK, I intended to implement a chainstate snapshot and a merged mining PoW, which will be explained later. Here I want to convey my respect to all the good work mentioned before. As a gesture, I will honor the founder reward of Zcash in Bitcoin Zero.

2 zk-SNARK

The zk-SNARK implemented in Bitcoin Zero is the same as that implemented in Zcash 1.0.12. So, here I spare myself repeating the explanation. Well personally, I am willing to discuss zk-SNARK with anyone who is also interested. I also want to recommend this series of articles written by Ariel Gabizon as a good start: `https://z.cash/blog/snark-explain.html`.

3 Chainstate Snapshot

One way to bring zk-SNARK to Bitcoin is to fork at certain height. That should allow Bitcoin Zero to create new blocks with new protocol when maintaining the whole Bitcoin transaction history in block files. A drawback I see in this scheme is the size of block files, which is over 100 GB. Note that only the chainstate, namely, the UTXO set is needed to start a new transaction, as people can spend their money according to the balance in their account without

the history of all transactions. So here is the idea. Given a Bitcoin chainstate at certain height, we aggregate the amount in different UTXO associate to the same address (scriptPubKey) as the balance of that address; We then filter out addresses with a balance lower than 1460 satoshi for such addresses can barely afford the transaction fee and usually contains irregular information with a relatively large size. Currently, the size of Bitcoin chainstate in leveldb is about 0.5 GB after the aggregation and filter. To use that Bitcoin chainstate snapshot in Bitcoin Zero, I created a transaction in the genesis block of Bitcoin Zero to reflect the balance of addresses and nothing else. Once we load that genesis block, Bitcoin Zero will have a chainstate equivalent to the Bitcoin chainstate at certain height. As to that height, I chose 478558 for the following reasons: This height has a lot of audience due to the BCC fork; After the BCC fork, there is a debate which one should be followed; Enough PoW has been done since then. Therefore, people should be able to agree on what is in that chainstate and what is not and everyone will be able to validate the snapshot as well as the genesis block of Bitcoin Zero. As a result, Bitcoin users will have the same balance in Bitcoin Zero as they had in Bitcoin at 478558 without 100 GB block files. The total amount of BTZ (Bitcoin Zero) in the genesis block is 16481813.80550197.

4 Merged Mining PoW

Let Bitcoin Zero use the same PoW as Bitcoin is not a good idea because it simply distract the hash power if Bitcoin Zero does not get no hash power at all. Hash power is essential to keep the blockchain safe. Fluctuations of hash power is also dangerous. Because transactions validated at height n and confirmed during the low hash power period may be overrode during the high hash power period when extra hash power decide to mine another chain starting at height n. This kind of fluctuations are introduced into both Bitcoin and Bitcoin Cash as a tug of war for hash power. Bitcoin Zero wants to avoid that. Actually, a brilliant solution has already been implemented in Namecoin for long, namely, merged mining PoW. Bitcoin Zero is going to follow the tradition stated at `https://en.bitcoin.it/wiki/Merged_mining_specification`. Notice that Bitcoin Zero will only require a Bitcoin-like block, that means it can be a Bitcoin Cash block as well. Moreover, in Bitcoin Zero, the coinbase transaction will be scanned for merged mining signature without unserialization to enhance compatibility. Merged Mining PoW will be the only valid PoW in the Bitcoin Zero main net. This will ensure no hash power distraction and all the hash power attracted by Bitcoin Zero will contribute to the whole network.

5 Parameter Specification

Bitcoin Zero integrate various protocols of which parameter definitions are overlapping. For clarification, this section discusses some parameters Bitcoin Zero use.

5.1 Address prefix

- PUBKEY_ADDRESS = 1;
- SCRIPT_ADDRESS = 3;
- ZCPAYMENT_ADDRRESS = z;

Addresses will remain the same for Bitcoin users. Notice that founder reward addresses will appear to be different from Zcash, but the underlying script will be the same.

5.2 Block size

- $BlockSize = 2\text{MB}$;
- $BlockSigOps = 20000$;
- $TargetBlockInterval = 2.5 * 60\text{s}$;

This set of parameter is set to be the same as Zcash. Notice that 2MB per 2.5 minutes is about 8MB per 10 minutes as in Bitcoin Cash.

5.3 Mining subsidy

- $InitialSubsidy = 50/4$;
- $PresetHeight = 4 * 478558$;
- $SubsidyHalvingInterval = 4 * 210000$;
- $NextSubsidyHalving = -478558 * 4 + 3 * SubsidyHalvingInterval$;

I am trying to make the new mining subsidy match the history reflected in the snapshot. The key factor is the block interval ratio, in other words, Bitcoin Zero generate 4 new blocks while Bitcoin generate 1 new block. As a result, the height of the snapshot is actually 4*478558 in Bitcoin Zero; After the genesis, the first block to mine will have 3.125 BTZ (Bitcoin Zero) before giving out founder rewards. Founder rewards will be the same as Zcash, which is 20% and ended at next subsidy halving.

5.4 DefaultPort and ChainID

- $DefaultPort = 8083$;
- $ChainID = 0$;

These two should not clash with other chains'. Please notify me if you find a clash.

6 Further Discussion

`https://github.com/bitcoinzero` will be used as the homepage of Bitcoin Zero. You are welcomed to discuss all related topics there. Here are some topics you may find interesting.

6.1 Merged mining slot ID

As stated in merged mining specification, currently the method determining a slot ID is practical and yet flawed. I am looking for an alternative.

6.2 Segregated witness

Segwit is an important improvement of Bitcoin that Zcash do not have. However, implementing segwit in Bitcoin Zero is beyond my scope. As stated on `https://github.com/zcash/zcash/issues/2593`, Zcash is trying to fix the transaction malleability in a different way. This is probably going to be a more practical way for Bitcoin Zero too. But concerns about other benefits segwit brings remains. Further discussions are needed. If Bitcoin Zero draws enough attention, implementing segwit will be back on the table.

7 Conclusion

Bitcoin Zero is a practise of my study of blockchain. Through Bitcoin Zero, I hope the idea of zero-knowledge proof will be known to more people in the field of cryptocurrency; I hope the chainstate snapshot and merged mining PoW will provide solutions to problems all altcoins meet. The test net will be started soon. According to the feedback, the main net will be scheduled. Please visit `https://github.com/bitcoinzero` for updates.

References

Miers, I., C. Garman, M. Green, and A. D. Rubin (2013). Zerocoin: Anonymous distributed e-cash from bitcoin. *IEEE Symposium on Security & Privacy*, 397–411.

Sasson, E. B., A. Chiesa, C. Garman, M. Green, I. Miers, E. Tromer, and M. Virza (2014). Zerocash: Decentralized anonymous payments from bitcoin. pp. 459–474.