June 16, 2018 (rev 0.1)

BEAM

The Scalable Confidential Cryptocurrency

What is BEAM?

BEAM is a next generation confidential cryptocurrency based on an elegant and innovative MimbleWimble protocol.

Things that make BEAM special include:

- Users have complete control over privacy - user decides which information will be available and to which parties, having complete control over his personal data in accordance to his will and applicable laws.
- Confidentiality without penalty - in BEAM confidential transactions do not cause bloating of the blockchain, avoiding excessive computational overhead or penalty on performance or scalability while completely concealing the transaction value.
- No trusted setup required
- Blocks are mined using Equihash Proof-of-Work algorithm
- Limited emission using periodic halving with total amount of coins ~210 million[1]
- No addresses stored in the blockchain - no information whatsoever about the either sender or a receiver of a transaction is stored in the blockchain.
- Superior scalability through compact blockchain size - using cut-through feature of MimbleWimble BEAM blockchain is orders of magnitude smaller than any other blockchain implementation.[2]
- BEAM supports many transaction types such as escrow transactions, time locked transactions atomic swaps and more.
- No premine. No ICO. Backed by a treasury, emitted from every block during the first five years.
- Implemented from scratch in C++ by a team of professional developers.

---

[1] Exact coin schedule is not finalized yet and will be published at a later date

[2] See more detailed explanation on MimbleWimble below to understand how this can be achieved without compromising blockchain security.

Introduction

Since Bitcoin, the first implementation of the idea of peer to peer electronic cash system proposed by Satoshi Nakamoto back in 2008 [1], the field of crypto currencies and blockchain based systems has exploded producing thousands of different projects, technologies and research papers. Today one can find such projects ranging from distributed computing to Enterprise solutions and applied to all fields from medicine to automotive industries.

However, the basic need for people to store their money and transact in a secure way without relying on a centralized authority is still the main use case and the most important, which is one of the reasons why Bitcoin is still the top cryptocurrency and is as influential today as it was almost ten years ago.

In Bitcoin, as in most crypto currencies since, your balance is represented by a series of transactions which can be traced back to the very beginning of a blockchain. In order to prove the validity of the system we need to make sure that each transaction in a chain is valid, and to do so without relying on a centralized entity, which is the main purpose of Bitcoin nodes and miners. All participants in the system must agree, or using more professional terms "reach consensus", on an official version of the transaction history and be able to do so without trusting each other or anyone else. The ability of the system to do so is the true strength of the Bitcoin idea.

Failure of Anonymity and The Need for Confidentiality

Initially, transactions in the Bitcoin network were believed to be anonymous. By generating random private and public key pairs, and using the public part to form an address that could be used to receive and control transactions, many Bitcoin users assumed that nothing in that process could link to their real identity.

They turned out to be wrong. Using blockchain analysis, research has shown that there are always data leaks [2]. These can come from exchanges, merchants, OTC deals or even by collecting and clustering the blockchain data. It is then possible to deanonymize users, and since all data, including transaction amounts, is open and permanently stored in a public ledger, once users identity is known all their transactions past and future as well as their balance, become directly linked to them as a person.

This situation is far from ideal. Both individuals and organizations would prefer that their transactions and balance remain confidential and could only be seen only by parties specifically authorized by them to do so. This would require limiting the visibility of transaction details, including transferred amounts and identities of the participants and keeping as little information as possible about the transactions in the public record to prevent future analysis and a potential disclosure.

Introducing MimbleWimble

In August 2016 a new protocol was published by an anonymous author, suggesting an elegant approach to the topic of efficient confidential blockchain. It is called MimbleWimble[3], a reference to a spell from Harry Potter books, and it builds upon two concepts originally proposed by Greg Maxwell, namely Confidential Transactions [3] and Transaction Cut - Through [4]. The following is a high level explanation of the key principles of MimbleWimble. For more detailed explanation please read the original whitepaper [5].

Confidential transactions are implemented by using cryptographic commitment scheme which has two basic properties: hiding and binding. It is similar to giving someone a closed safe box with some message inside that only you know the combination for. When time comes you can reveal the key and the person can make sure that your commitment is valid (binding) while he can not know what is was before the key is received (hiding)

MimbleWimble utilizes a well known commitment scheme called Pedersen Commitment that achieves this using Elliptic Curve Cryptography and is of the form

$$C = r * G + v * H$$

Where *r* is a blinding factor, a secret key hiding the real value *v* and G and H are generator point on a specific elliptic curve.

[3] Read full whitepaper here: https://download.wpsoftware.net/bitcoin/wizardry/mimblewimble.txt

Each input and output of a transaction is thus a linear combination of two factors: an actual value of the transaction and a blinding factor. In order to transfer ownership of a UTXO (Unspent Transaction Output) a sender needs to reveal its value and blinding factor to the receiver, which in turn needs to create a new output commitment using a different blinding factor, known only to him. Due to the linearity property of Pedersen Commitments, if we have two identical transactions: from A to B, and then from B to C, we can cut through the intermediate transaction, resulting in a merged transaction from A to C, which is a valid transaction in the system.

Since block is just a list of transactions, each with its list of inputs and outputs, a block can be seen as one large transaction as well, allowing us to “cut through” i.e merge all intermediate outputs both within a single block as well as across multiple blocks in the blockchain. Extending this approach to the entire chain, we get a system that only needs to store the current UTXO state, instead of entire transaction history. Validity of the history that brought us to this state can be confirmed by storing only the headers of the previous blocks which hold the proof of validity of previous states (using a structure called a Merkle tree) and Proof of Work that allows to reach consensus on which of the header chains should be considered the correct one (in case of blockchain branching).

Since all that is needed to prove ownership of the UTXO is the value and the unique blinding factor, there is no need to store any addresses in the blockchain. After creating the transaction between two wallets, either online or using any other secure mechanism, only the commitment

is recorded in the blockchain. This means that no matter the resources of the attacker, no personal information can be extracted from the blockchain.

In addition to Inputs, Outputs, Proofs and fees, each MimbleWimble transaction includes, the transaction kernel, which in its most basic form contains the difference between blinding factors of sender and receiver. Each transaction should also contain a non interactive zero knowledge range proof to ensure that transaction value is positive without revealing the actual value. It is important since allowing the user to create transactions with negative value would result in ability to arbitrarily create new coins which should be prohibited by the system. For this purpose we use Bulletproofs [6], a compact and highly computation efficient implementation of zero knowledge range proofs that are attached to every transaction and checked by the system during transaction validation.

Q&A:

Question: Why is BEAM using Equihash mining?

Answer: Equihash PoW mining algorithm is well adopted by miners globally. Equihash is based on solving a Generalized Birthday Problem. It is IO bound, meaning that it requires quite a large amount of memory as opposed to Bitcoin's SHA256 that requires a lot of processing power. Equihash is built in a way that does not allow easy tradeoff between processing power and memory thus making it difficult to use with ASIC miners that existed at the time of its creation. Today there are dedicated ASIC miners that can mine Equihash ten times more efficiently than average CPU.

Question: How does compact blockchain work? Is data actually deleted from the blockchain?

Answer: No data is ever deleted from the blockchain, since a blockchain is append only by definition. What a compact blockchain means is that information needed to validate the entire blockchain is much smaller than the complete list of transactions. The user wallet, a new node connected to the system, or an existing one that does not want to store all the information can only download block headers and current state to verify the entire blockchain.

Question: What is the performance of BEAM in terms of number of transactions per second?

Answer: We do not have exact numbers yet. However it is safe to say that it will be slightly better than bitcoin and existing privacy coins. Having said that it is important to emphasize that the performance will not be high enough for BEAM to be used as “means of exchange”. Which is why we believe that BEAM will be primarily used as “store of value”. In the future it might be

possible to improve performance using second layer out of chain solutions such as Lightning network or Thunderella.

Question: Does BEAM have a UI Wallet?

Answer: Yes, at launch BEAM will release a desktop wallet application for Mac, Windows and Linux.

Please submit additional questions to our Community group on Telegram:

@BeamPrivacy | https://t.me/BeamPrivacy

References:

[1] https://bitcoin.org/bitcoin.pdf

[2] https://arxiv.org/abs/1708.04748

[3] https://people.xiph.org/~greg/confidential_values.txt

[4] https://bitcointalk.org/index.php?topic=281848.0

[5] https://download.wpsoftware.net/bitcoin/wizardry/mimblewimble.txt

[6] https://eprint.iacr.org/2017/1066.pdf