

Claims

1. A computer-implemented method of resolving short transaction identifier collision in a blockchain network, comprising:
 - receiving block data from a sending node, including a block Merkle root and a set of short transaction identifiers from a sending node;
 - for each short transaction identifier, locating a corresponding full transaction identifier in a mempool;
 - calculating a Merkle tree based on the full transaction identifiers, the Merkle tree having a Merkle root;
 - determining that the calculated Merkle root does not match the block Merkle root;
 - sending, to the sending node, Merkle tree hashes from an intermediate layer of the Merkle tree;
 - receiving, from the sending node, resolution data identifying which of the Merkle tree hashes is incorrect; and
 - repeating the sending of Merkle tree hashes and receiving of resolution data until a collision is resolved.
2. The method of claim 1, wherein each short transaction identifier is a truncation of its corresponding full transaction identifier.
3. The method of claim 1 or claim 2, wherein the resolution data includes a flag for each of the Merkle tree hashes for the intermediate layer indicating whether that Merkle tree hash is valid.
4. The method of claim 1 or claim 2, wherein the resolution data includes full transaction

identifiers for a portion of a bottom layer of the Merkle tree.

5. The method of any one of claims 1 to 4, wherein the intermediate layer is a layer of the Merkle tree between an identified unmatched Merkle hash and a bottom layer of the Merkle tree.
6. The method of claim 5, further comprising selecting the intermediate layer.
7. The method of any one of claims 1 to 6, wherein the Merkle tree hashes include partial Merkle tree hashes.
8. The method of any one of claims 1 to 7, wherein receiving block data includes receiving, from the sending node, a pre-emptive set of Merkle tree hashes from a selected layer of the Merkle tree.
9. A computing device to resolve short transaction identifier collision in a blockchain network, the computing device including:
 - one or more processors;
 - memory;
 - computer-executable instructions stored in the memory that, when executed by the one or more processors, cause the processors to carry out the method claimed in any one of claims 1 to 8.
10. A computer-readable medium storing processor-executable instructions for resolving short transaction identifier collision in a blockchain network, the processor-executable instructions including instructions that, when executed by one or more processors, cause the processors to carry out the method claimed in any one of claims 1 to 8.