**Overview**

Born at the block height of 478,558, Bitcoin Cash (BCH) has been dedicated to bringing a reliable electronic cash to the world and fulfilling Satoshi’s original vision as a "peer-to-peer electronic cash." It enjoys global seamless circulation, permissionless innovation and other features. How to issue token on the Bitcoin Cash Blockchain? Many developers have brought up with ideas such as Colored-Coins. Andrew Stone proposed to add OP\_GROUP to implement the token scheme as he mentioned in *Enable representative tokens via OP\_GROUP on Bitcoin Cash*. The OP\_GROUP solution can only be implemented by changing consensus rules of Bitcoin Cash. More specifically, it enables functions similar to that of ERC20 token protocol on the Ethereum network.

Any proposals enabling token issuance that requires certain consensus upgrades will inevitably cause problems, including technical risks, harsh conflicts and huge controversy among community developers. Such controversial proposals often end up into a failure. This difficulty could help prevent “radical” initiatives being implemented to ensure the stability and security of the network protocol. However, it is harder to promote innovation. The controversy that led to the expansion of the independent block of the Bitcoin Cash community, the prolonged and unconstrained generation, is an even more unavoidable evidence of social psychology.

Innovation requires a PERMISSIONLESS community. We have also been exploring ways to implement smart contracts on Bitcoin Cash Blockchain without changing the consensus rules. After tremendous research efforts, we have noticed the Omni Layer protocol, a scheme to implement token issuance through the OP\_RETURN opcode. It is the technical basis for daily distribution and circulation of USDT. The Omni Layer runs on top of Bitcoin Blockchain. Since the Omni Layer protocol uses the MIT license (open source), we forked the Omni Layer protocol and implemented the tech features on Bitcoin Cash Blockchain to achieve token issuance. We named this technical solution Wormhole protocol, and the original token in the protocol is named Wormhole Cash.

**Security model and execution procedures**

**Wormhole node**

**Cognition of node**

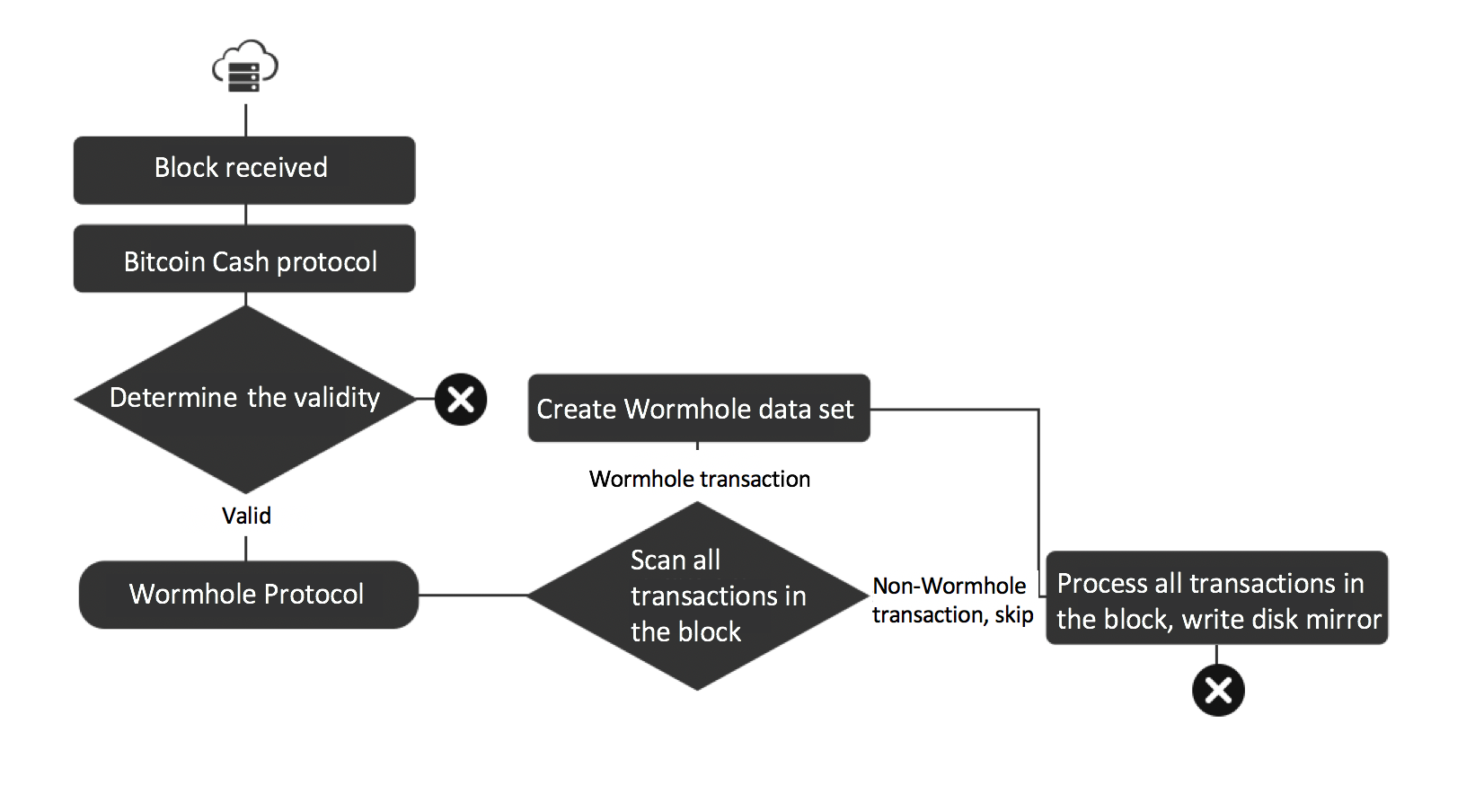
Wormhole node is a superset of Bitcoin Cash node, it is implemented by adding Wormhole protocol onto Bitcoin Cash’s client.

Wormhole client can be used as a Wormhole full node as well as a Bitcoin Cash full node, which enables both Bitcoin Cash protocol and Wormhole protocol.

Transaction received by Wormhole node

* It can receive and verify Wormhole transactions, as well as receiving and verify ing Bitcoin Cash transactions.

**Execution of node**



After the Wormhole node is launched, it will communicate with other nodes in the network (including: Bitcoin Cash node),receive blocks and transaction messages. When receiving a new block from the network, it will execute the following procedures:

* Firstly, use the Bitcoin Cash protocol to detect all transactions in the block in accordance with the protocol rules, continue to execute; or, discard the block;
* Next, use the Wormhole protocol to detect each transaction in the block, and use the Wormhole compliant transaction to build the Wormhole data set in the node;
* When all transactions in the block have been processed, the Wormhole data set of the current node will be mirrored and written to the disk file.

**Wormhole Transaction**

The Wormhole transaction essentially consists of a special Bitcoin Cash transaction that utilizes a special opcode: OP\_RETURN in the Bitcoin Cash script to append the Wormhole protocol to the opcode. Wormhole transaction has the following relationship with Bitcoin Cash transaction:

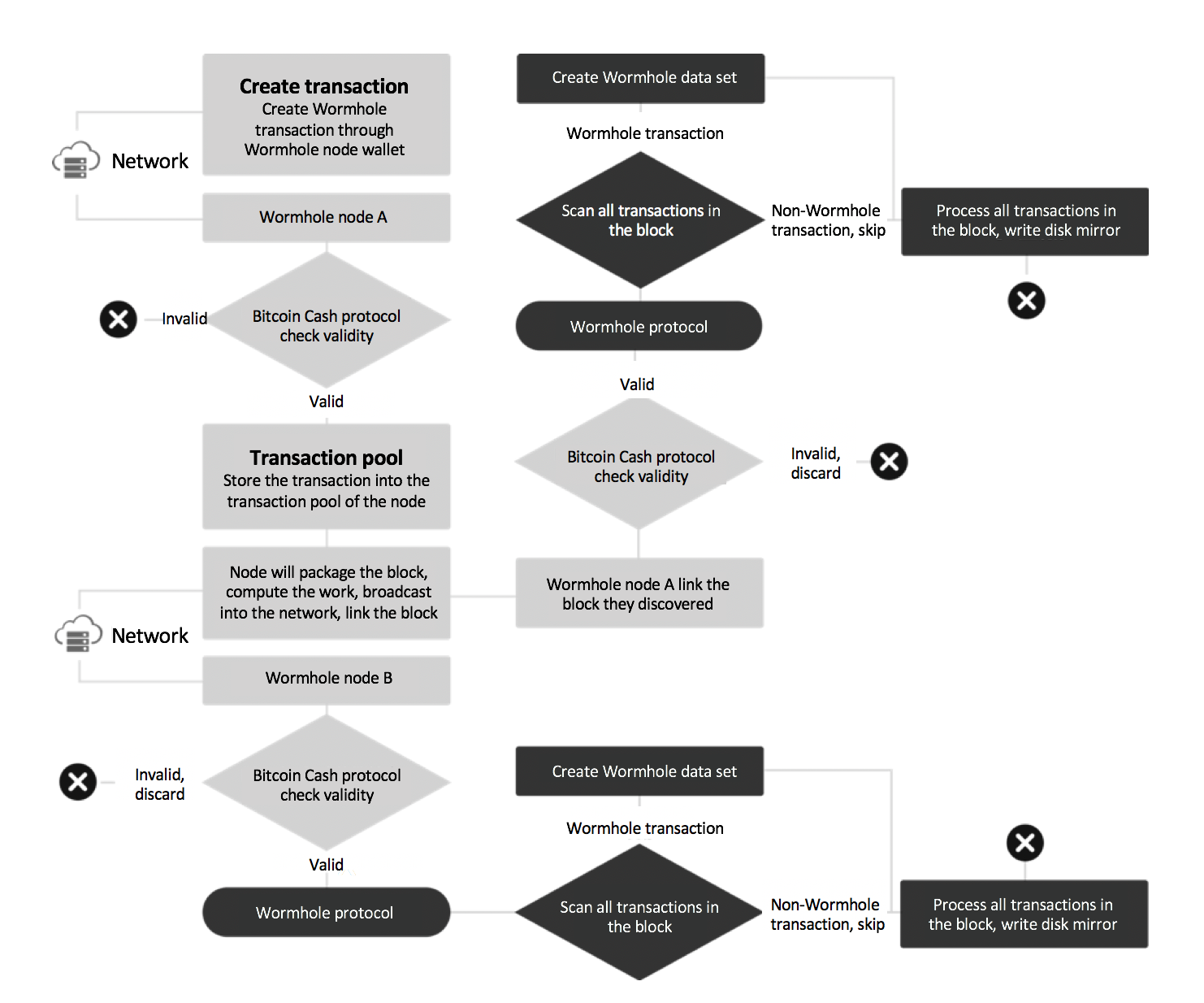
* Wormhole transaction is a subset of the Bitcoin Cash transaction

Wormhole transaction has two states in the blockchain, and transactions in both states are valid Bitcoin Cash transactions.

* Valid: Wormhole transaction meet the conditions of the transaction type;
* Invalid: Wormhole transaction does not meet the conditions of the transaction type;
* Conditions of the Wormhole transaction type can be found in: Wormhole-Spec

Based on the premises above: as long as the transaction is a valid Bitcoin Cash transaction, the Wormhole node will receive and package the verification, so there will be an invalid state of Wormhole transaction on the blockchain.

Example: When a Wormhole transaction is created, the process is as follows:



**Wormhole account and Bitcoin Cash address**

Wormhole protocol accepts account model, each Bitcoin Cash address is an account, and each account can hold different types of token.

**WHC basic currency**

The Wormhole system created a basic currency WHC, which will be used as a transaction medium for charging gas of smart contracts; for trading on a decentralized exchanges on-chain; and for the issuance of various tokens.

The source of the WHC in the system is generated by burning BCH; WHC is obtained by constructing a burning transaction according to a fixed ratio.

The requirements for a burning transaction are as follows:

* The first transaction output (index 0): must be the burning output, that is, sending BCH to the burn address, the amount must be >= 1 BCH.
* The second transaction output (index 1): Must be the payload data of the Wormhole transaction, labeling the transaction type as burning BCH receiving WHC.
* Note:

o Transferring directly to the burning address will not generate WHC, which will result in the loss of the BCH of the transfer;

o When the BCH amount transferred to the burning address is < 1 BCH, it does not generate WHC, and the BCH of the transfer will be lost;

The exchange ratio is as follows:

* 1 BCH = 100 WHC; 1 WHC = 100,000,000 C;

Burning address:

* Main network: bitcoincash:qqqqqqqqqqqqqqqqqqqqqqqqqqqqqu08dsyxz98whc
* Test Network: bchtest:qqqqqqqqqqqqqqqqqqqqqqqqqqqqdmwgvnjkt8whc
* Regression test network: bchreg:pqqqqqqqqqqqqqqqqqqqqqqqqqqqqp0kvc457r8whc

WHC maturity: After creating a burning transaction, the corresponding WHC will not immediately reach the sender's account, it requires a certain confirmation time (maturity), then the WHC will reach the sender's account.

Burning maturity:

* Main network: After 1000 blocks are confirmed, the corresponding WHC will reach the sender's account; in the subsequent block, the WHC will be allowed to spend or transfer the account.

o Example: At a block height of 500, a valid burning transaction (tx1) is confirmed, at which point the burning maturity is 1; at a block height of 1499, the combustion transaction (tx1) has been confirmed 1000 times. At this point, the burning maturity is 1000 and the WHC arrives at the sender's account. After the block height of 1499, the WHC obtained from this burning is allowed to be spent.

* Test Network: After 3 blocks are confirmed, the corresponding WHC will reach the sender's account.
* Regression test network: After 1 block is confirmed, the corresponding WHC will reach the sender's account.

**Procedures of processing blocks in a Wormhole node**

In the Wormhole nodes, each new block needs to be linked to the main chain when it is received, and two situations might occur:

* Append the received block to the end of the current main chain;

o When the node receives the new block (no chain rearrangement occurs), the node will check all transactions in the block for compliance with Bitcoin Cash protocol, blocks that do not comply with the Bitcoin Cash protocol rules will be discarded; afterwards, blocks that comply with Bitcoin Cash protocol will be checked according to Wormhole protocol. The block will check the transactions that comply with Wormhole protocol and verify the transactions, and updates the Wormhole data record of the Wormhole node. After all the transactions in the block are processed, The Wormhole data in the current system is written into the disk file as a mirror of the current block height.

* Blockchain rearrangement occurs after receiving a new block;

o When the node is in the chain rearrangement state, the Wormhole node deletes all the data after the rearrangement block height in memory, and then loading the disk mirror file of the forking block. If the loading is successful, the block of the new chain will be rescanned from the forking point, then building a Wormhole data set. Finally, when each block has been processed, the current system state will be written to disk as the mirror of current block height; if the mirror file fails to load, Wormhole system will delete all Wormhole data sets in memory, and starting from the block height at which the function is deployed, rescan all block data on the main chain to build a new Wormhole data set.

**Wormhole's security model**

Wormhole has two-layer protection security.

The first layer is the transaction security of Bitcoin Cash, Bitcoin Cash uses the POW mining algorithm as the decentralized timestamp server. The algorithm has been running stably for nearly 10 years. The UTXO model has the following advantages:

* UTXO requires no maintenance balance
* UTXO is an independent data logging unit that can accelerate verification of transactions
* UTXO model has nothing to do with events, it is only associated with locking/unlocking the scripts
* UTXO has high performance when processing transactions

The Wormhole protocol uses the UTXO security model of Bitcoin Cash, and Bitcoin Cash's decentralized timestamp server model.

The second layer of protection are the nodes who are running the Wormhole protocol. The data that does not comply with the Wormhole protocol will not be parsed by the nodes of the Wormhole protocol. Each node has the ability to calculate the nearest final legal state of the Wormhole by reparsing the transaction data.

**Future**

Wormhole’s roadmap: <https://github.com/copernet/spec/blob/master/whcwhitepaper.md#wormhole>

**Conclusion**

The lack of smart contracts has always been a major weakness of the public Blockchain based on the UTXO model. The Wormhole protocol can add the account model to achieve smart contracts in the case of fully reconfiguring the security and reliability of UTXO. It will provide more possibilities to Bitcoin Cash.