Privacy and Security - **Guaranteed**

Boolberry Solves CryptoNote Issues

Boolberry’s feature:

Improved transaction identification

In this presentation you’ll find out how **Boolberry reduces block chain bloat compared to *Ordinary CryptoNote coins.**

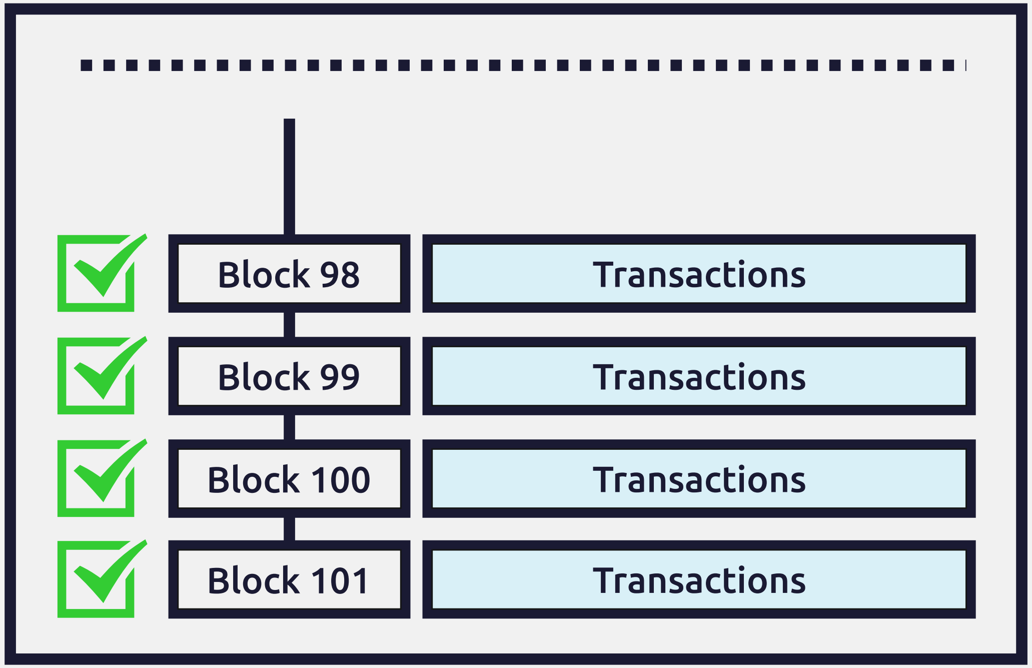
***Ordinary CryptoNote -** Coins based on the original CryptoNote core, such as **ByteCoin**, **DuckNote**, **Monero**, etc.

Block chain

What is a **block chain** and how does it work?

The block chain is a database shared by all network users that stores the transaction history. A transaction is not recognized until it is added to the block chain, which is referred to as confirmation.

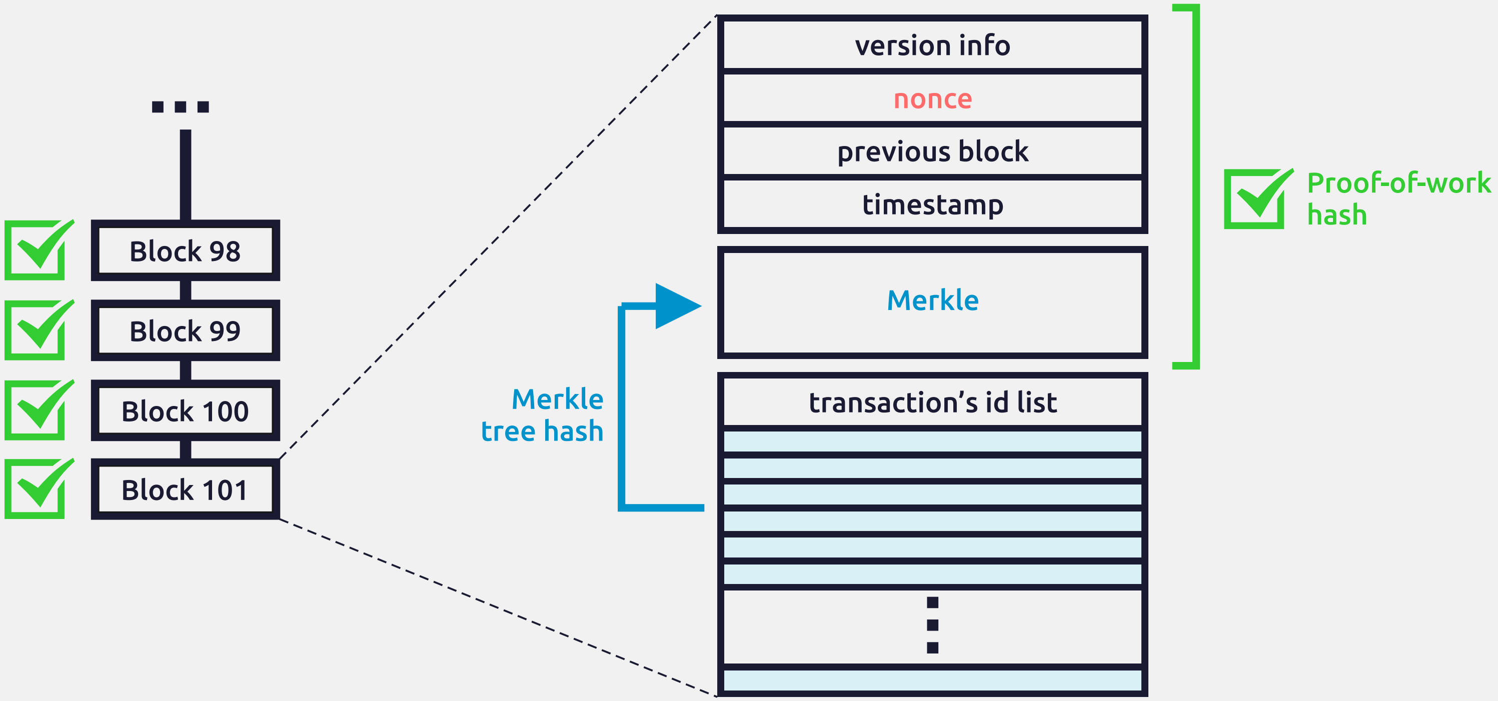
Blockchain



Block chain

What does a block look like?

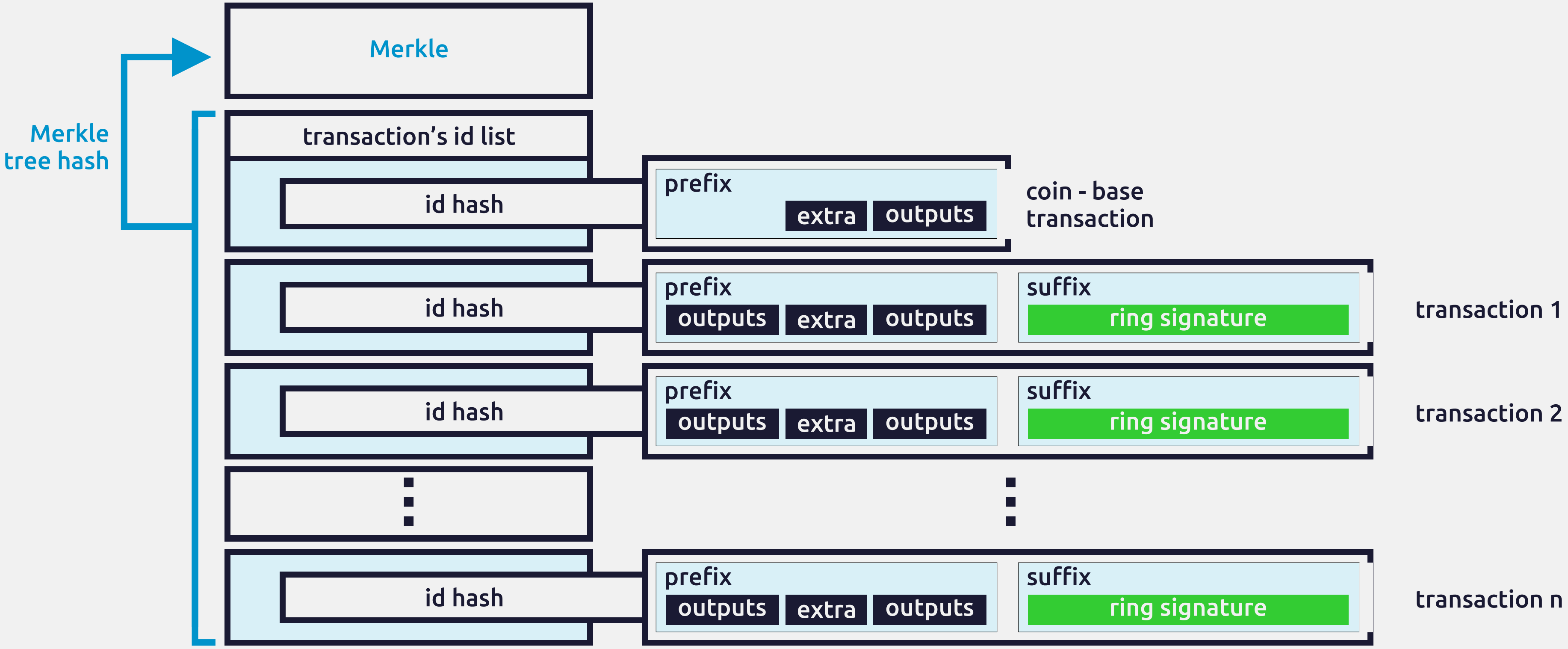
Simplified block structure:



Header - Contains service information (version info, nonce, previous block id and timestamp).
Merkle - A summary built from the block's transaction identifiers.
Transaction's id list - list of transaction's identification hashes, that was included into the block's merkle tree

Block chain

How do transaction get included into the block ?



A transaction gets included into block's transactions list by an identifier calculated from both the transaction prefix and suffix (ring signatures).

The Problem - Bloated Blockchains

Examination of the **Boolberry** block chain (28-Jul-2014) shows the average transaction size is 4065 bytes. Calculations show **ring signatures take up an average of 55%** of that size.

And these calculations are for a block chain where mixins are not widely used yet. When mixins are used ring signatures take up 60-90% of the transaction size.

Ordinary CryptoNote coins have to keep all the ring signatures, since it is **not possible to prove that a transaction belongs to a block** without them.

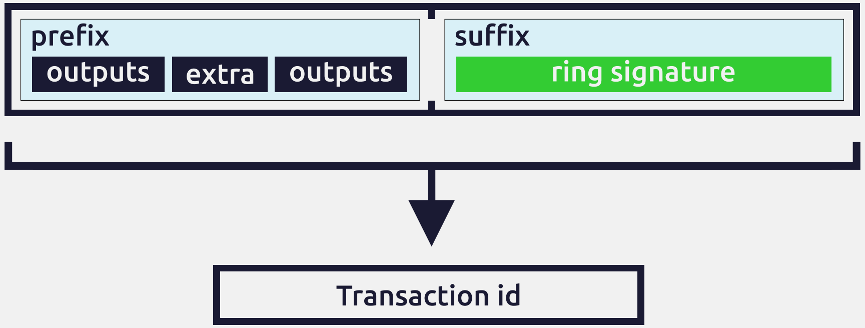
boolberry solution: Cut Off the Ring Signatures

Once a transaction gets a lot of confirmations (say one year old transaction with hundreds of thousands confirmations) the ring signature is no longer needed… even if transaction's output is not spent yet.

So why not just cut it off?

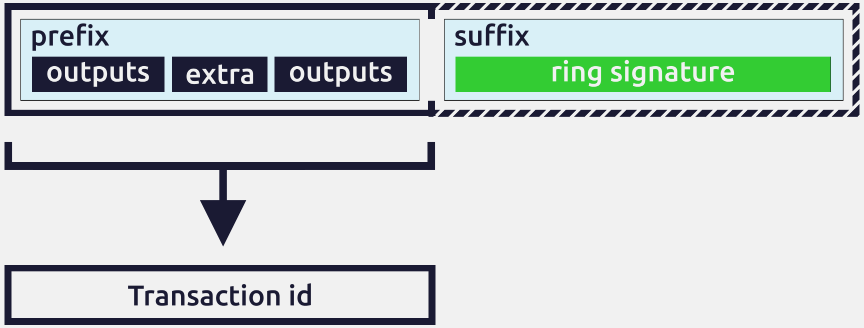
Let's compare!

Ordinary CryptoNote Coin



Ordinary CryptoNote calculates transaction id hash using all

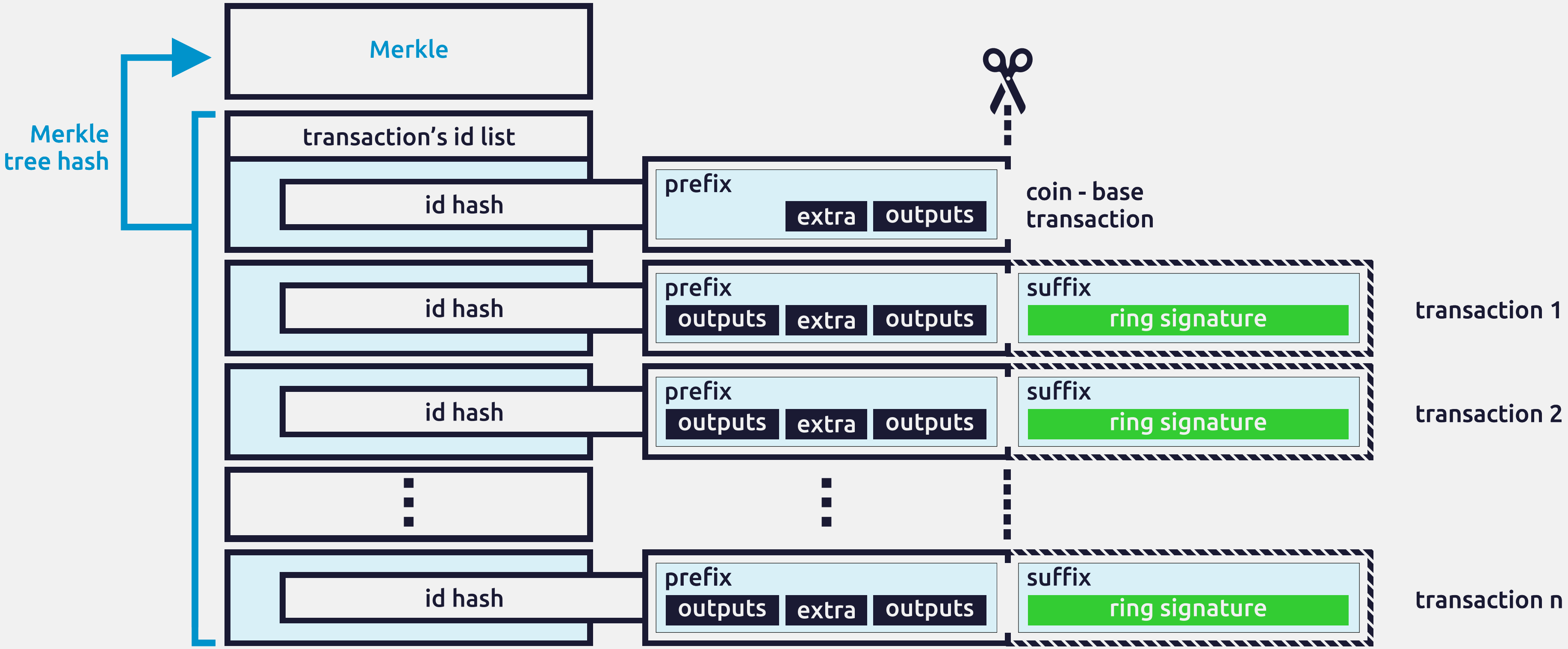
boolberry



Boolberry calculates transaction id hash using only the transaction prefix. Ring signatures are excluded from transaction id hash.

Block chain

How are transactions included in a Boolberry block?

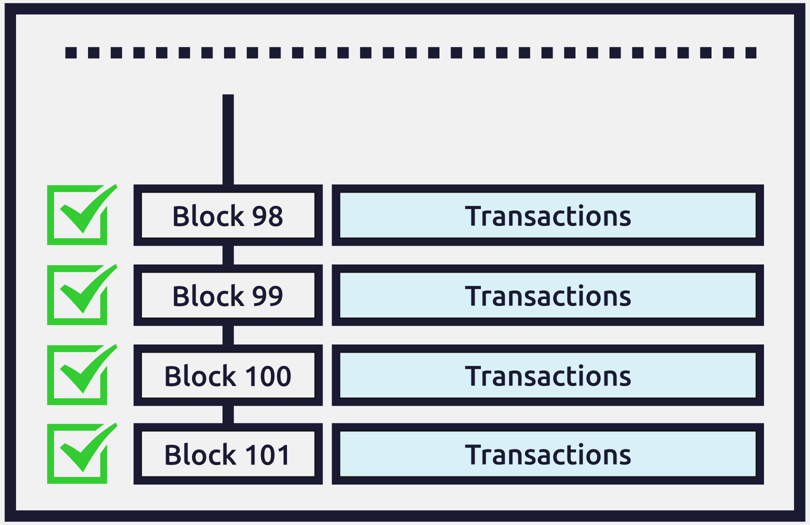


Each transaction included into block's transactions list by identifier calculated from transaction prefix only! This allows **Boolberry** to cut-off ring signatures from old transactions but still able to prove that transactions belong to given block and protected by Proof-of-Work of this block.

Block chain

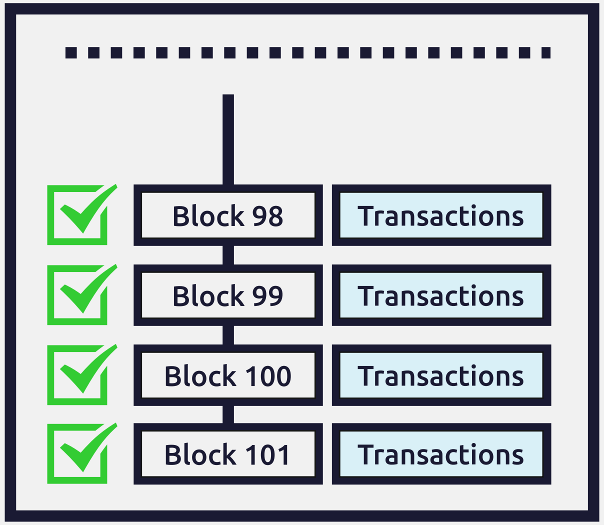
Let’s compare the Ordinary CryptoNote block chain
and the **Boolberry** block chain after one year:

Ordinary CryptoNote Coin



✓	Block 98	Transactions
✓	Block 99	Transactions
✓	Block 100	Transactions
✓	Block 101	Transactions

boolberry



✓	Block 98	Transactions
✓	Block 99	Transactions
✓	Block 100	Transactions
✓	Block 101	Transactions

Guess what?

Boolberry is designed to use resources more efficiently!

Boolberry **will to drop the ballast of ring signatures** for old transactions, even if transaction outputs is not spent yet. We'll start to cut off ring signatures after first year of currency live (we gonna do that at least with checkpoints, but also we gonna start public discussion to talk about other more interesting/smart ways to do that).

This feature will make Boolberry **Block Chain at least 55% and up to 90%** smaller than Ordinary CryptoNote coins.
Compact block chain produce faster synchronization for better user experience and convenience!

Guess what?

Boolberry is the most convenient modified CryptoNote coin to date!

Boolberry is trading on www.poloniex.com and www.bittrex.com

For more information please visit www.boolberry.com

Contact: press@boolberry.com