

Boolberry Solves CryptoNote Flaws

Boolberry's feature: Unlinkable Outputs

In this presentation you'll find out how anonymity works in ordinary CryptoNote technology and **Boolberry's** modified CryptoNote technology.

Let's compare!

Ordinary CryptoNote Technology

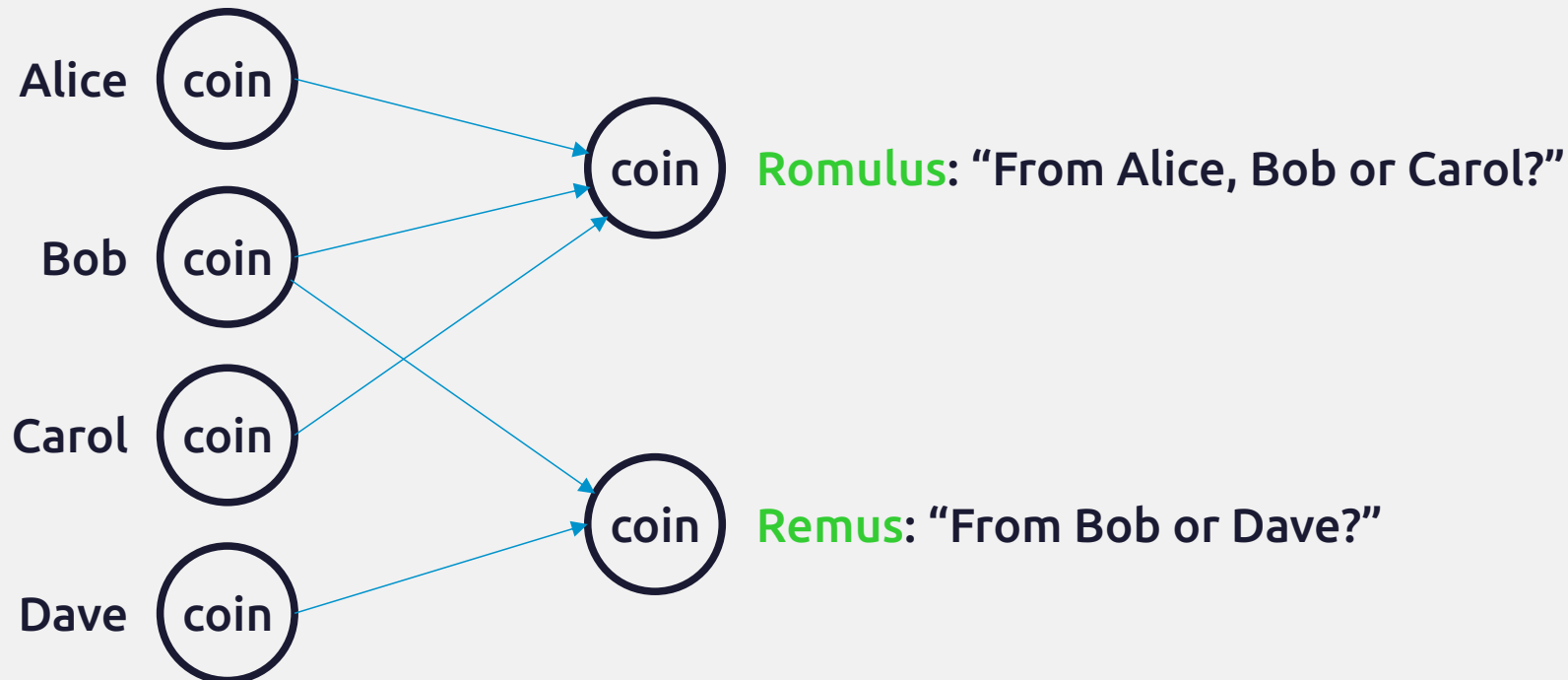
Alice wants to send a coin to **Romulus** and keep this transfer **private**.

To achieve this, she uses Bob's and Carol's coins as ***mixins**.

At the same time, **Dave** wants to send a coin to **Remus**, and also wants to keep the transfer **private**. To achieve this he took **Bob's** coin as a ***mixin**.

***mixin** - it's a part of Cryptonote technology that makes your transfer private.

Ordinary CryptoNote transfer

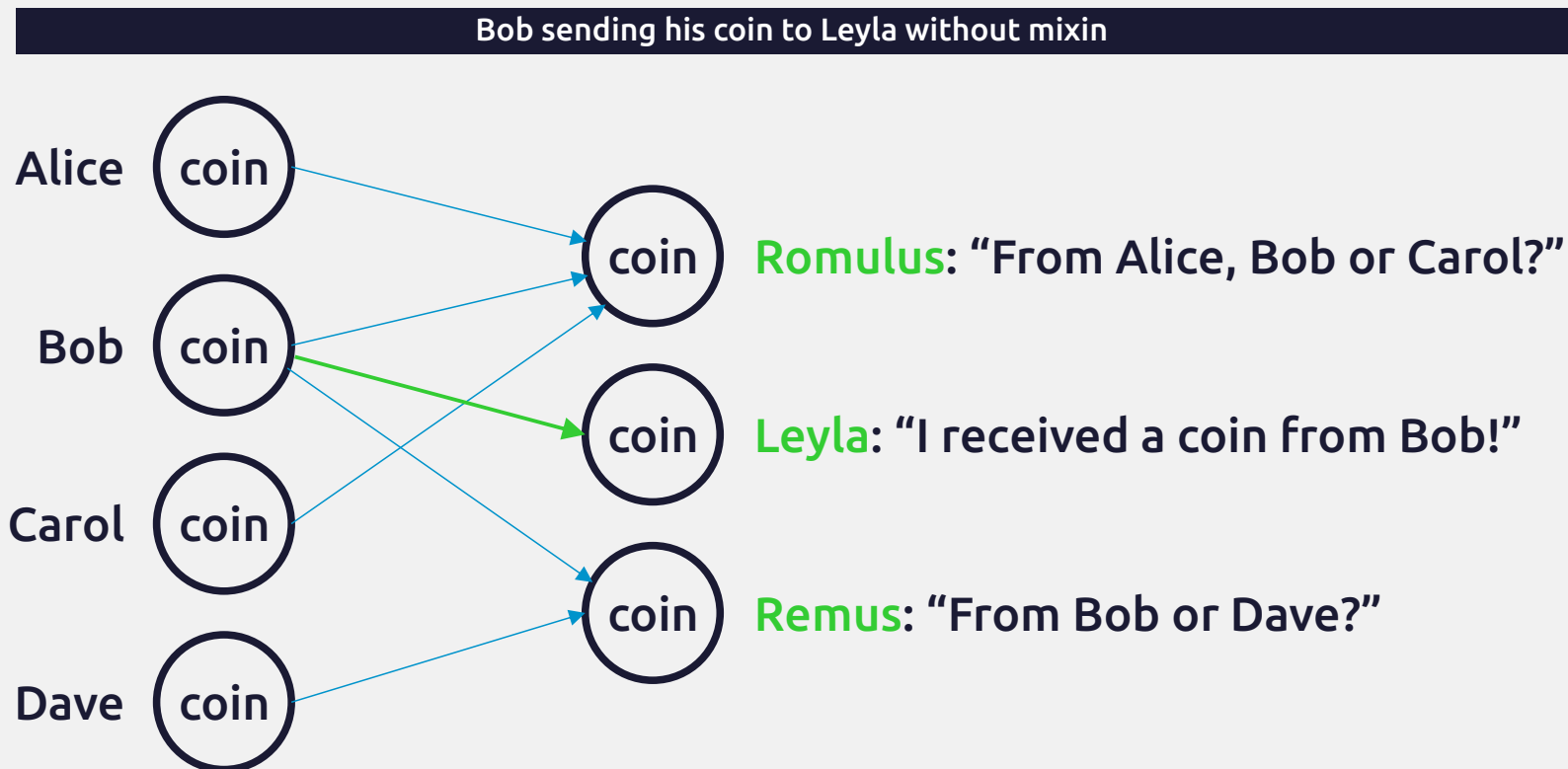


Let's compare!

Ordinary **CryptoNote** Technology

Romulus' and **Remus'** transfer is unlinkable. Great!

But what if **Bob** will decide to send his coin to **Leyla** **without mixin**?

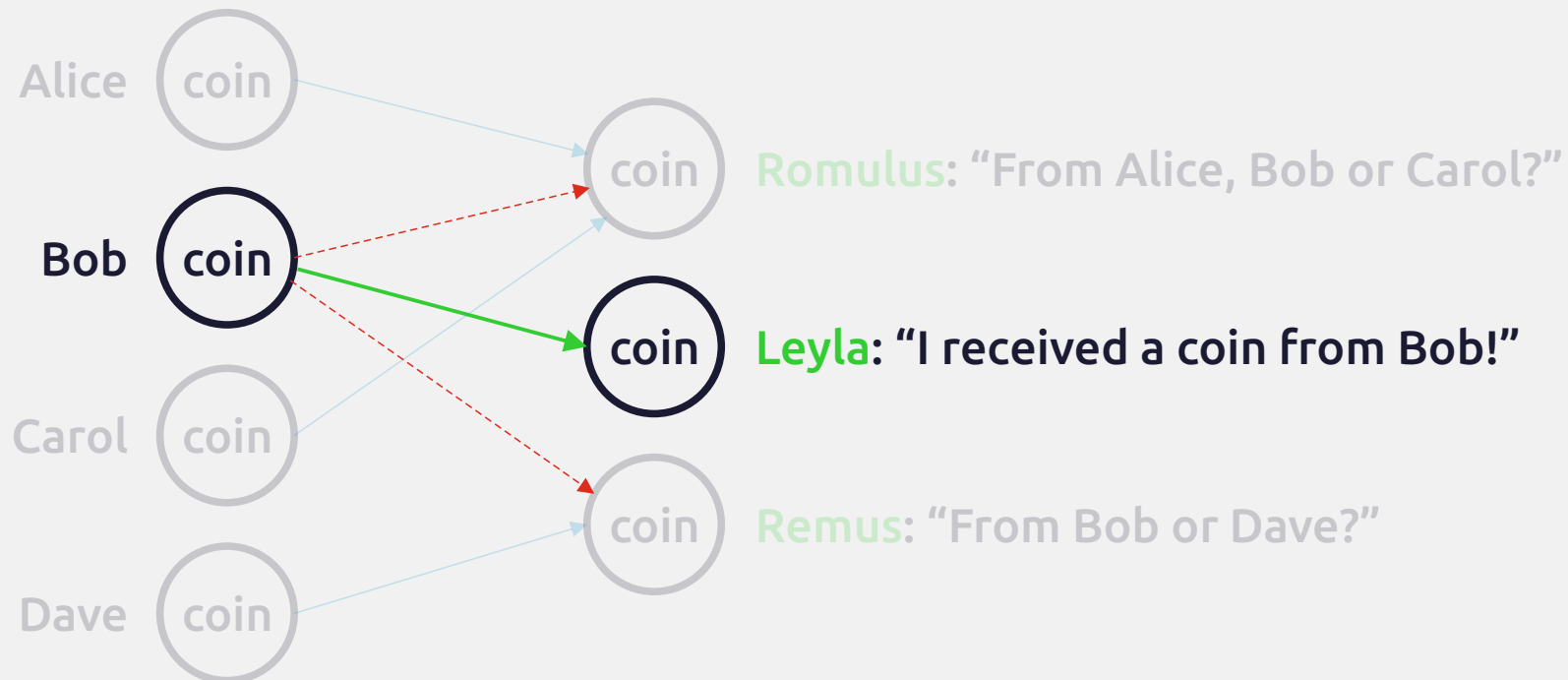


Let's compare!

Ordinary **CryptoNote** Technology

Once **Bob** sent his coin without mixins,
his coin in other **mixins** became **fake**.

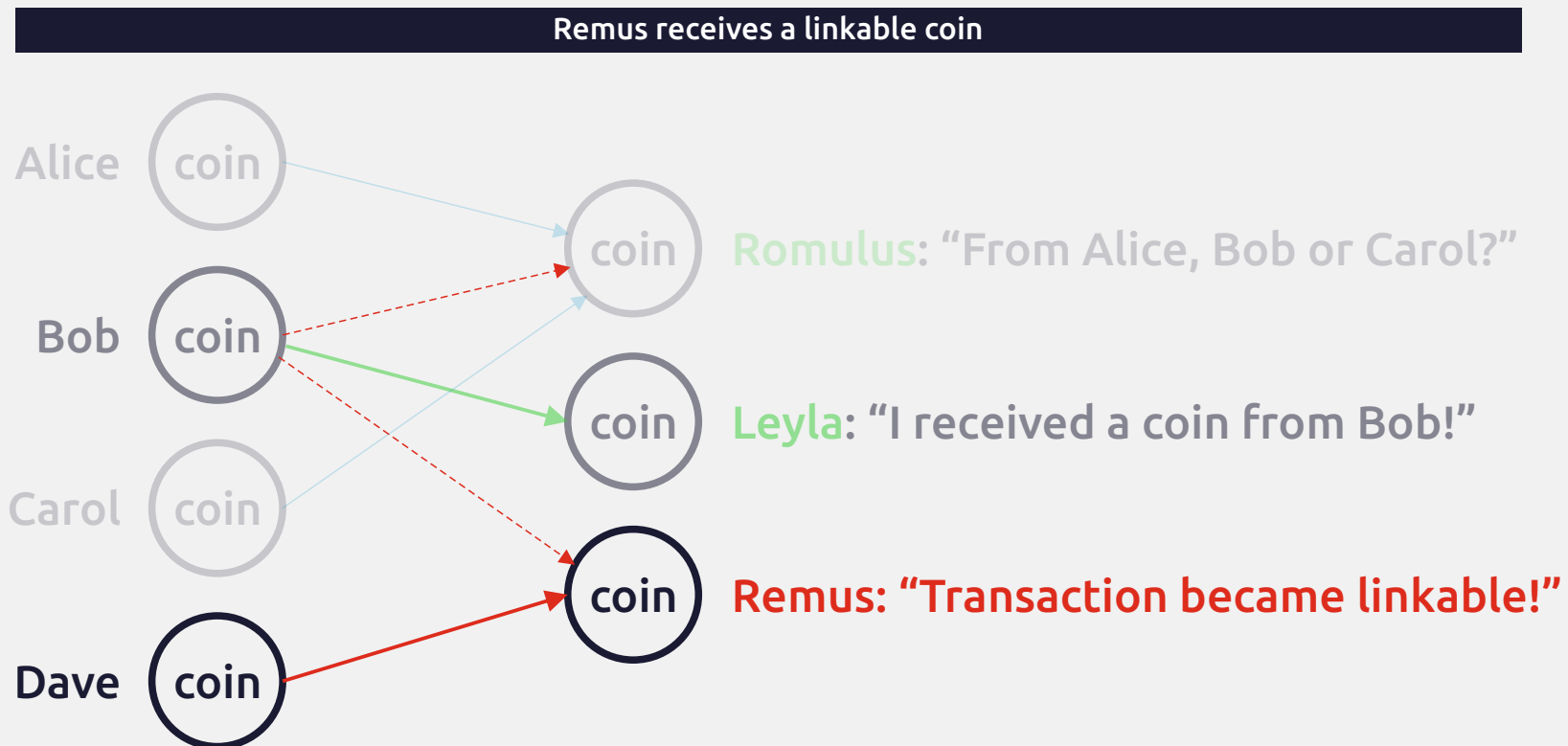
Bob sending his coin to Leyla without mixin



Let's compare!

Ordinary **CryptoNote** Technology

Since all mixins with **Bob's** coin became **fake**,
Dave's transfer **is not unlinkable anymore!**

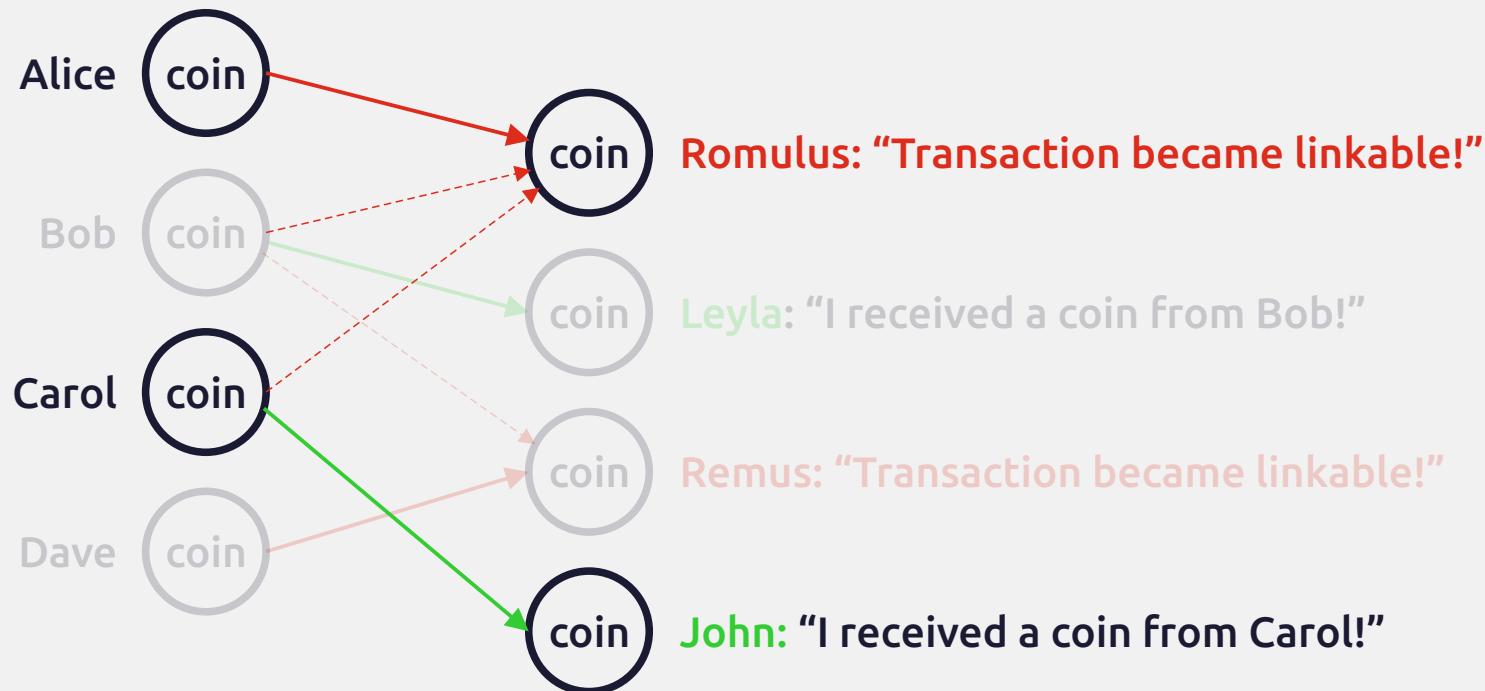


Let's compare!

Ordinary **CryptoNote** Technology

The same issue occurs when **Carol** sends her coin without mixin to **John**.
Alices's transfer **is not unlinkable anymore!**

Carol sending her coin to John without mixin



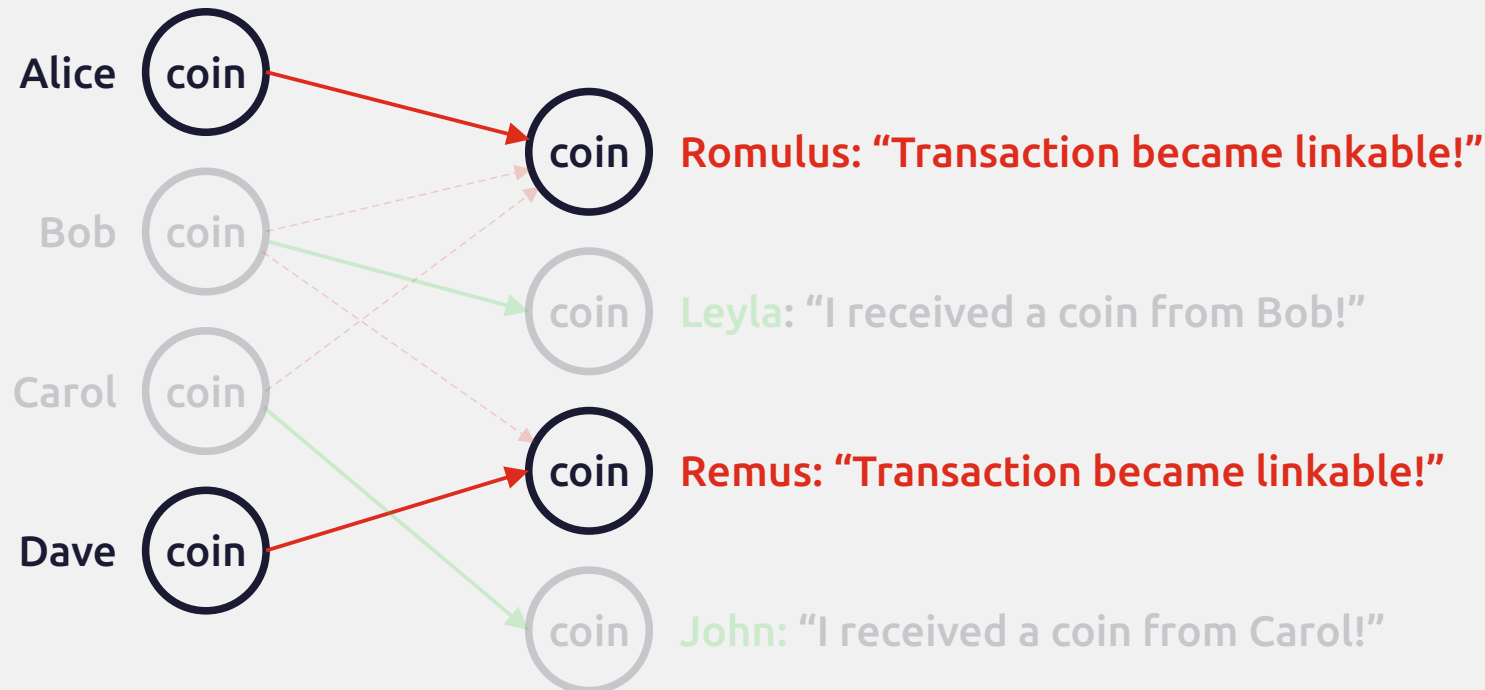
Let's compare!

Ordinary CryptoNote Technology

The problem is that ordinary CryptoNote coin's (Bytecoin/Monero)
***ring signatures will lose unlikability** from time to time.

***ring signature** - Cryptographic algorithm used in CryptoNote technology for transaction validation.

Carol sending her coin to John without mixin



How does boolberry solve this critical issue?

Modified **CryptoNote** Technology

Unlike no other **CryptoNote** coins such as **Bytecoin** and **Monero**, **Boolberry** has a special **flag** in each transaction's output.

With that flag the sender can set the output to be used only with specified number of mixins.

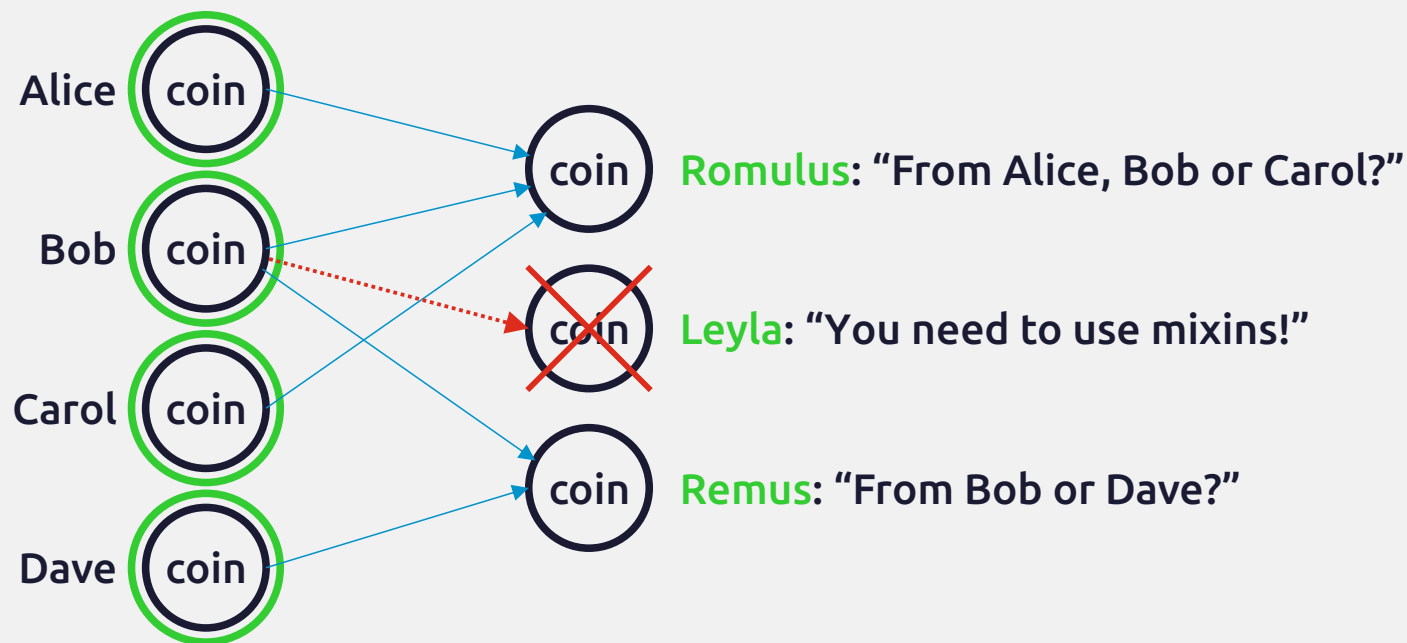
In other words, this flag guarantees that this coin won't be spent without mixins, so it will never compromise ring signatures in which it was involved.

Boolberry's solution

Modified **CryptoNote** Technology

Boolberry's outputs with guaranteed anonymity

Bob is trying to send his coin without mixins, but he can't!

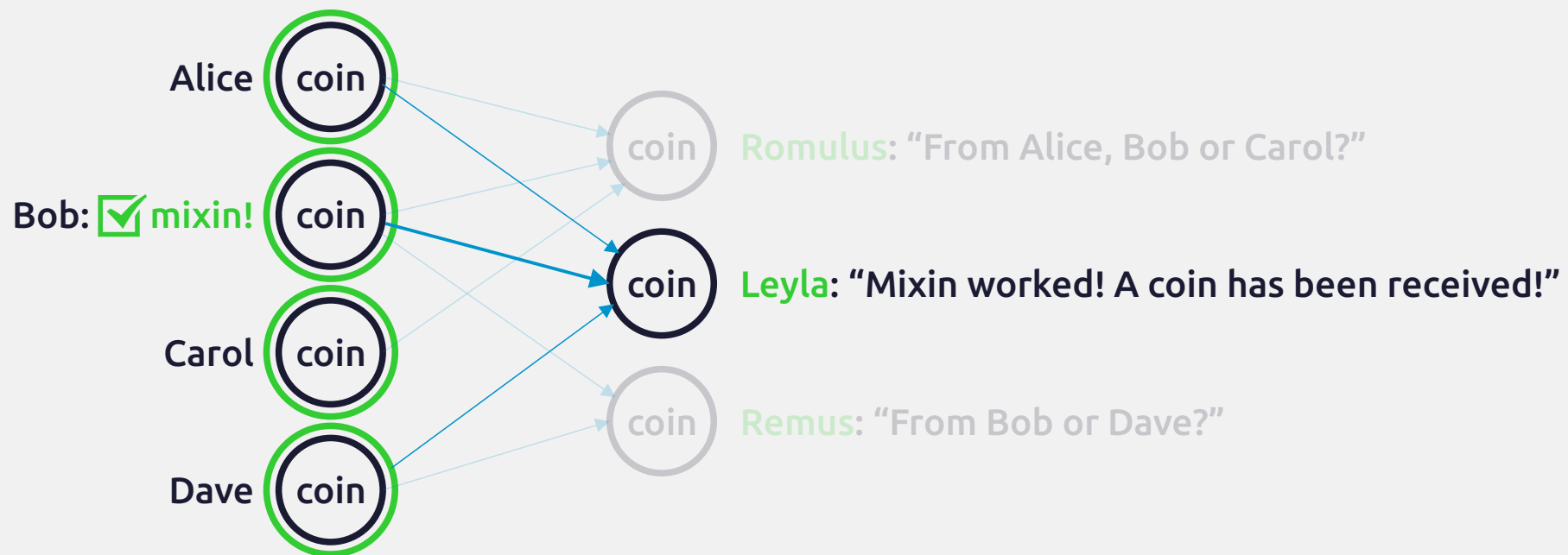


Boolberry's solution

Modified **CryptoNote** Technology

Boolberry's outputs with guaranteed anonymity

The only way to send this coin for Bob is with mixin

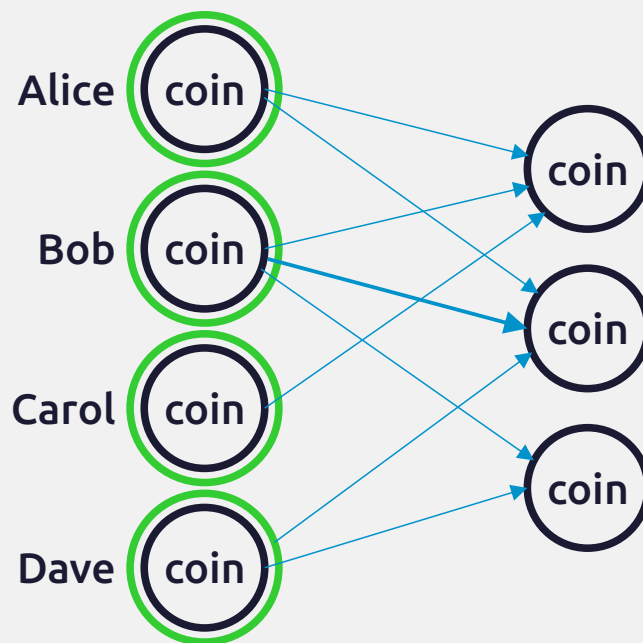


Boolberry's solution

Modified **CryptoNote** Technology

Boolberry's outputs with guaranteed anonymity.
Using this feature **you can be sure** that your transfers
will stay unlinked forever.

Privacy and security - Guaranteed



Guess what?

Boolberry is the first and only
CryptoNote coin that can guarantee
unlinkability for users!

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

For more information please visit www.boolberry.com