This is a pre-release document.

Mining Pool Strategies

Preserving the Integrities of Pool-Controlled Outputs

By Justin Ehrenhofer

The Issue: Explained

Monero mining pools often publish their list of mined blocks and payout transactions. While this is useful for transparency, it negatively impacts the outputs that these pools control.

These outputs may be included in other users’ transactions, which would then be known to be decoys. The effective ringsize is smaller.

This deck covers potential mitigations to preserve the integrity of pool-controlled outputs and their effectiveness.

1. Stealth pool

Don’t publish any coinbase or transaction history.

This one is easy to understand but the least realistic: pools should not reveal any of this information.
While this is best, it would likely receive some pushback from miners who value the transparency.

2. Listing and blackballing all coinbase outputs

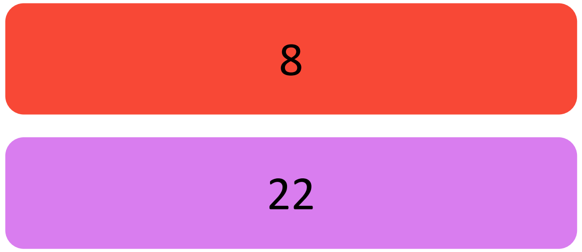
Blackball all coinbase outputs known to be mined by an exchange. Do not post transaction history.

8

This is a pre-release document.

3. Listing and blackballing all pool-controlled outputs

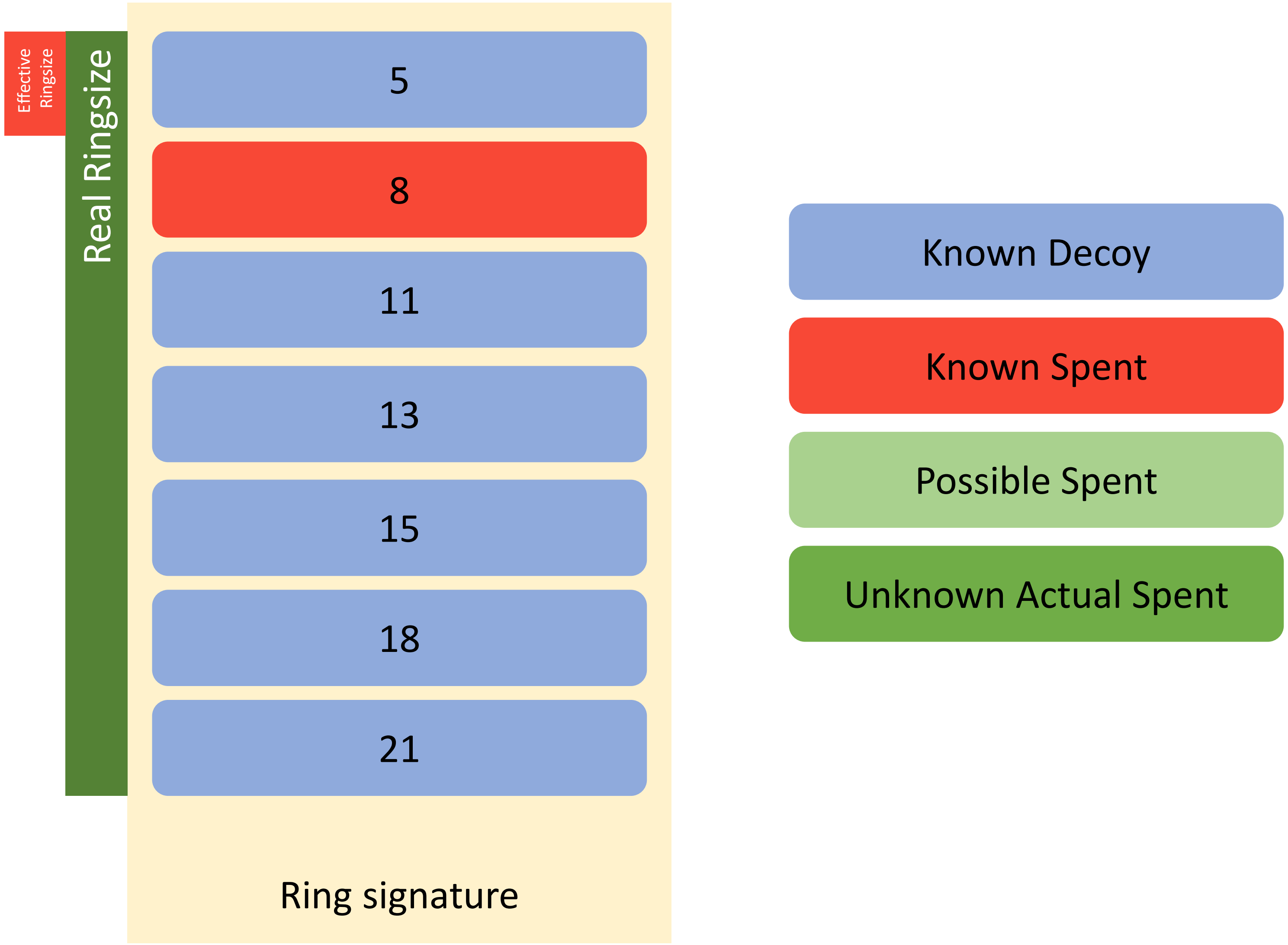
Blackball all outputs known to be controlled by an exchange, including coinbase outputs. Post all transaction history.



4. Multi-’o’ pool payouts

The pool includes other outputs it controls or previously controlled in its ring signatures. A pool mines a new block and receives the corresponding coinbase transaction. The pool publishes its complete block and transaction history.

If the pool makes a transaction now, then it’s clear which output is used, since the pool only ever controlled one output.



Effective Ringsize

Real Ringsize

5

8

11

13

15

18

21

Ring signature

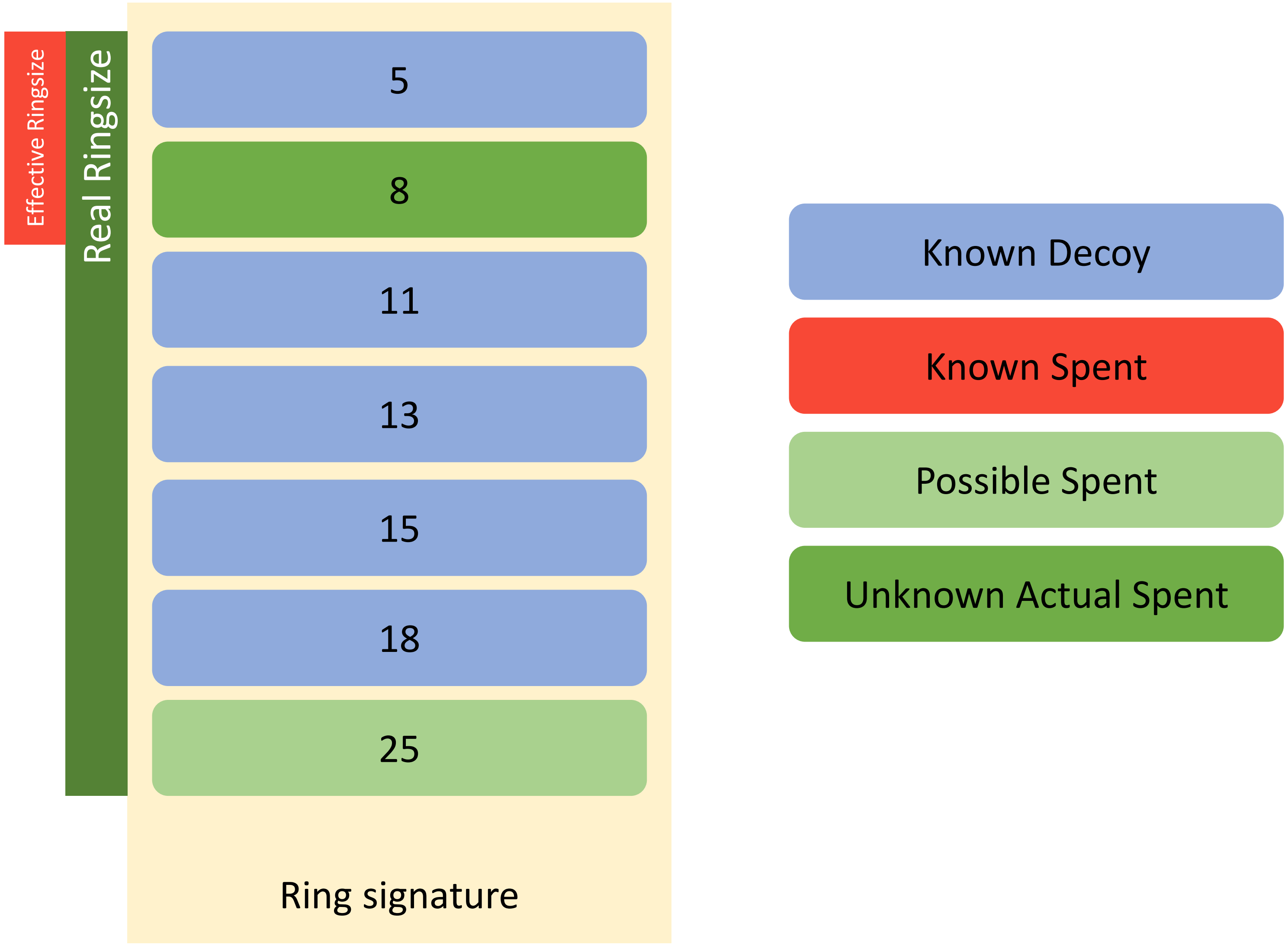
Known Decoy

Known Spent

Possible Spent

Unknown Actual Spent

Suppose the pool mines another block and is assigned another coinbase output. The transaction could look like this, with both green outputs being possible outputs spent.



Effective Ringsize

Real Ringsize

5

8

11

13

15

18

25

Ring signature

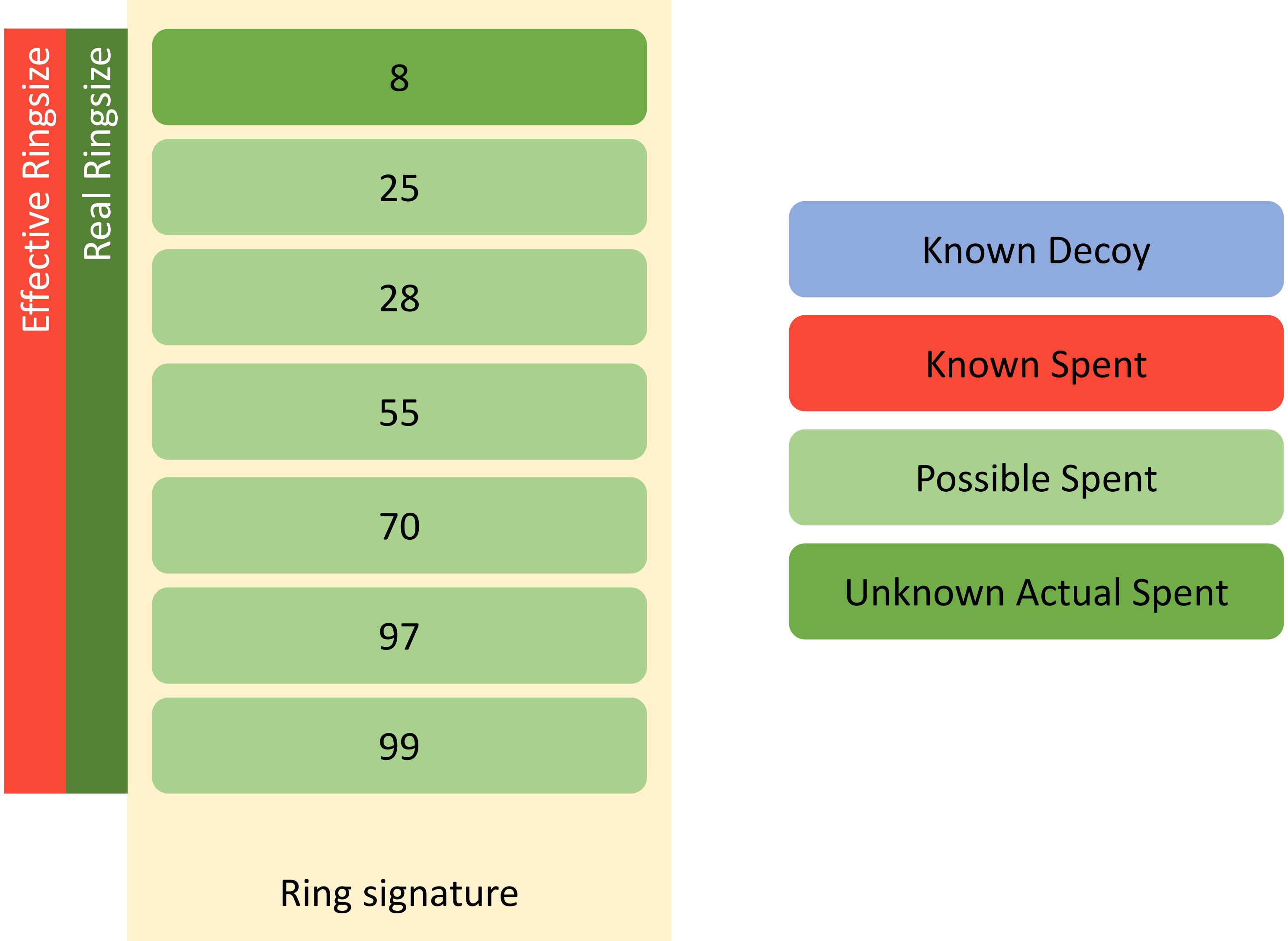
Known Decoy

Known Spent

Possible Spent

Unknown Actual Spent

The pool can select any of its current and previously-controlled outputs as decoys, so that up to all of them can be possible ones spent.



Effective Ringsize

Real Ringsize

8

25

28

55

70

97

99

Ring signature

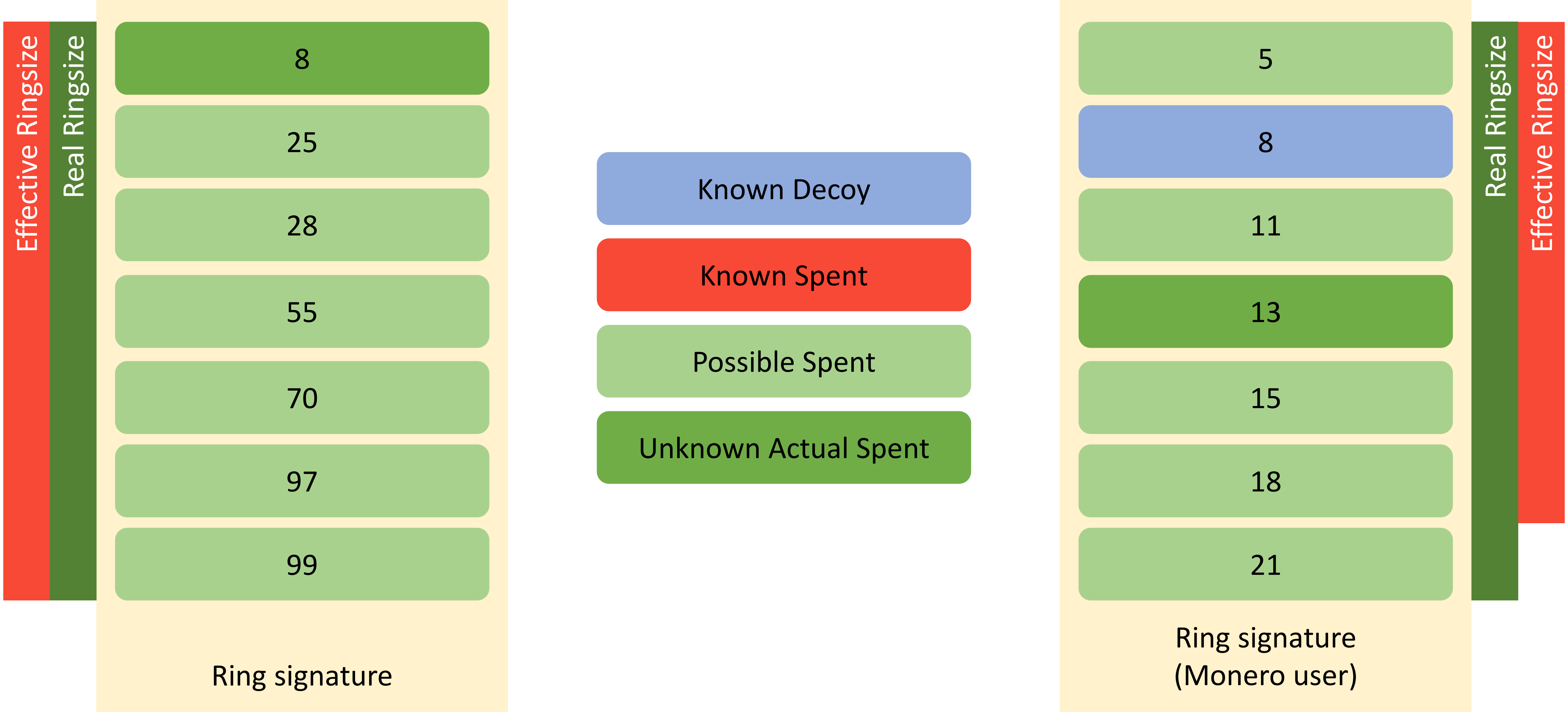
Known Decoy

Known Spent

Possible Spent

Unknown Actual Spent

Unfortunately, this is not especially useful at protecting the integrities of outputs. For transactions by other users, included outputs controlled by the pool are known to be decoys. As a result, this method isn't very helpful. It provides ambiguity for the pool so no one knows what outputs are spent in each transaction, but it does little to hide the pool is spending these funds. Other users' decoys are known to be fake.



Effective Ringsize

Real Ringsize

8

25

28

55

70

97

99

Ring signature

Known Decoy

Known Spent

Possible Spent

Unknown Actual Spent

5

8

11

13

15

18

21

Ring signature
(Monero user)

Real Ringsize

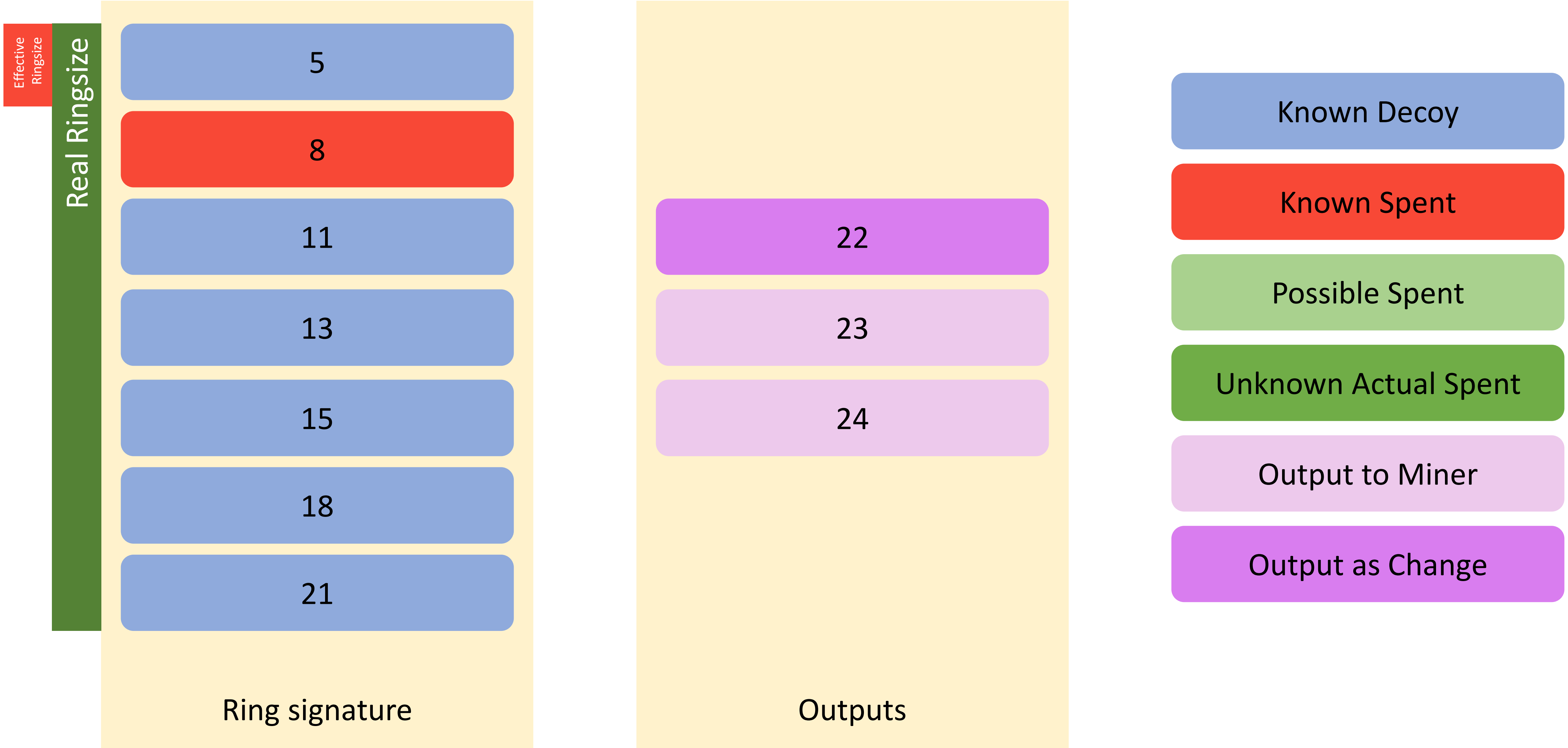
Effective Ringsize

5. Pools include miner payout outputs in their ring signatures

A pool includes outputs paid to miners in its ring signatures. A pool mines a new block and receives the corresponding coinbase transaction. The pool publishes its complete block and transaction history.

8

The pool makes its first payment. The initial coinbase output is known to be spent. Three outputs are created, two going to miners and one returning as change.



Effective Ringsize

Real Ringsize

5

8

11

13

15

18

21

Ring signature

22

23

24

Outputs

Known Decoy

Known Spent

Possible Spent

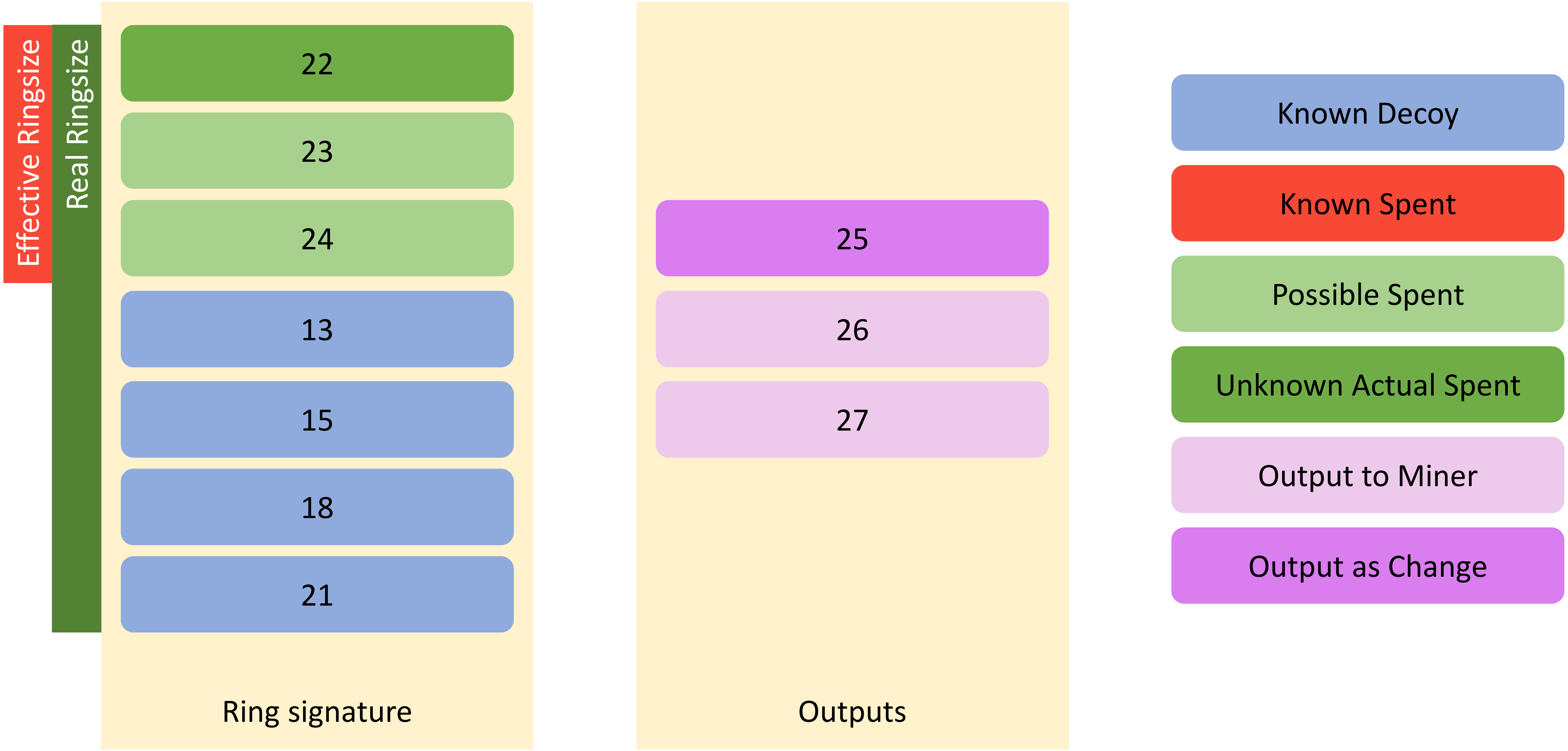
Unknown Actual Spent

Output to Miner

Output as Change

This is a pre-release document.

For the second payment, the pool selects a set (or all) of the outputs created in the previous transaction. In doing so, it is now unclear which output is actually spent, since all three could be spent.



Effective Ringsize

Real Ringsize

22

23

24

13

15

18

21

Ring signature

25

26

27

Outputs

Known Decoy

Known Spent

Possible Spent

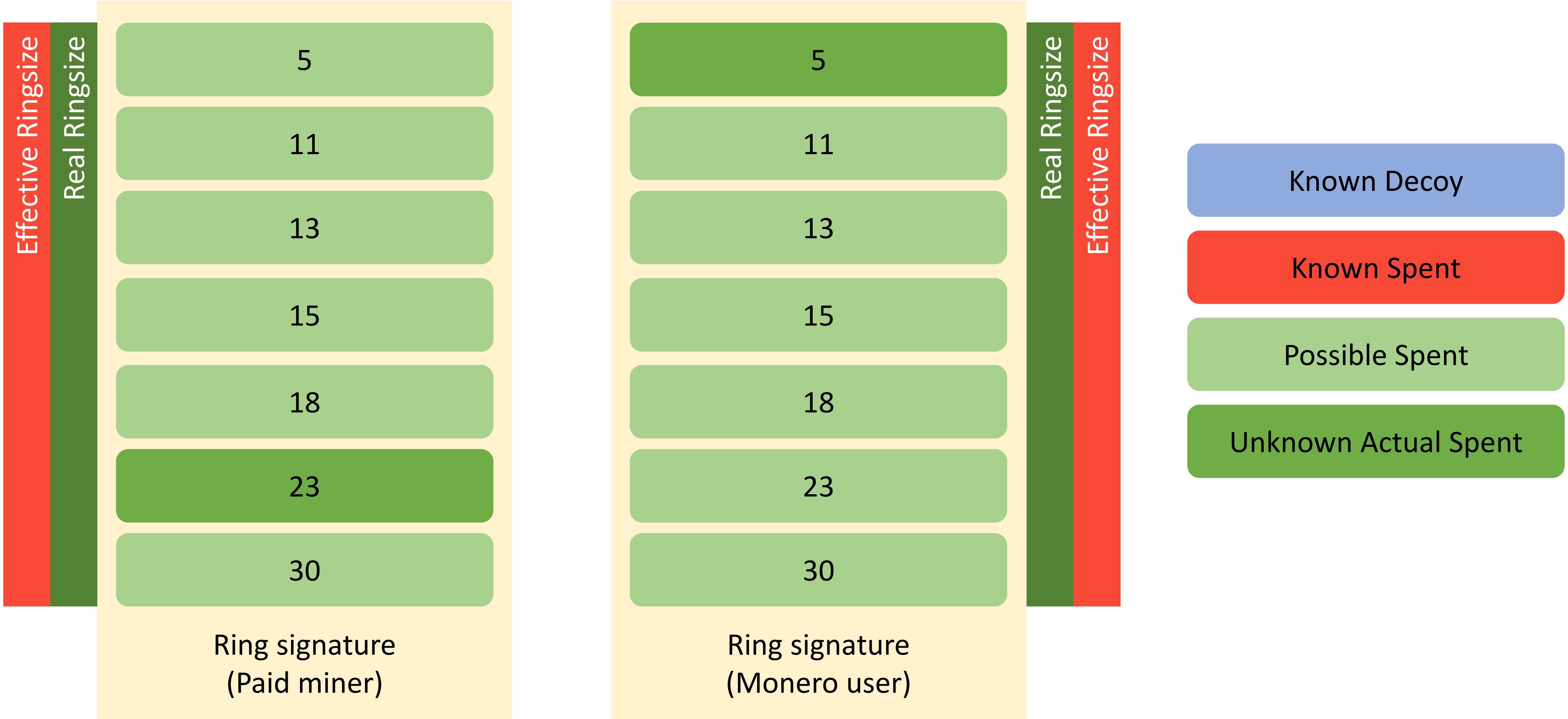
Unknown Actual Spent

Output to Miner

Output as Change

This is a pre-release document.

Most importantly, other transactions created by the paid miners look indistinguishable from transactions that other Monero users. The integrities of the change outputs are preserved.



Effective Ringsize

Real Ringsize

5

11

13

15

18

23

30

Ring signature
(Paid miner)

5

11

13

15

18

23

30

Ring signature
(Monero user)

Real Ringsize

Effective Ringsize

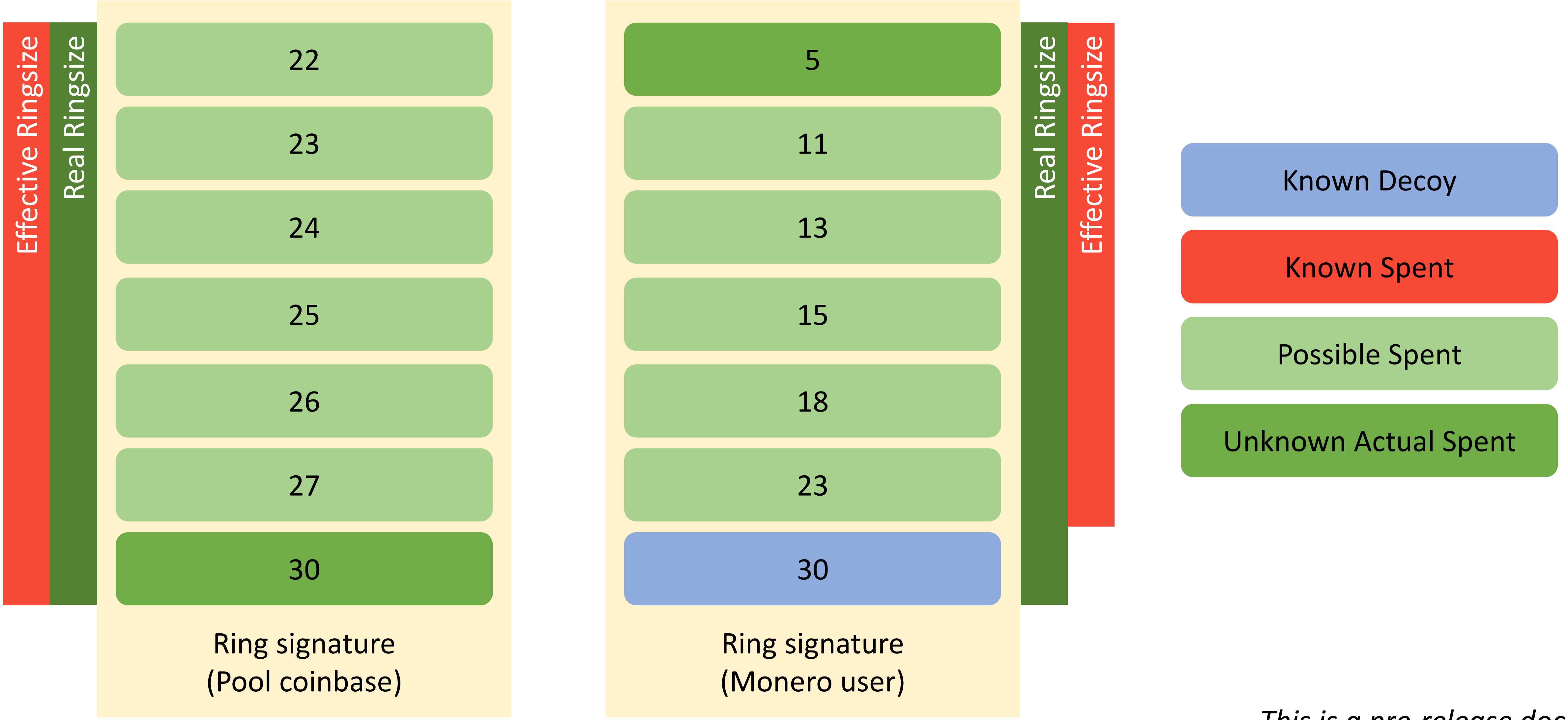
Known Decoy

Known Spent

Possible Spent

Unknown Actual Spent

Unfortunately, coinbase outputs are still compromised, since attackers know that the coinbase outputs could only be associated with transactions by the pool. While a coinbase output could be hidden among several other possible spent outputs (as shown below), it does not protect other non-pool transactions. These coinbase outputs should be blackballed or churned (see method #6).



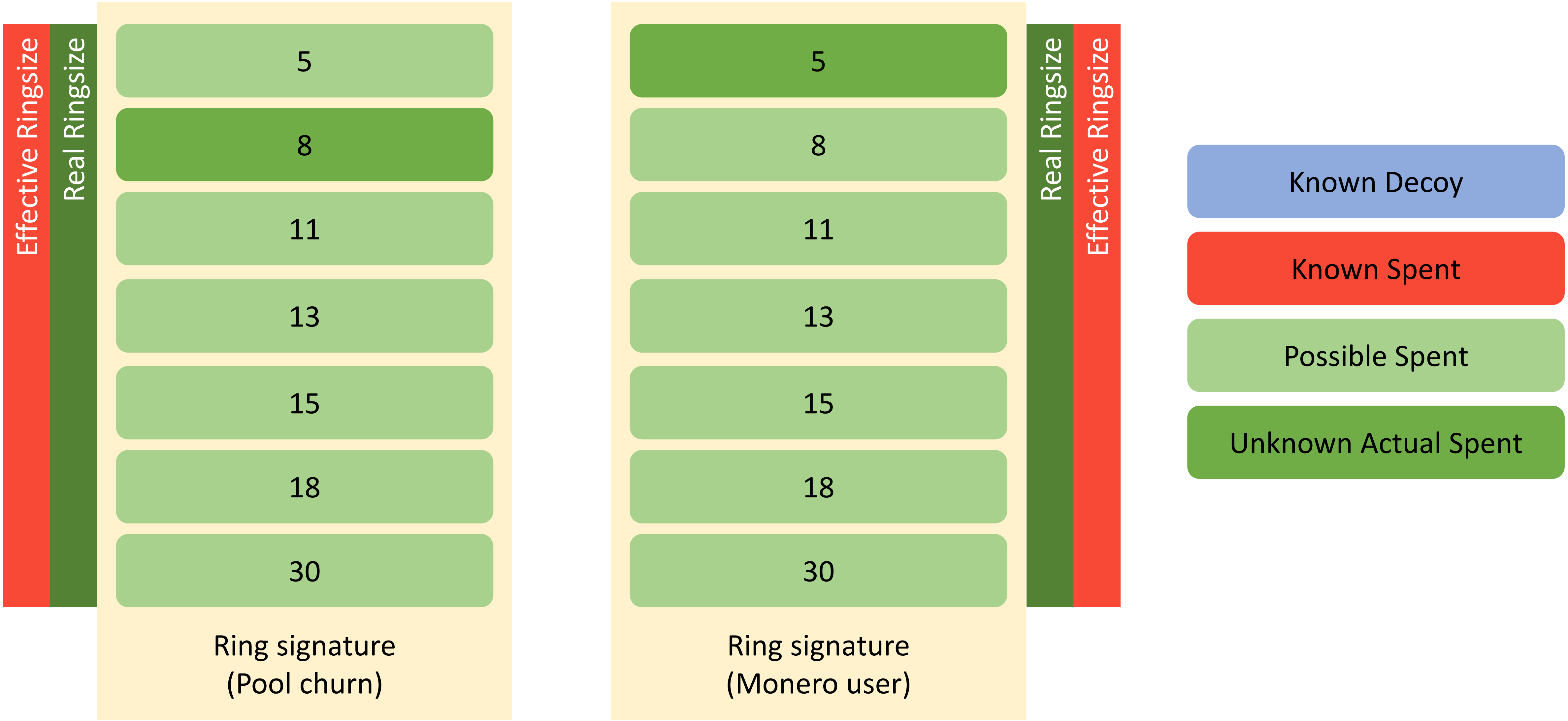
This is a pre-release document.

6. Secret churning

A pool churns all coinbase outputs *x* times without publishing the churn transactions. A pool mines a new block and receives the corresponding coinbase transaction. The pool publishes all other mined block and transaction history.

8

The pool undergoes churning without publishing the churn transaction on the site. The output, when not combined with other known mined coinbase outputs in their own ring signatures, is indistinguishable in other transactions when it is used as a decoy. If combined with other mined coinbase outputs, blackball coinbase outputs.



Effective Ringsize

Real Ringsize

5
8
11
13
15
18
30

Ring signature
(Pool churn)

5
8
11
13
15
18
30

Ring signature
(Monero user)

Real Ringsize

Effective Ringsize

Known Decoy

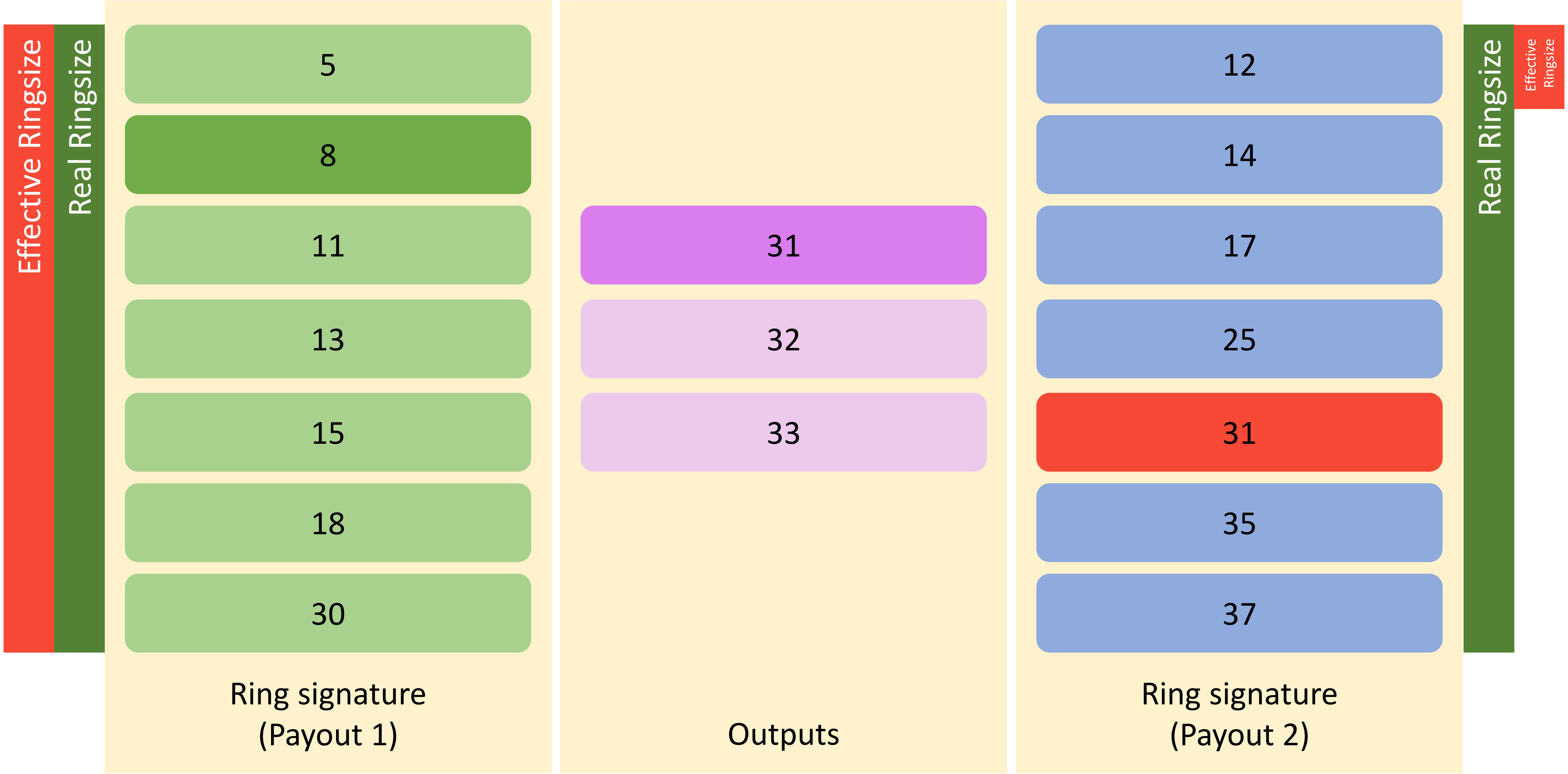
Known Spent

Possible Spent

Unknown Actual Spent

This is a pre-release document.

Unfortunately, subsequent transactions' change outputs are not protected, since the change output will be clearly used as the input of the next transaction. This can be avoided if the pool only publishes coinbase outputs and does not publish a list of other transactions, or if the pool uses a different input selection algorithm.



This is a pre-release document.

Wallet Work

Wallets should be configured to include the following functionality:

1. Choose a pool input selection algorithm (eg: --selection-mode pool)
2. Avoid using coinbase outputs by default (eg: --avoid-coinbase true)
3. Churning mechanism
4. Add mechanism for fetching blackball lists by URL

Best mitigations:
In general:

1. Prefer solutions with the least amount of revealed public data.
2. Prefer solutions where no wallet interaction is necessary.
3. Prefer solutions where in the case of wallet interaction, it can be a simple fix.
4. Prefer solutions with the least impact on the network.

Protection identification code:

What information is highly actionable? 0 – None, 1 – Coinbase, 2 – Change, 3 – Coinbase and Change
What information is revealed? 0 – None, 1 – Coinbase, 2 – Change, 3 – Coinbase and Change
What blackballing is necessary? 0 – None, 1 – Coinbase, 2 – Change, 3 – Coinbase and Change
What is the additional network impact? 0 – None, 1 – Different selection algorithm, 2.x – x Coinbase churns, 3.x – Coinbase churns and different selection algorithm, 4.x – Change churns, 5.x – Coinbase and Change churns, 6 – Other; x = version for churning

[0000]:
Become a stealth pool. Reveal no coinbase or transaction history.

Pros
No information is public
No wallet interaction needed
No additional strain on network

Cons
More potential for pool corruption

Happy people
Network

Sad people
Miners

[0201]:

Reveal transaction history but not coinbase history.
Include payout outputs in ring signatures.

Pros

No wallet interaction needed
No additional strain on network

Cons

More potential for pool corruption
One count of limited actionable public information (change outputs)

Happy people

Network

Sad people

Miners

[0102]:

Reveal coinbase history but not transaction history.
Churn coinbase outputs.

Pros

No wallet interaction needed

Cons

More potential for pool corruption
Churns strain the network and add cost
One count of limited actionable public information (coinbase outputs)

Happy people

Network (privacy)

Sad people

Miners
Pool
Network (bloat)

[0303.x]:

Reveal coinbase and transaction history.
Churn coinbase outputs.
Include payout outputs in ring signatures.

Pros

No wallet interaction needed

Cons

Churns strain the network and add cost
Two counts of limited actionable public information (coinbase and change outputs)

Happy people

Network (privacy)

Sad people

Pool
Network (bloat)

[1110]:
Reveal coinbase history but not transaction history.
Blackball/avoid coinbase outputs (provide API to scrape).

Pros
No additional strain on network

Cons
One count of significant public information (coinbase outputs)
Simple wallet interaction needed
More potential for pool corruption

Happy people
Network (bloat)

Sad people
Network (privacy)
Miners

[1311]:
Reveal coinbase and transaction history.
Blackball/avoid coinbase outputs (provide API to scrape).
Include payout outputs in ring signatures.

Pros
No additional strain on network

Cons
One count of significant public information (coinbase outputs)
One count of limited actionable public information (change outputs)
Simple wallet interaction needed

Happy people
Network (bloat)

Sad people
Network (privacy)

This is a pre-release document.

[3330]:
Reveal coinbase and transaction history.
Blackball/avoid pool outputs (provide API to scrape).

Pros
No additional strain on network

Cons
Two counts of significant public information (coinbase and change outputs)
Complex wallet interaction needed

Happy people
Network (bloat)

Sad people
Network (privacy)

[0305.xy]:

Reveal coinbase and transaction history.
Churn each output individually before sending every transaction.

Pros

No wallet interaction needed

Cons

Two counts of limited actionable public information (coinbase and change outputs)
Churns strain the network and add cost

Happy people

Network (privacy)

Sad people

Network (bloat)
Pool