grincon1
2019.11.22 // c-base berlin

Ethereum 9 3/4

Mimblewimble on Ethereum with zk-SNARKs

@wanseob

QTUM

SPARK POOL

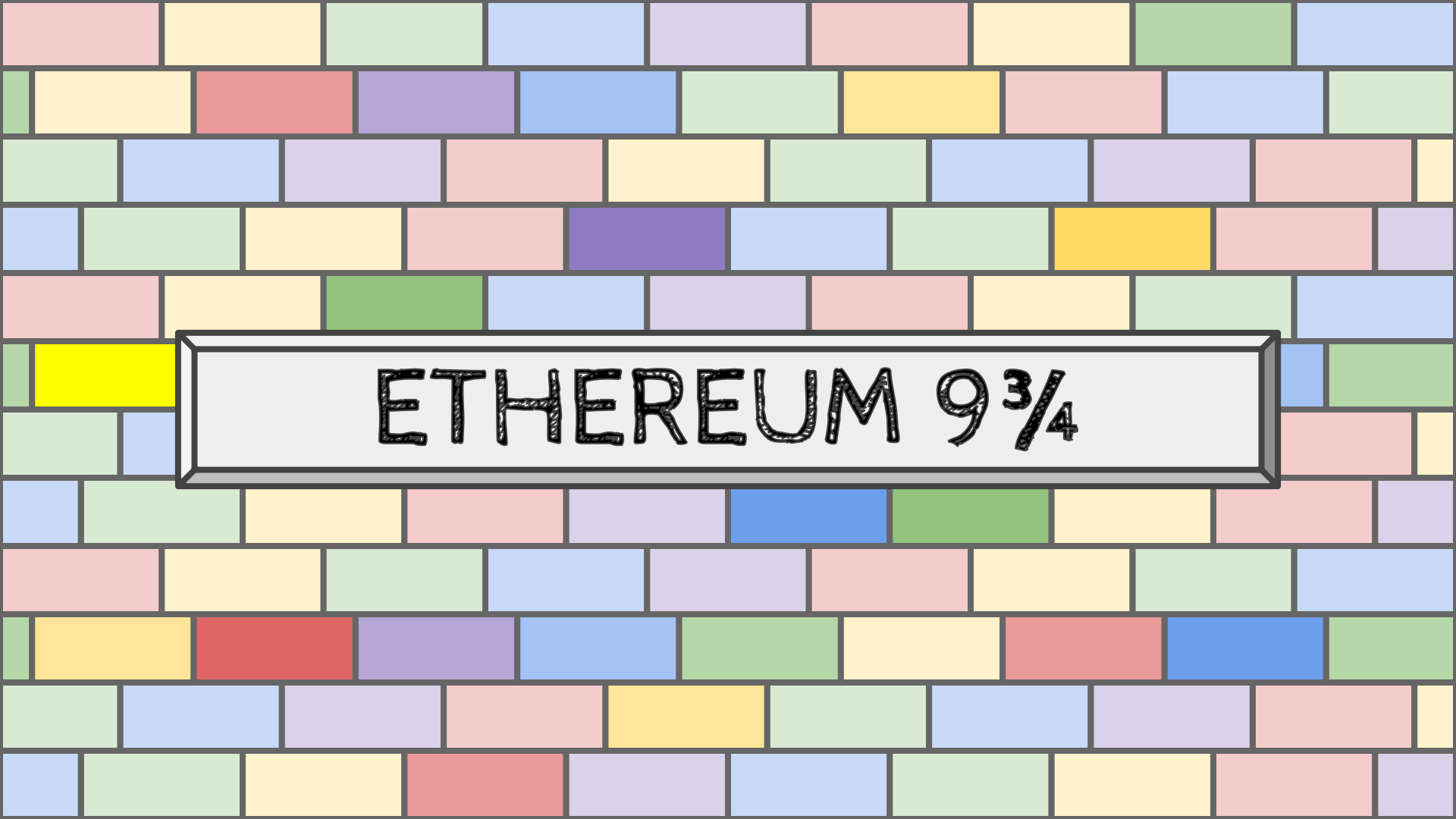
Wanseob Lim
nonce (Crypto community)
Ethcon
github.com/wanseob
twitter: @wanseoblim


venmo


pay

wanseob.eth


He has only 1 ETH !
He’s using CDP and lending lots of money
wanseob.eth
He’s using Binance and withdrew 32 ETH!


ETHEREUM 9¾

Ethereum 9¾ is the gateway to the magical world where we can use the Mimblewimble spell...

Muggle world

Magical world

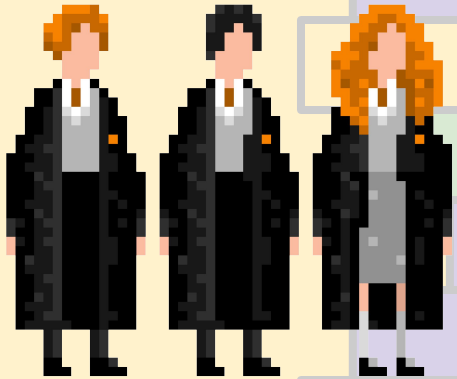
ETHEREUM 9¾

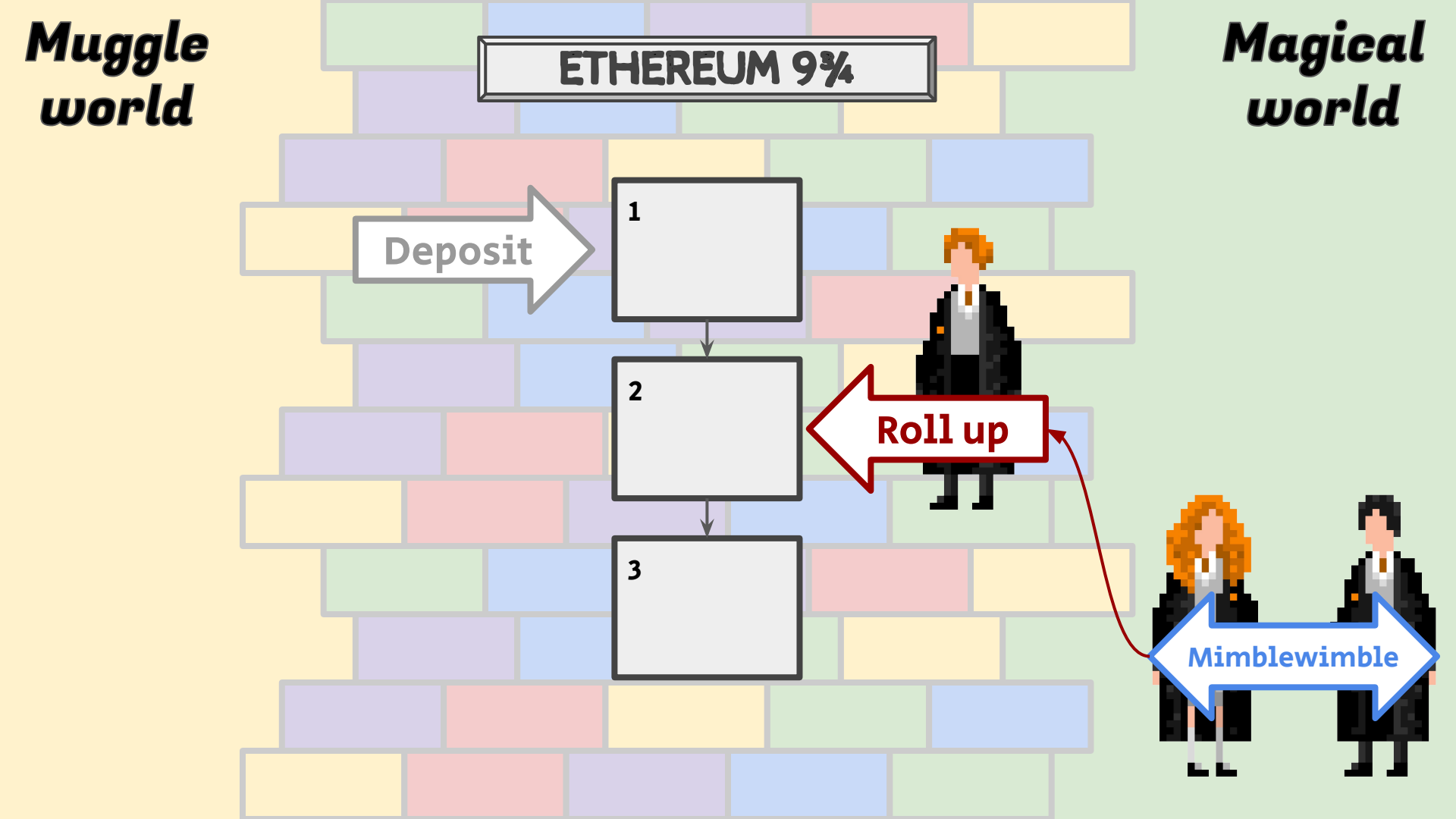
Deposit

1

2

3




Muggle world
ETHEREUM 9¾
Magical world
Deposit
1
2
3
Roll up
Mimblewimble

Muggle world

Magical world

ETHEREUM 9¾

Deposit

1

2

3

Roll up

Roll up

Mimblewimble

Mimblewimble

Mimblewimble

Fees in ERC20

Muggle world

Magical world

ETHEREUM 9¾

2

Roll up

3

Roll up

4

Withdraw

Technical details

zk-SNARKs friendly

zk-SNARKs friendly

zk-SNARKs friendly

Mimblewimble TXO

$$\textit{private key}\ r \qquad \textit{value}\ v$$

Mimblewimble TXO

$P(321..., 112...)$

Mimblewimble on the
baby Jubjub curve.

Mimblewimble equation

+ Input TXO	$+ (r_{in} \bullet G + v_{in} \bullet H)$
− Output TXOs	$- (r_{out1} \bullet G + v_{out1} \bullet H)$
	$- (r_{out2} \bullet G + v_{out2} \bullet H)$
− Fee	$- v_{Fee} \bullet H$
= Excess	$= r_{excess} \bullet G + \boxed{0 \bullet H}$

$$v_{in} - (v_{out1} + v_{out2} + v_{fee}) = 0$$

Mimblewimble transaction

\+ Input TXO

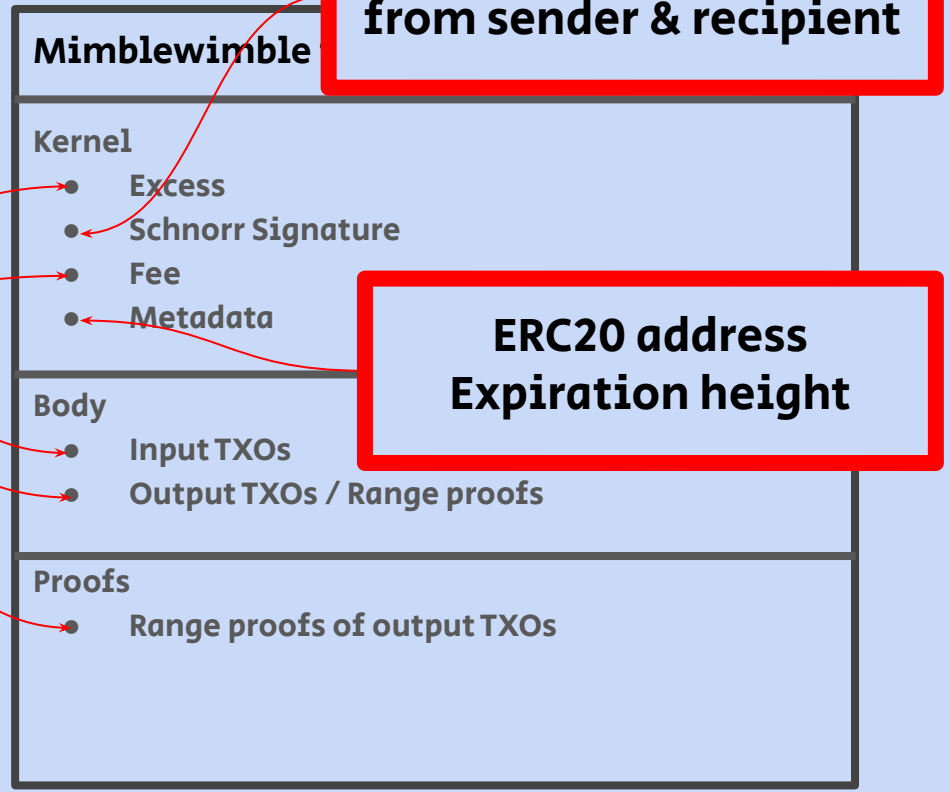
\- Output TXOs

$$r \cdot G + v \cdot H$$

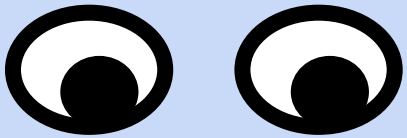
$$0 \leq v < safe\_range$$

\- Fee

= Excess



Problem of Mimblewimble on Ethereum



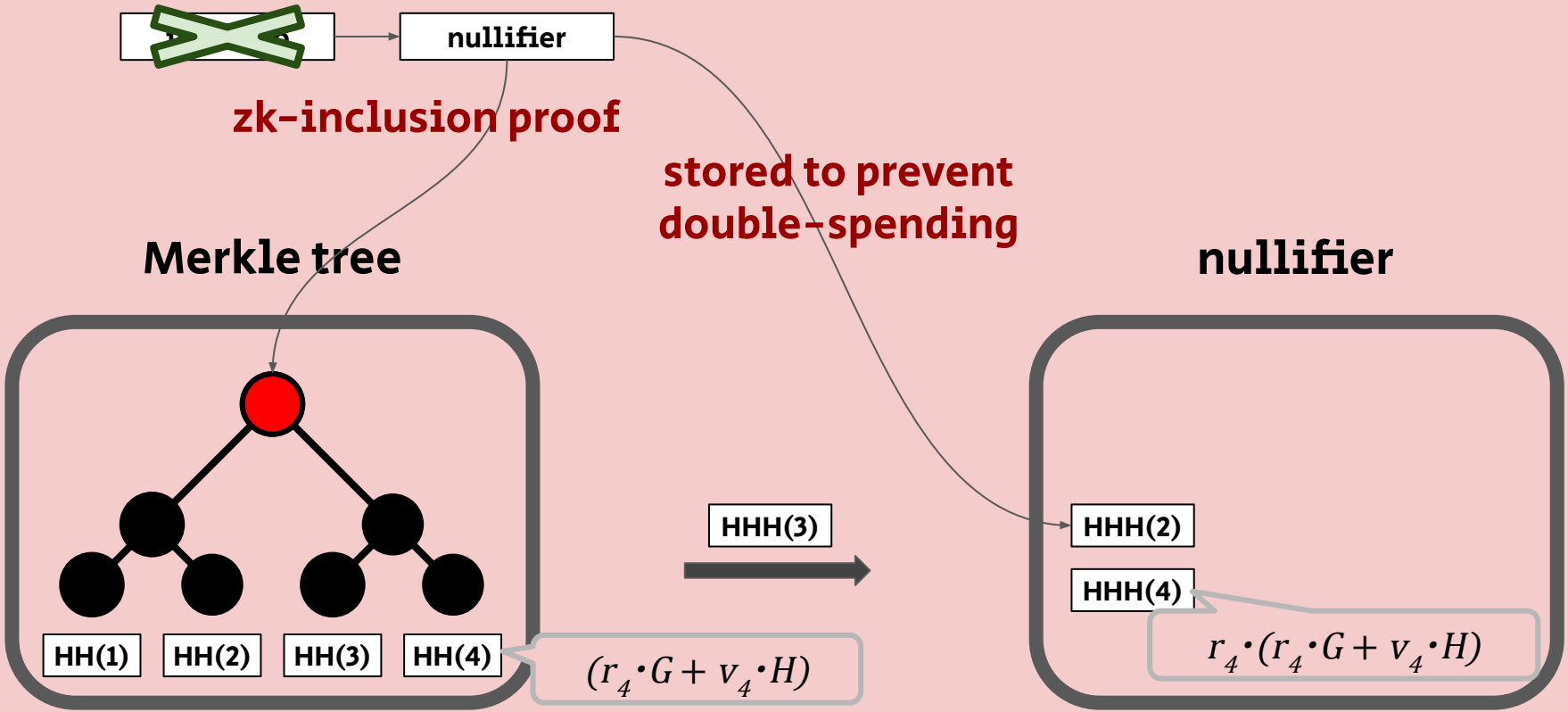
Mimblewimble transaction

Kernel
- Excess
- Schnorr Signature
- Fee
- Metadata

Body
- **Input TXOs**
- Output TXOs / Range proofs

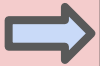
Proofs
- Range proofs of output TXOs

Commitment-nullifier scheme



Zk Mimblewimble transaction

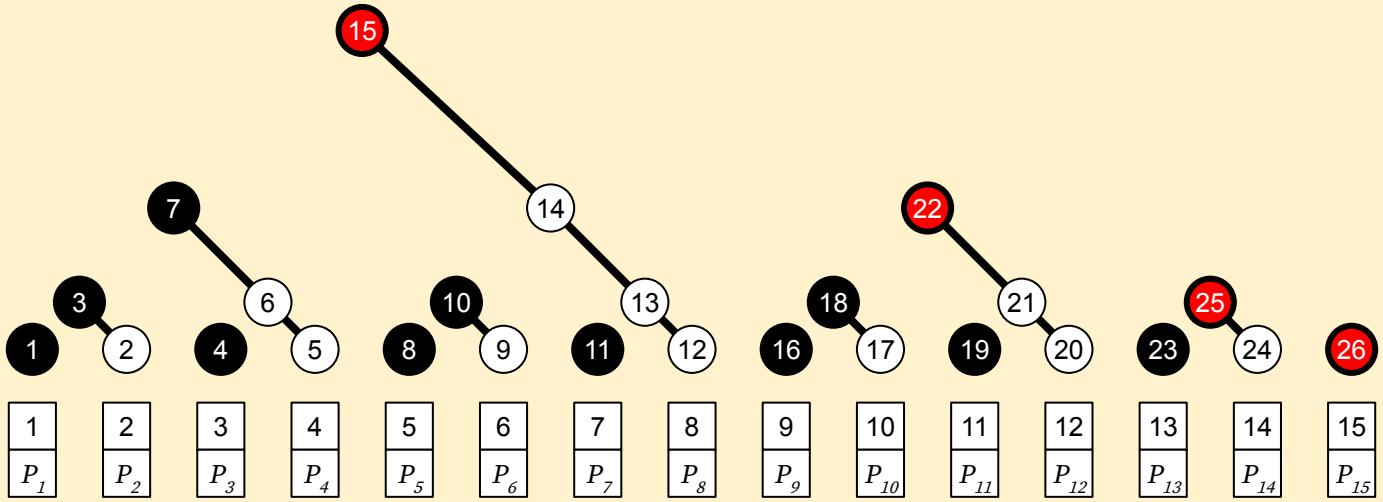
Original Mimblewimble transaction
Kernel • Excess • Schnorr Signature • Fee • Metadata
Body • Input TXOs • Output TXOs / Range proofs
Proofs • Range proofs of output TXOs



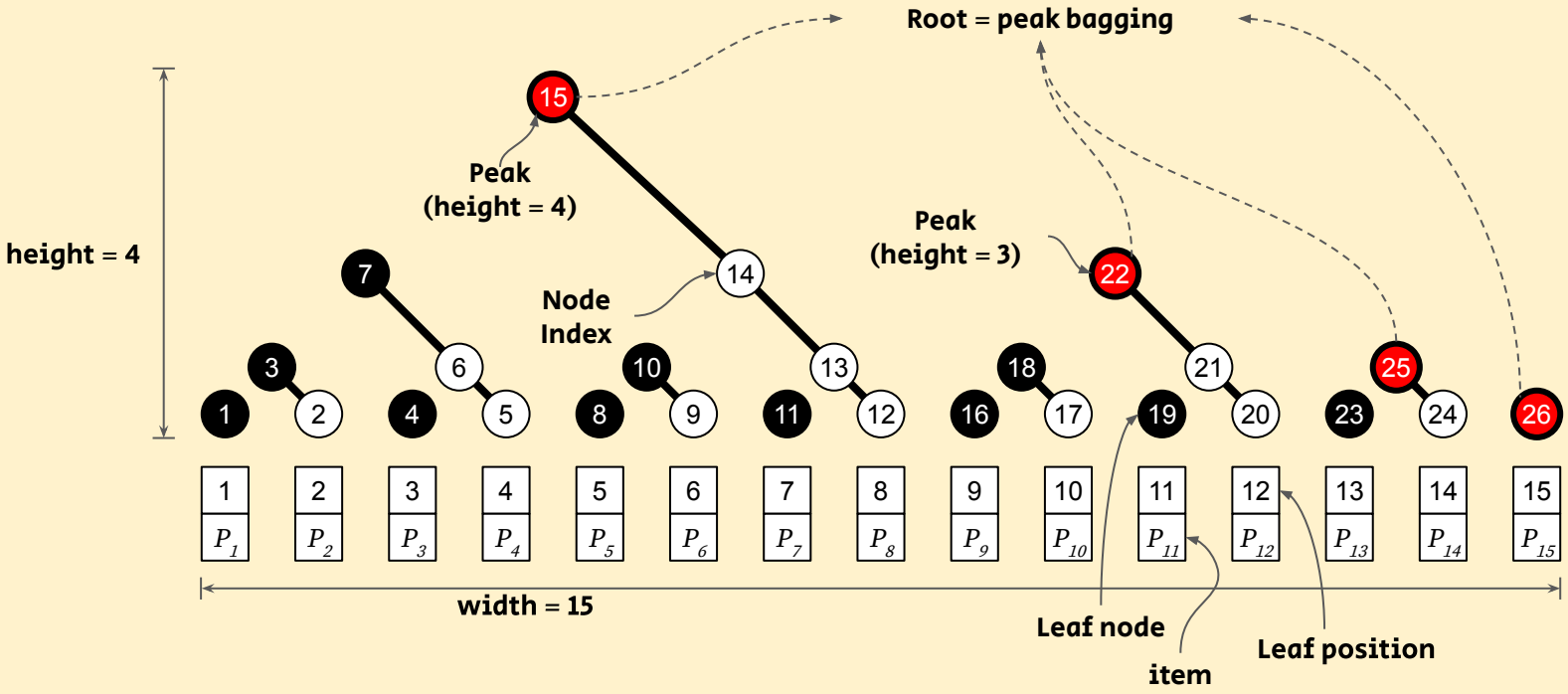
Zk Mimblewimble transaction
Kernel • Excess • Schnorr Signature • Fee • Metadata
Body • Spent tags(nullifier) • Output TXOs
Proofs • Range proofs of output TXOs • Inclusion proofs of spent tags • Mimblewimble proof

zk-Roll Up friendly data structure

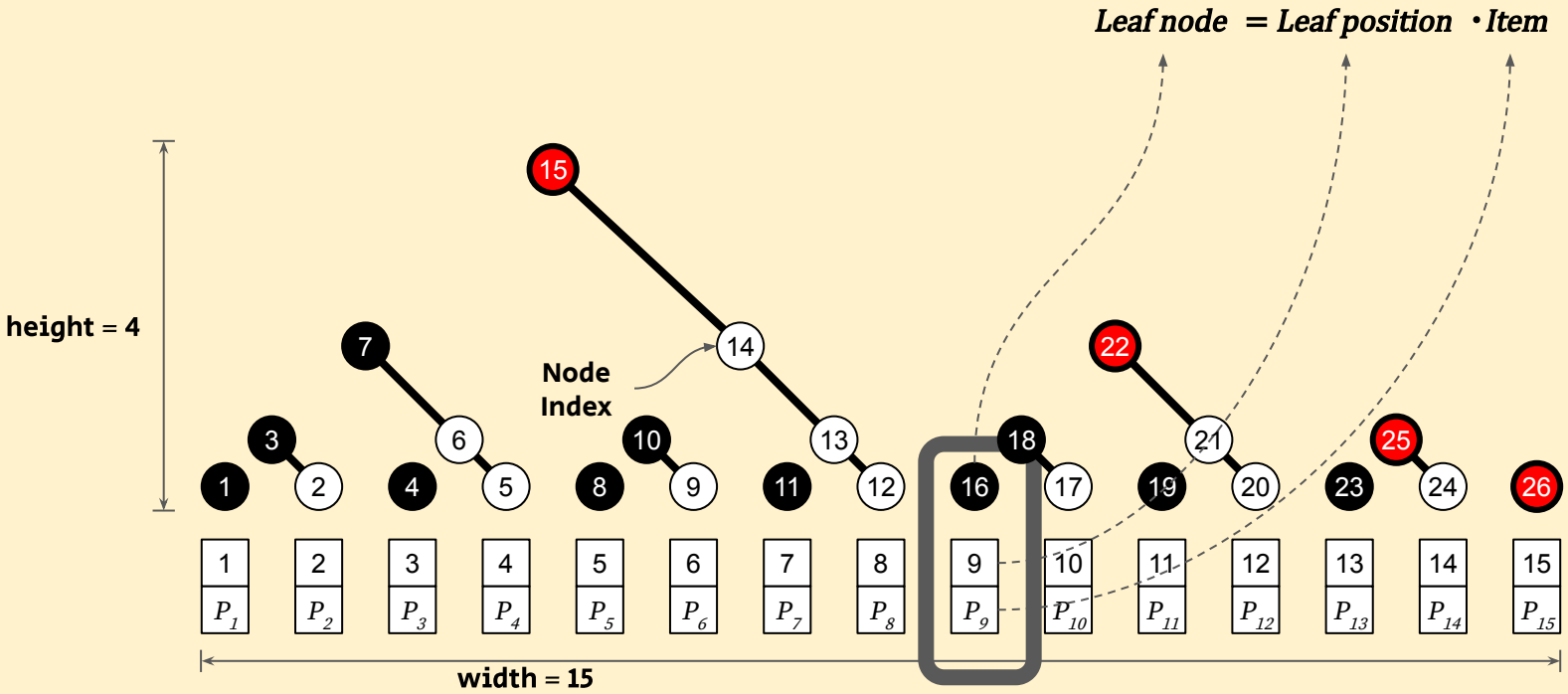
Merkle Mountain Range



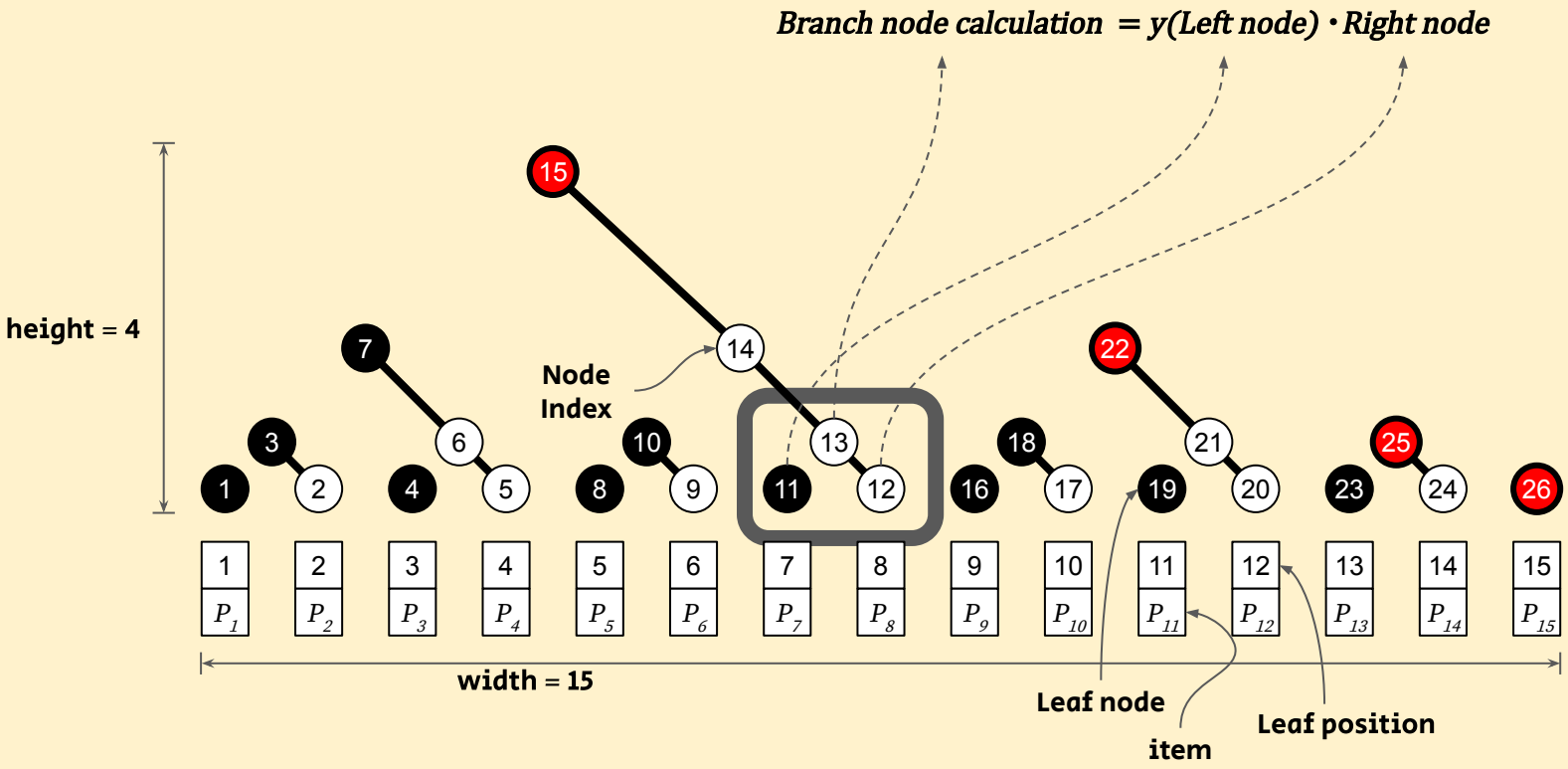
Pedersen Merkle Mountain Range



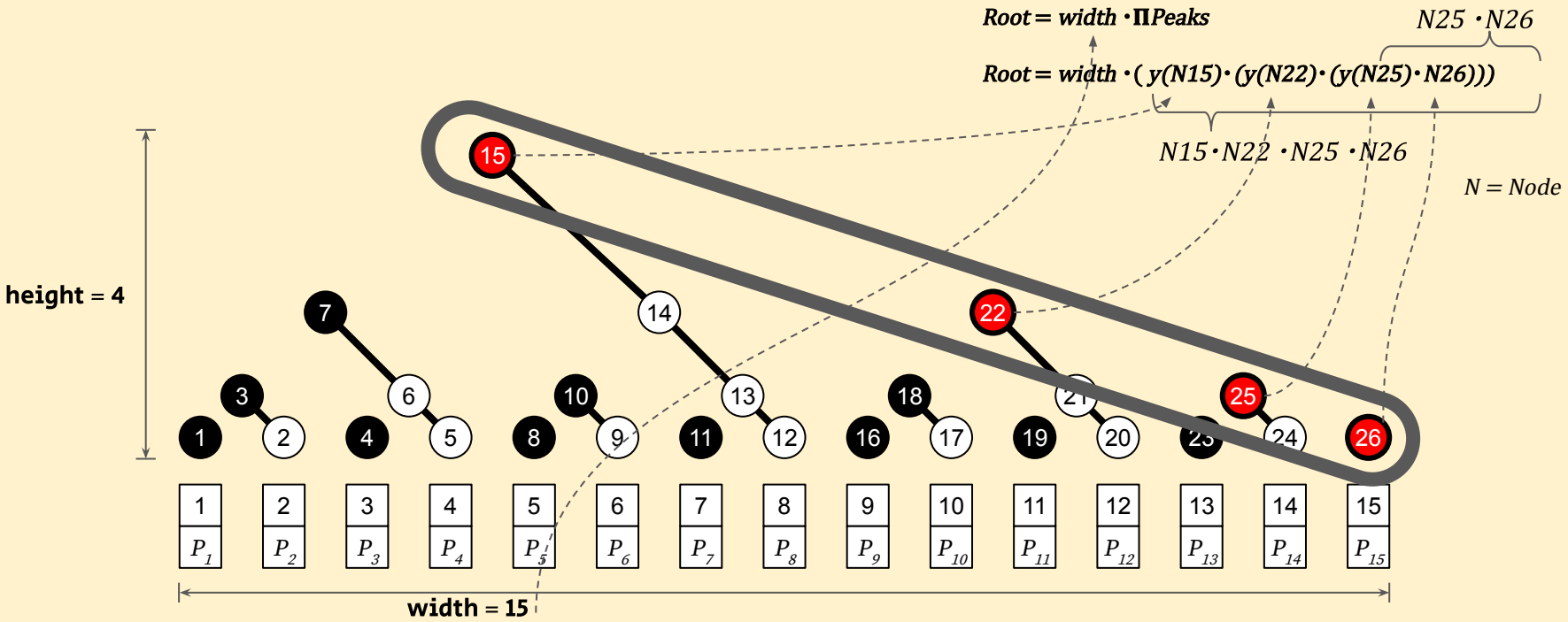
Pedersen Merkle Mountain Range - Leaf node



Pedersen Merkle Mountain Range - Branch node



Pedersen Merkle Mountain Range - Root



Proof for challenge

Tested with 3GHz 8 core CPU(Ryzen 1700) & 32Gb DDR4 RAM

	Constraints	Gas consumption	Proof generation(sec)
Deposit proof	29,140	612,273	3 s
Withdraw proof	588,910	658,043	3.5 s
Range proof	19,679	568,232	2 s
MMR Inclusion Proof	399,644	613,809	24 s
Mimblewimble Proof	141,552	975,399	9 s
MMR Roll up 8 items (4 txs)	1,614,383	1,392,269	1m 47s
MMR Roll up 16 items (8 txs)	2,906,951	2,127,267	3m 19s
MMR Roll up 32 items (16 txs)	5,492,087	3,597,531	7m 20s
MMR Roll up 64 items (32 txs)	**10,662,359**	6,541,946	17m 30s

Optimistic roll up

```
function rollUp(
        Tx[] memory txs,
        uint root,
        uint newRoot,
        uint[] proof
) internal {
        verifyTxWithZkSNARKs(txs, proof);
        ...
}
```

Optimistic roll up

```
function optimisticRollUp(
        Tx[] memory txs,
        uint root,
        uint newRoot,
        uint[] proof
) internal {
        // verifyTxWithZkSNARKs(txs, proof);
        save(keccak256(msg.data), RollUp(txs, proof));
        ...
}
```

Optimistic roll up (in Petersburg)

	Gas(Avg)	Gas per tx	Maximum TPS
oll up t	3,859,179		0.17 tx/sec
2 tx	6,645,227	3,322,613	0.20 tx/sec
16	49	15	4. tx/ c
Optimistic roll up 32 tx	4,694,516	146,703	4.53 tx/sec

Istanbul
50,000 gas / tx

Possibility of DAO & Defi

1. Anyone can be a relayer!
2. Relayers can get transaction fee using Mimblewimble protocol
3. Relayers can set their own tx fee policy.
4. Proof of Stake is needed for the optimistic roll up.
5. Proof of Stake + Tx Fee = DAO & De-Fi?

Future works

1. Optimization
2. Relayer client (in progress)
3. Mobile client (in progress)
4. Goblins' network
    a. Relayer's network to provide the instant finalization
5. Destroying the horcruxes

Summary

Mimblewimble transaction & commitment-nullifier
: Easy to implement on zk SNARKs. Totally hides where inputs come from

Pedersen Merkle Mountain Range
: Enables efficient roll up. It is able to append up to 256(Istanbul) items at once.

Optimistic Roll up
: Fraud proof without DA problems. It reduces gas cost down to 50k gas per transaction in Istanbul. (Standard ERC20: 50k ~ 100k gas per transaction)

Repositories

Ethereum 9¾ Repository:
https://github.com/ethereum934/eth-mimblewimble

Technical details:
https://ethresear.ch/t/ethereum-9-send-erc20-privately-using-mimblewimble-and-zk-snarks/6217

And... just like Grin

THANK YOU