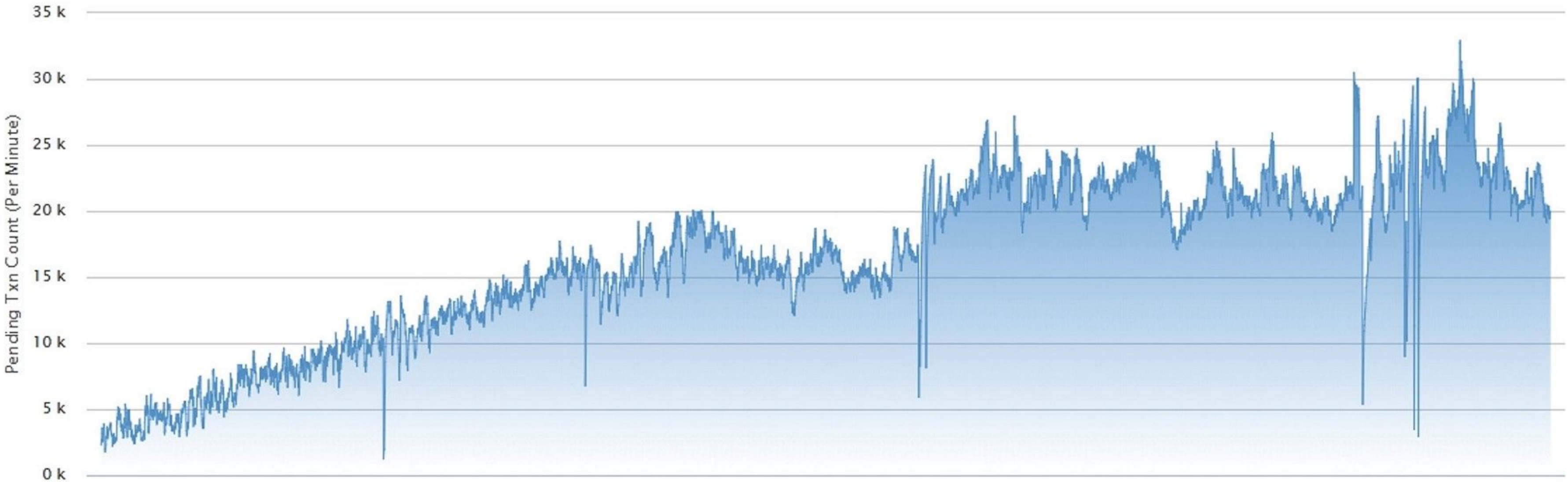
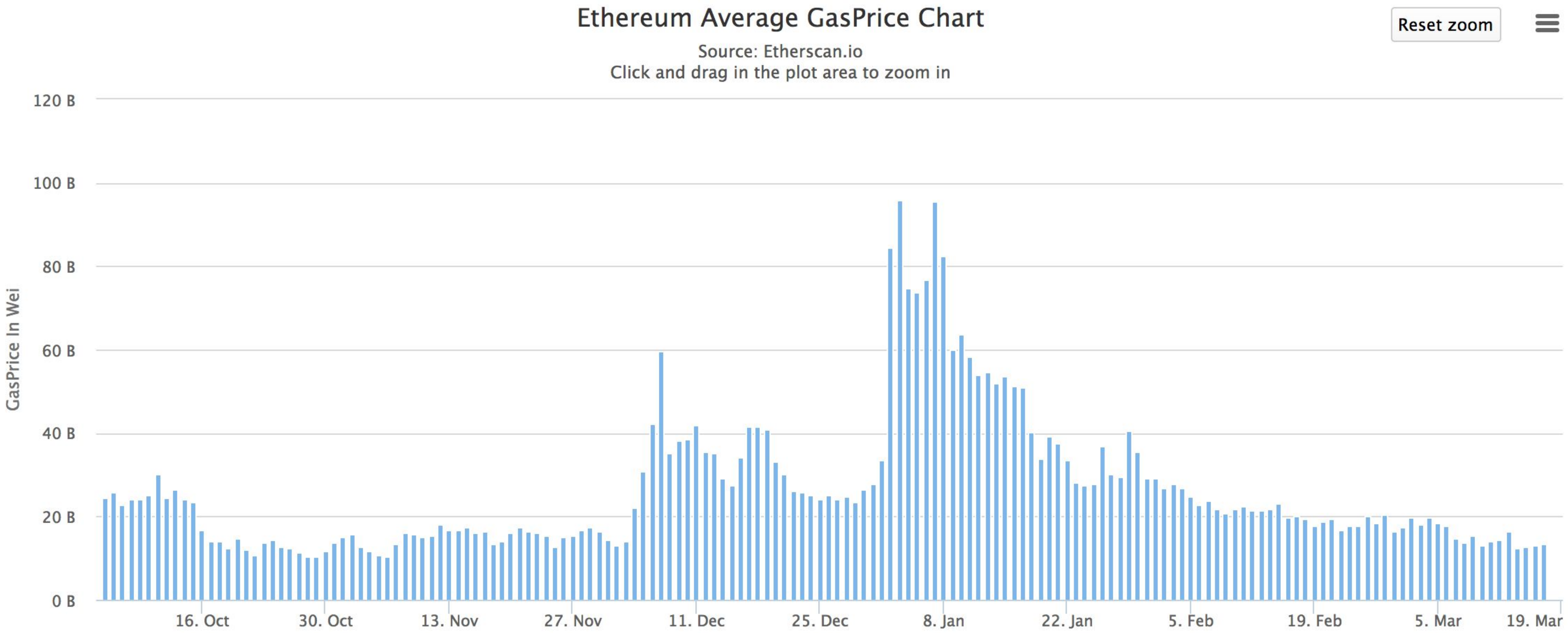
GOMETH

a sidechain experiment
@codecontext



Ethereum Pending Transactions Queue - Time Series

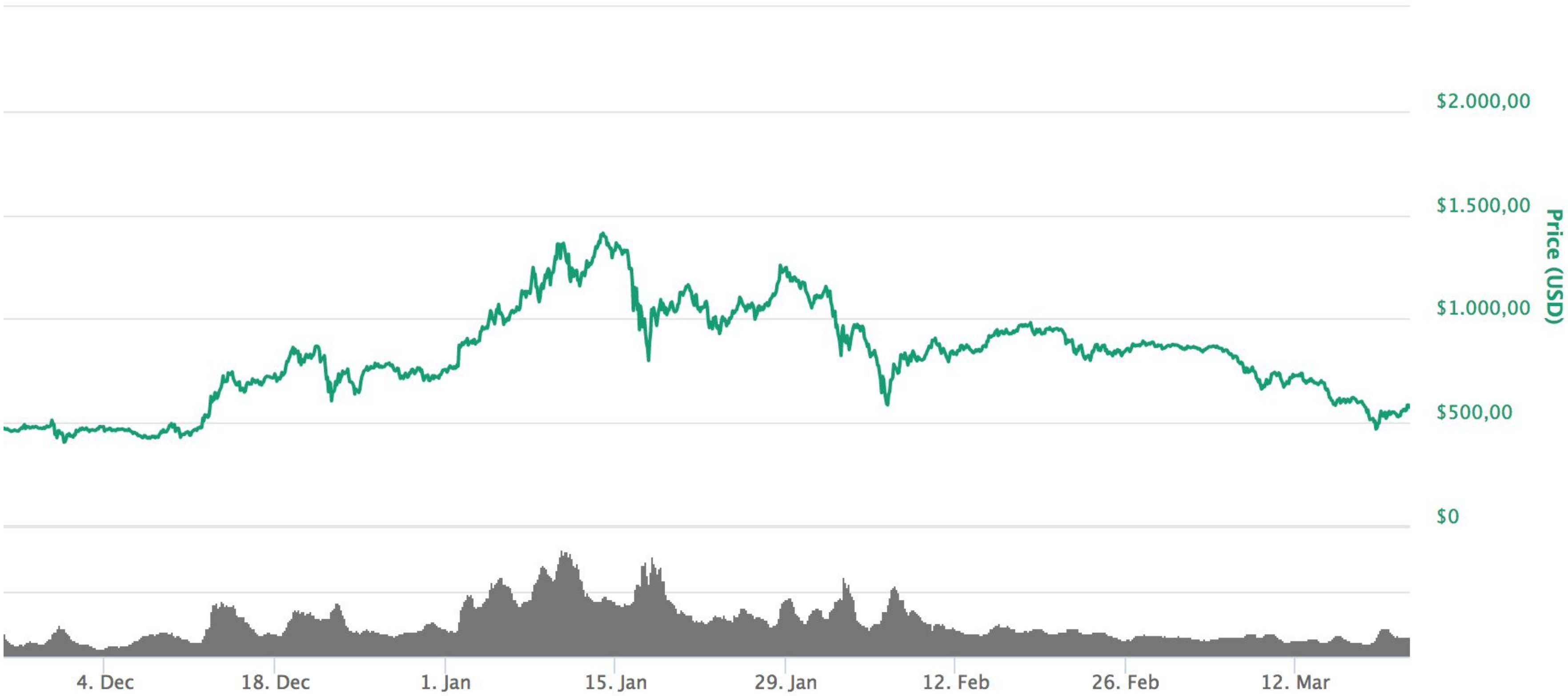
Source: Etherscan.io
(From 12/3/2017 to 12/7/2017)
Click and drag in the plot area to zoom in

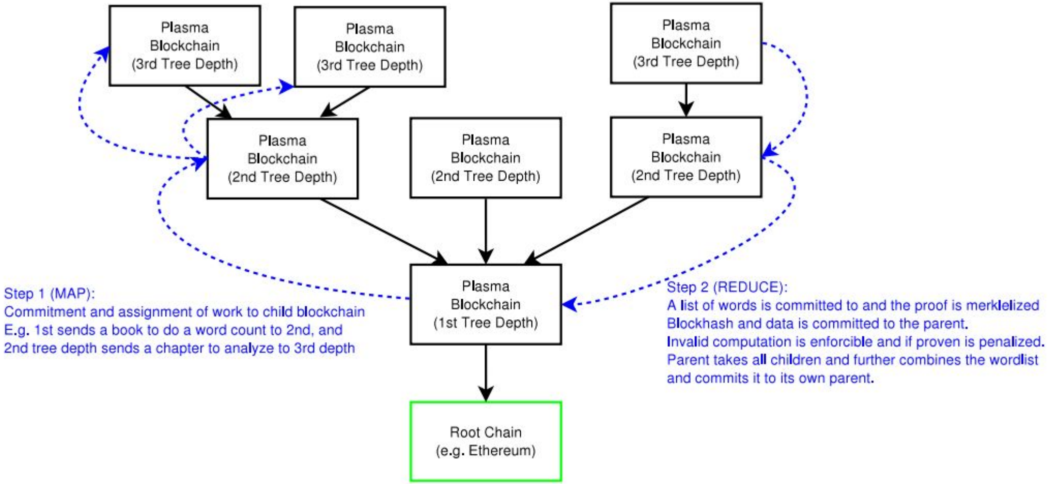


Ethereum Average GasPrice Chart

Source: Etherscan.io

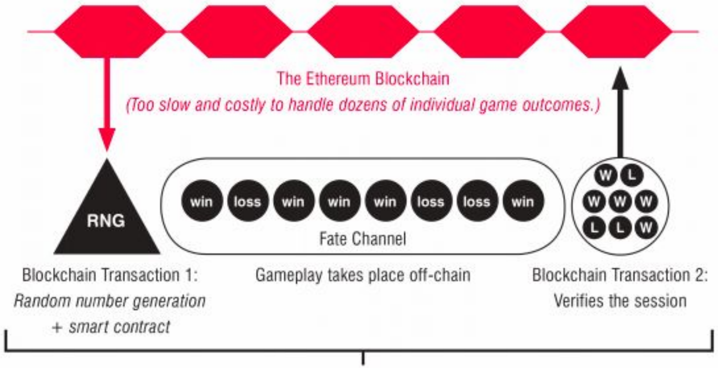
Click and drag in the plot area to zoom in


$2.000,00
$1.500,00
$1.000,00
$500,00
$0
Price (USD)
4. Dec
18. Dec
1. Jan
15. Jan
29. Jan
12. Feb
26. Feb
12. Mar


Plasma Blockchain (3rd Tree Depth)
Plasma Blockchain (3rd Tree Depth)
Plasma Blockchain (3rd Tree Depth)
Plasma Blockchain (2nd Tree Depth)
Plasma Blockchain (2nd Tree Depth)
Plasma Blockchain (2nd Tree Depth)
Plasma Blockchain (1st Tree Depth)
Root Chain (e.g. Ethereum)

Step 1 (MAP):
Commitment and assignment of work to child blockchain
E.g. 1st sends a book to do a word count to 2nd, and
2nd tree depth sends a chapter to analyze to 3rd depth

Step 2 (REDUCE):
A list of words is committed to and the proof is merklelized
Blockhash and data is committed to the parent.
Invalid computation is enforcible and if proven is penalized.
Parent takes all children and further combines the wordlist
and commits it to its own parent.

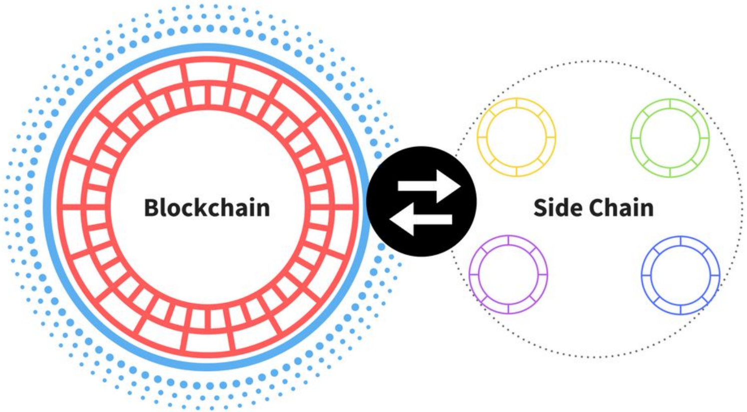


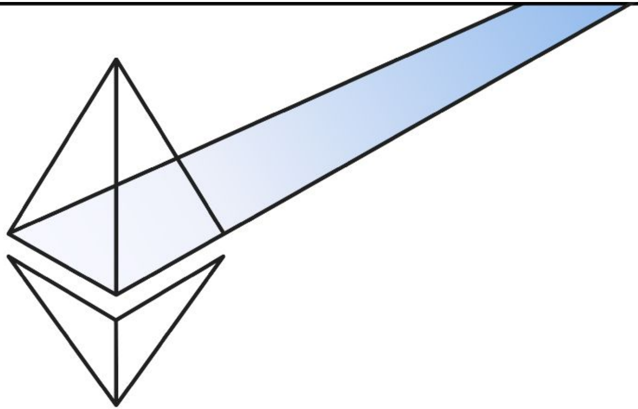
Blockchain Transaction 1:
Random number generation
+ smart contract

Gameplay takes place off-chain

Blockchain Transaction 2:
Verifies the session

Fate Channel:
Just 2 blockchain transactions





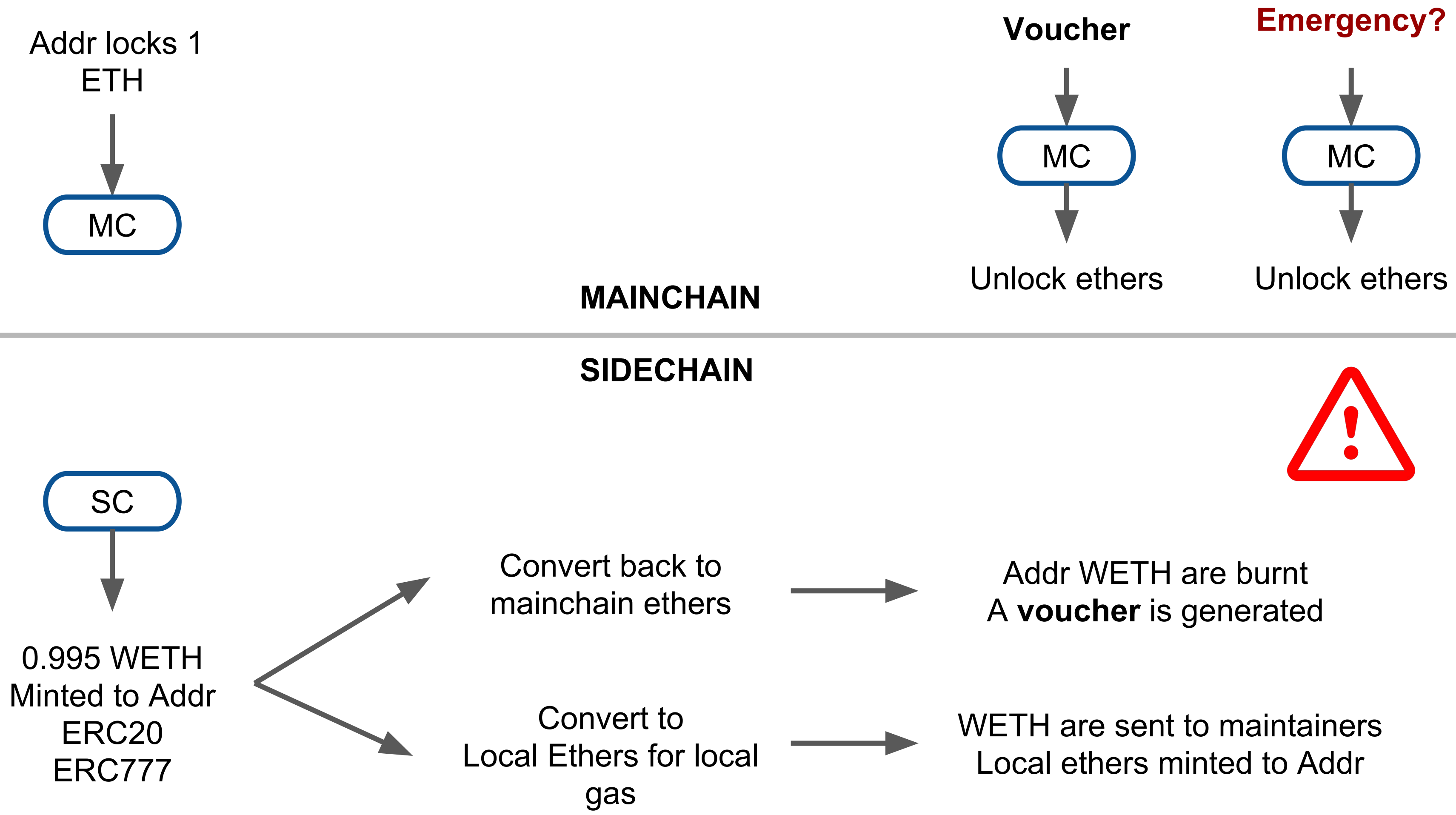
ScalingNOW!

Reviewing Scaling Solutions for Ethereum DApps

28 videos in https://goo.gl/QwZLzw

WEB3

GiVETH



Addr locks 1 ETH

MC

Voucher

MC

Unlock ethers

Emergency?

MC

Unlock ethers

MAINCHAIN

SIDECHAIN

SC

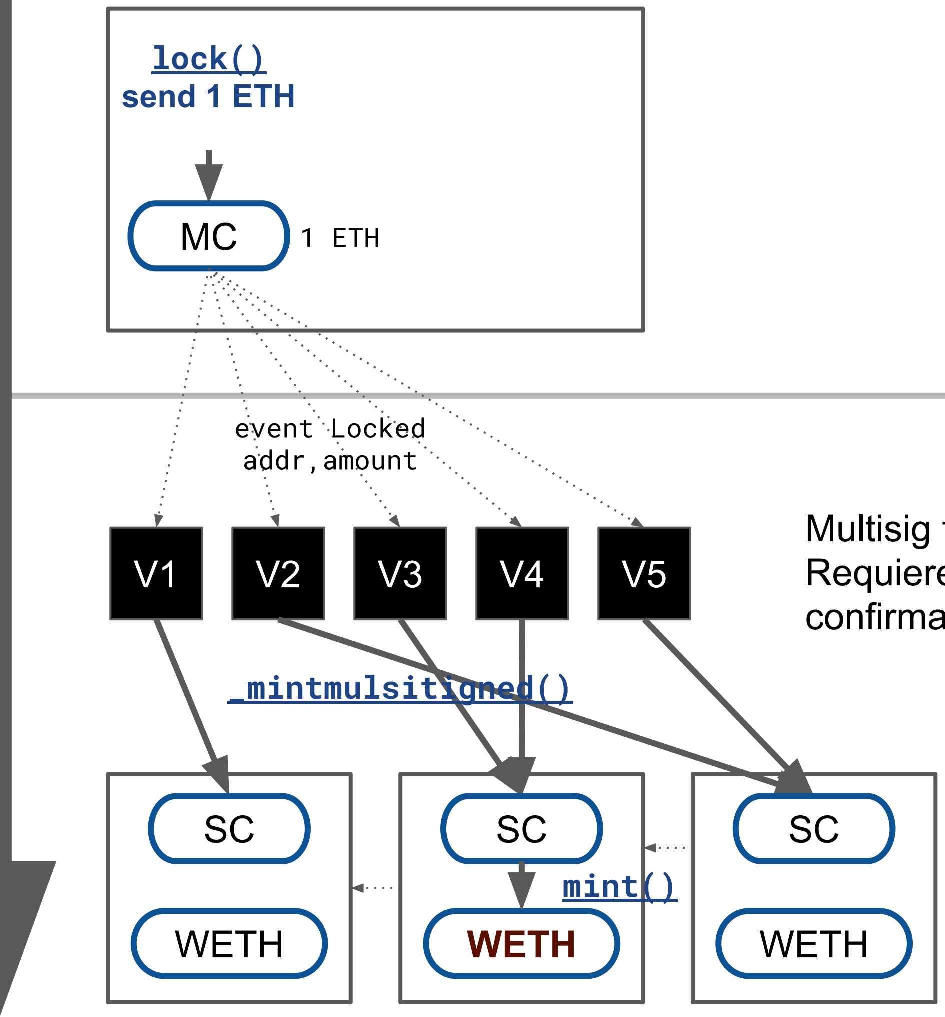
0.995 WETH
Minted to Addr
ERC20
ERC777

Convert back to mainchain ethers

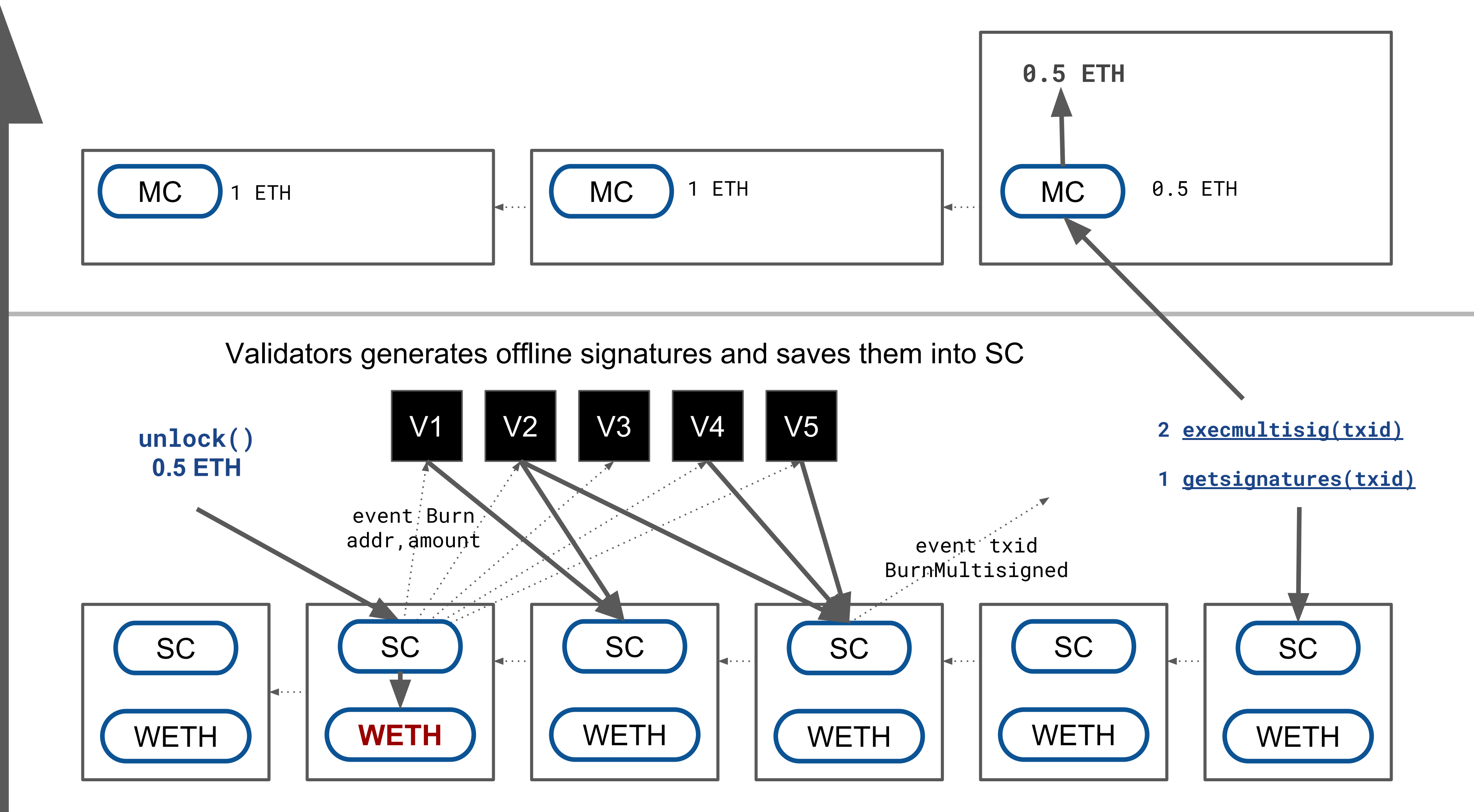
Addr WETH are burnt
A **voucher** is generated

Convert to
Local Ethers for local gas

WETH are sent to maintainers
Local ethers minted to Addr

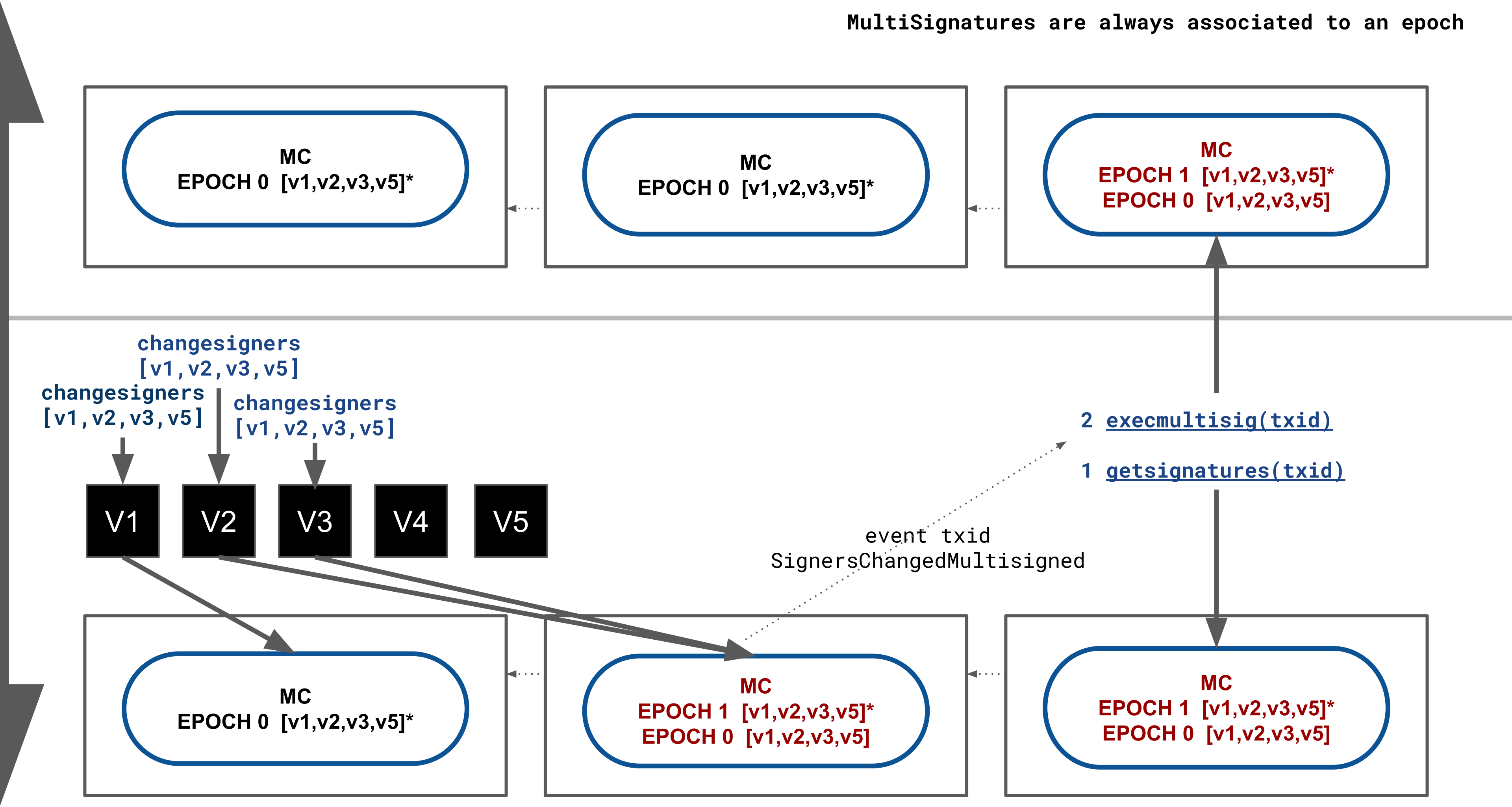


Multisig transaction
Requieres ⅔
confirmations



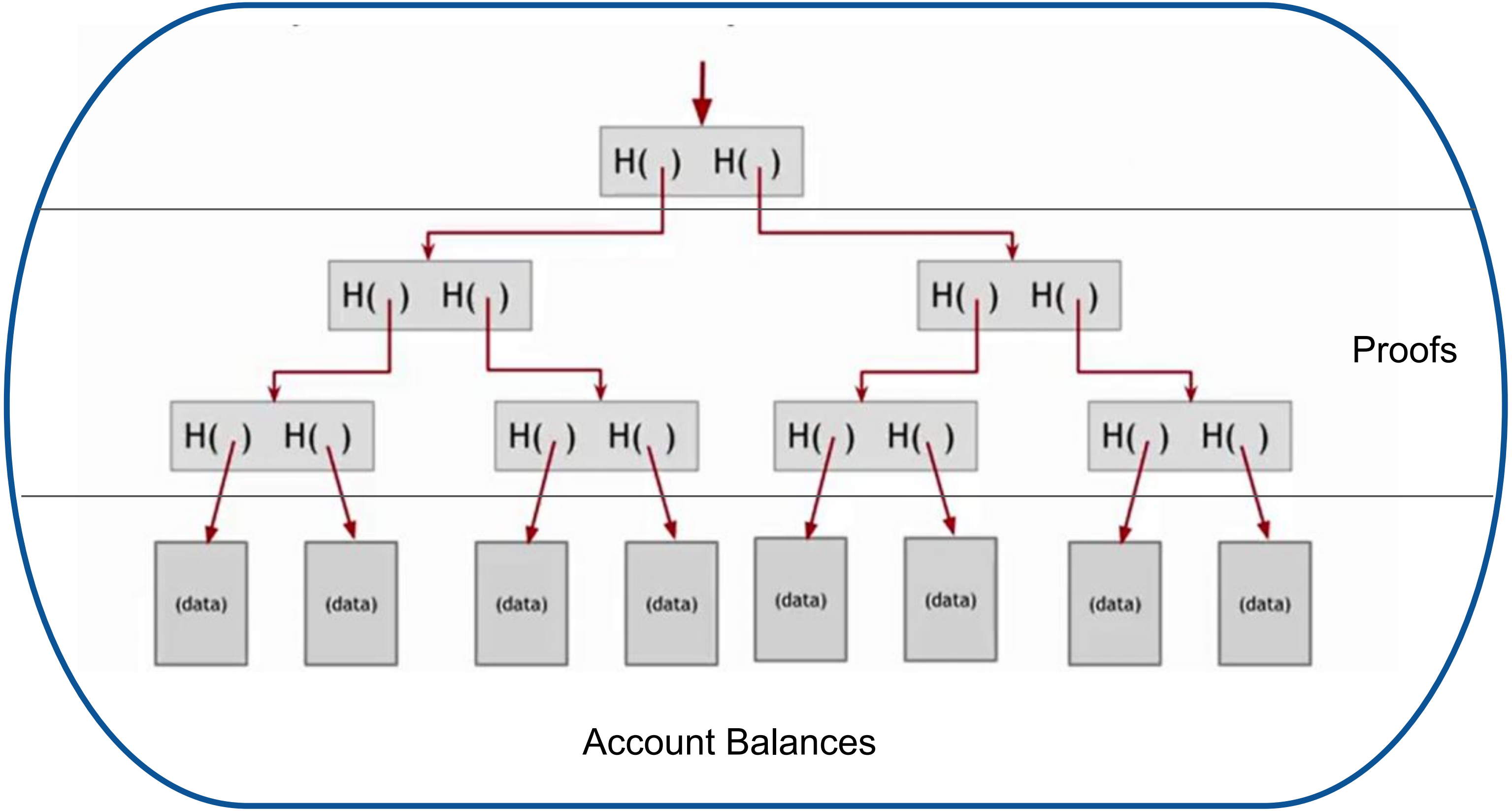
MC
1 ETH
MC
1 ETH
0.5 ETH
MC
0.5 ETH
Validators generates offline signatures and saves them into SC
unlock()
0.5 ETH
V1
V2
V3
V4
V5
event Burn
addr,amount
event txid
BurnMultisigned
2 execmultisig(txid)
1 getsignatures(txid)
SC
WETH
SC
WETH
SC
WETH
SC
WETH
SC
WETH
SC
WETH

MultiSignatures are always associated to an epoch



WETH

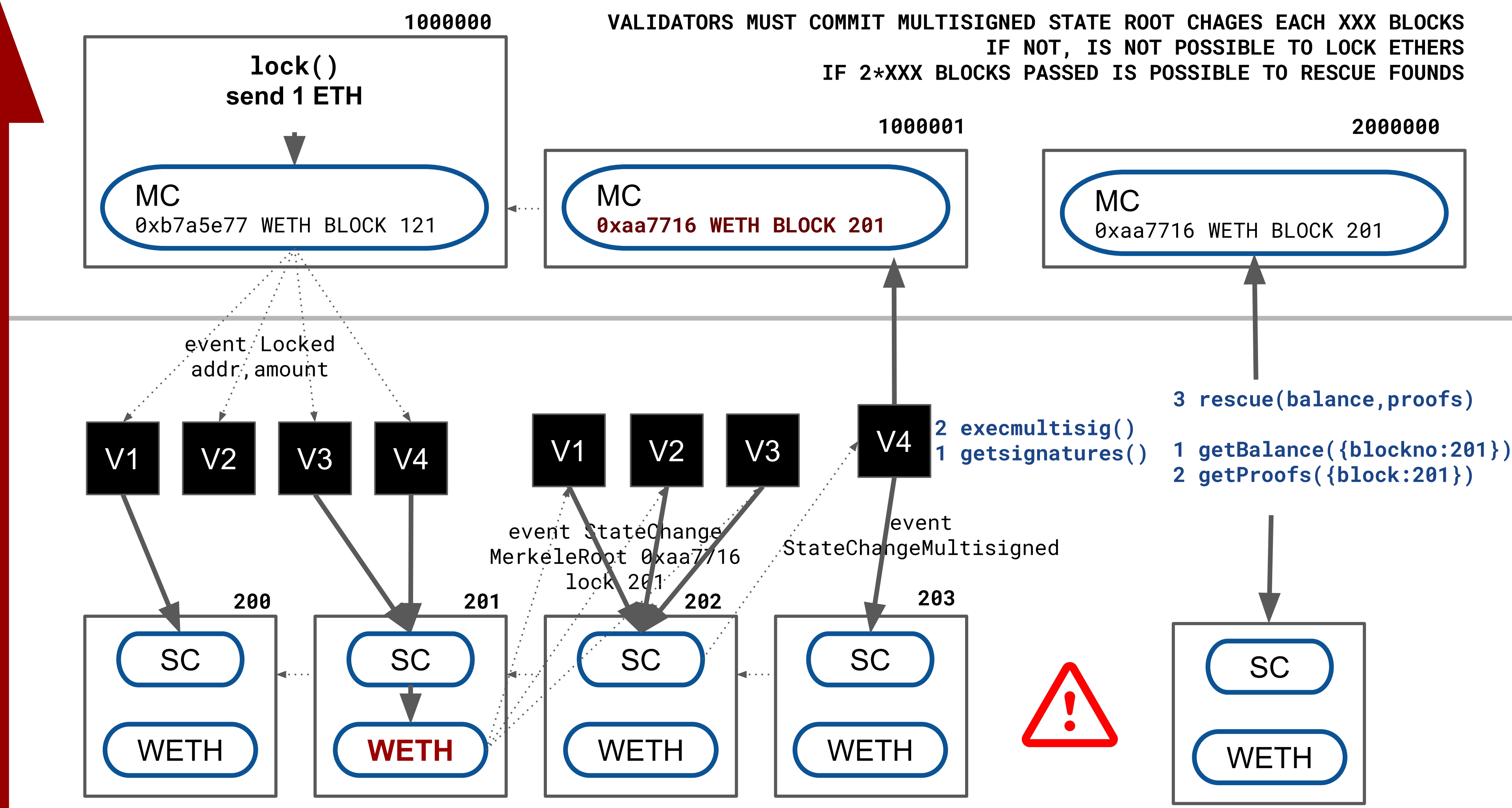
Root hash multi signed by validators



Proofs

Account Balances

VALIDATORS MUST COMMIT MULTISIGNED STATE ROOT CHAGES EACH XXX BLOCKS
IF NOT, IS NOT POSSIBLE TO LOCK ETHERS
IF 2*XXX BLOCKS PASSED IS POSSIBLE TO RESCUE FOUNDS



A multisig that also manages offchain signatures with historic set of signers
https://github.com/adriamb/gometh-contracts/blob/master/contracts/OfflineMultisig.sol

The mainchain and sidechain contracts
https://github.com/adriamb/gometh-contracts/blob/master/contracts/GomethMain.sol
https://github.com/adriamb/gometh-contracts/blob/master/contracts/GomethSide.sol

Patricia tree implementation by Christian Reitwiessner
https://github.com/adriamb/gometh-contracts/blob/master/contracts/PatriciaTree.sol

Wrapped ether ERC20 (ERC777 comming, uses OpenZeppelin)
https://github.com/adriamb/gometh-contracts/blob/master/contracts/WETH.sol

Golang server
https://github.com/adriamb/gometh-server

Next steps

- Add more tests
- Prepare for real use cases
  - Golang async handling of transactions/receipts
  - Kafka for handling events/transactions
  - Multisig support for “alias address” to send concurrent transactions with different addresses
- Alternatives to global settlement
  - WETH balances has also tx count, is possible to proof that lock() operation is not done when committing the WETH root when using signed state root & merkle proofs
- PoA stuff
  - Automatic update PoA authorities on events (geth clique)
- PoS stuff
  - Validators stake slashing conditions