bitfwd

Demystifying The Ethereum World Computer

bitfwd

About Me

- Vincent
- Head of Tech @ bitfwd

- Twitter: @vncnttrn
- Linkedin: /in/vncnttrn

bitfwd

bitfwd telegram

- Join our telegram!

https://t.me/bitfwd

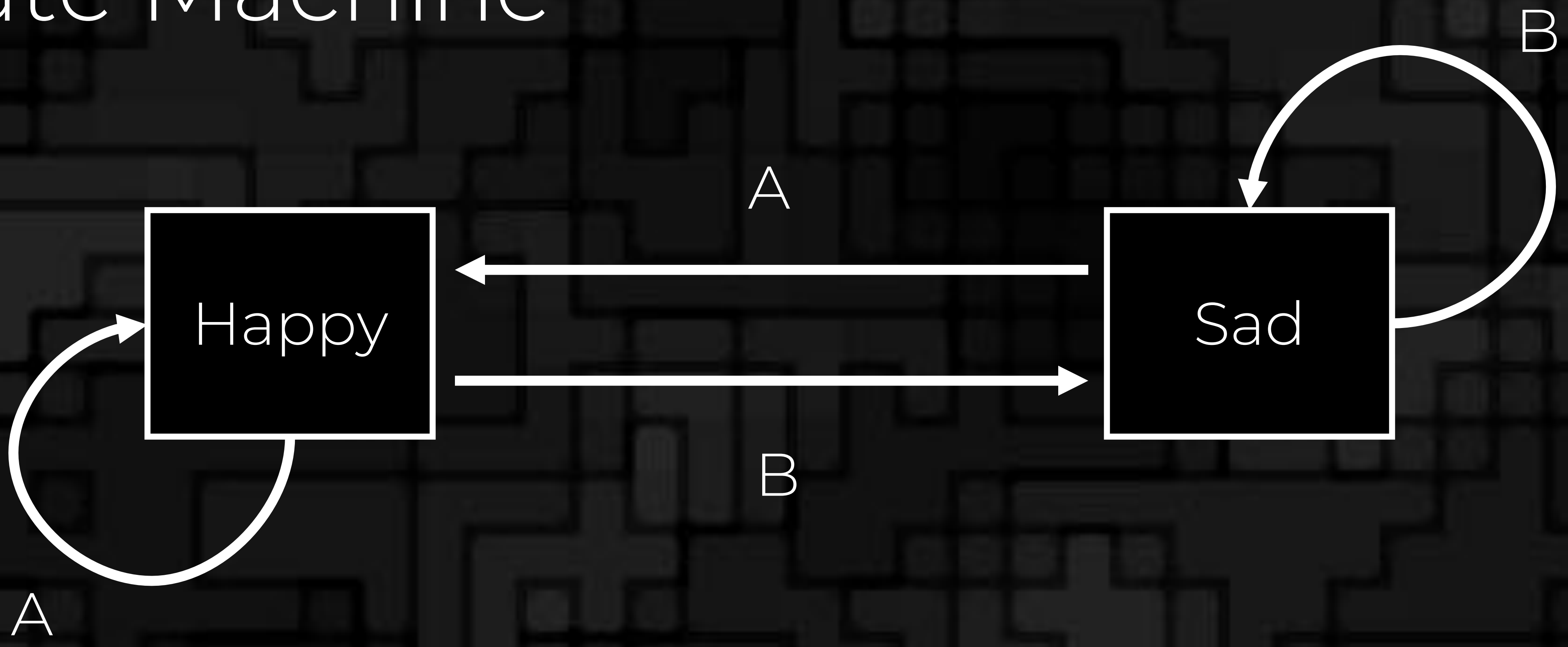
bitfwd

Blockchain

Blockchain

- Cryptographically secure
- A single instance of the machine responsible for all transactions in the system.
- The state that this machine stores is shared and open.

State Machine



Ethereum

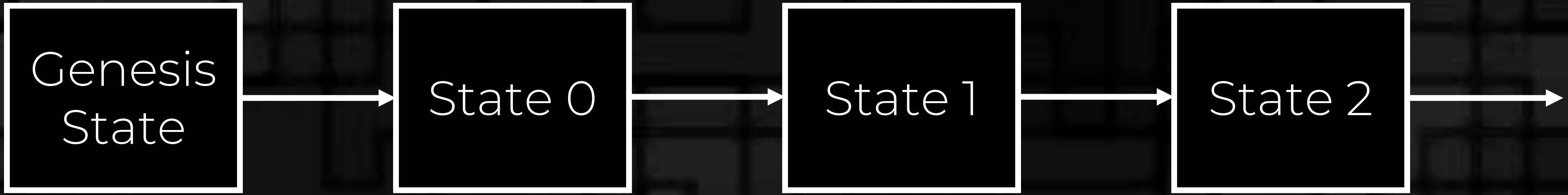
- State Machine.
- Triggered by transactions.
- Transactions must be valid to trigger a state transition.

bitfwd

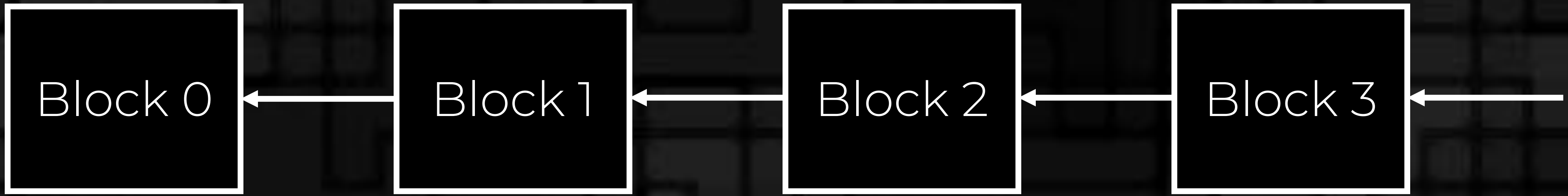
Ethereum

- Began with a “genesis state” or block.
- Ethereum had a coin offering, so these balances were encoded in the state.
- State transitions continue based on transactions.
- State transitions propagate forward, you cannot transition to a previous state.

State Machine I



State Machine II



bitfwd

Ethereum

- Transactions force a state transition when validated.
- Miners compete to validate (like in Bitcoin).
- Miners are rewarded Ethers for their work.
- Forks occur just like in Bitcoin, resolved in a similar way.

Ethereum vs. Bitcoin

	Ethereum	Bitcoin
Block Time	~15 seconds	~10 minutes
Block Reward	3 ETH, down from 5	12.5 BTC
Adjustment	Never, until PoS	Every 4 years.
Uncle Reward	7/8 of block reward	No reward
Difficulty	Per block	Per 2 weeks.

Check out stats on ethstats.net

Uncles?

- Bitcoin -> Orphan
- Ethereum’s block times are short.
- Encourage solo mining by rewarding blocks that are included as uncles.
- Miner including uncle is also rewarded 1/32 ETH per uncle (max 2).

bitfwd

Accounts

Accounts

- Ethereum state has many “accounts” which interact with each other via transactions/messages.
- Each account has a state and a 20 byte address.
  - E.g. 0x5e55aFde2E20b2547E052466A97f4EcDF11381A1
- Two types of accounts: contract account + externally owned account.

Externally Owned Accounts

- Can send transactions to other EOA.
  - Transaction to EOA is value transfer.
- Can send transactions to contract.
  - Transaction to contract activates code.
- Requires signature by private key.

bitfwd

Contract Accounts

- Can only respond to other messages.
- Can make calls to other contracts.

Nonce

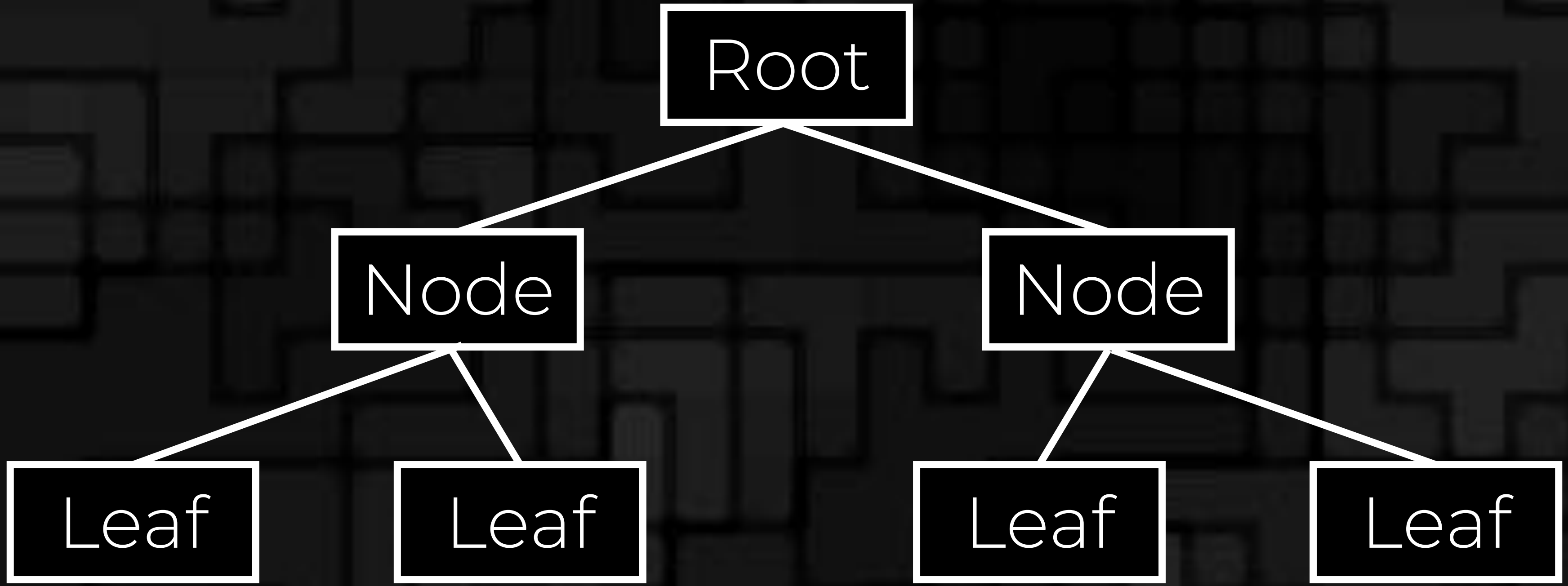
- Prevents double spending.
- Incrementing nonce.

Hash Function

- Unique number generator.
- Easy to compute going forward.
- Hard to compute going backwards.

KECCAK-256(‘hello0’) = ‘ee12c92f437d27fa1773b76e46274dcd440943065a2be5ec279abb2cea20aceb’

Merkle Tree



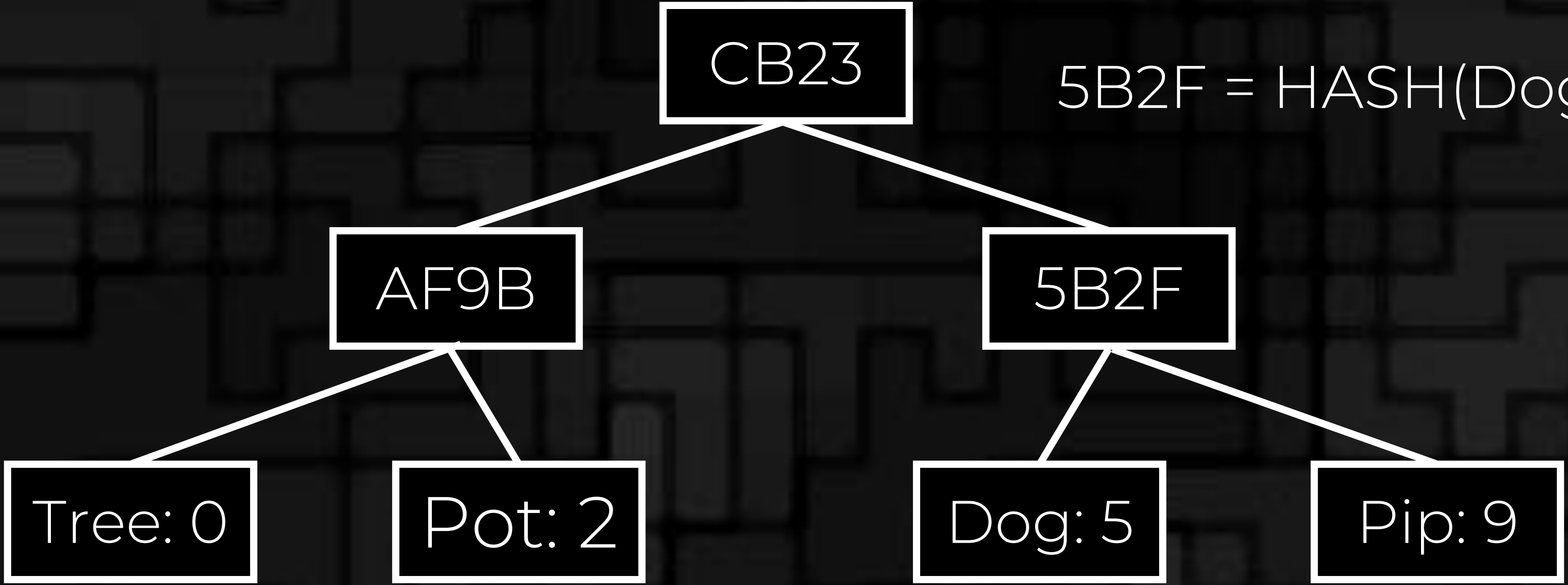
Merkle Tree

- Block header stores hash of the root node of three different Merkle trees.
- State, Transaction & Receipts.

Nodes

- Archive: full node, downloads everything from genesis to the current, executing each transaction. Takes ages.
- Light: instead of downloading and executing full chain/tx’s, downloads only list of chain headers, from genesis block to current head.

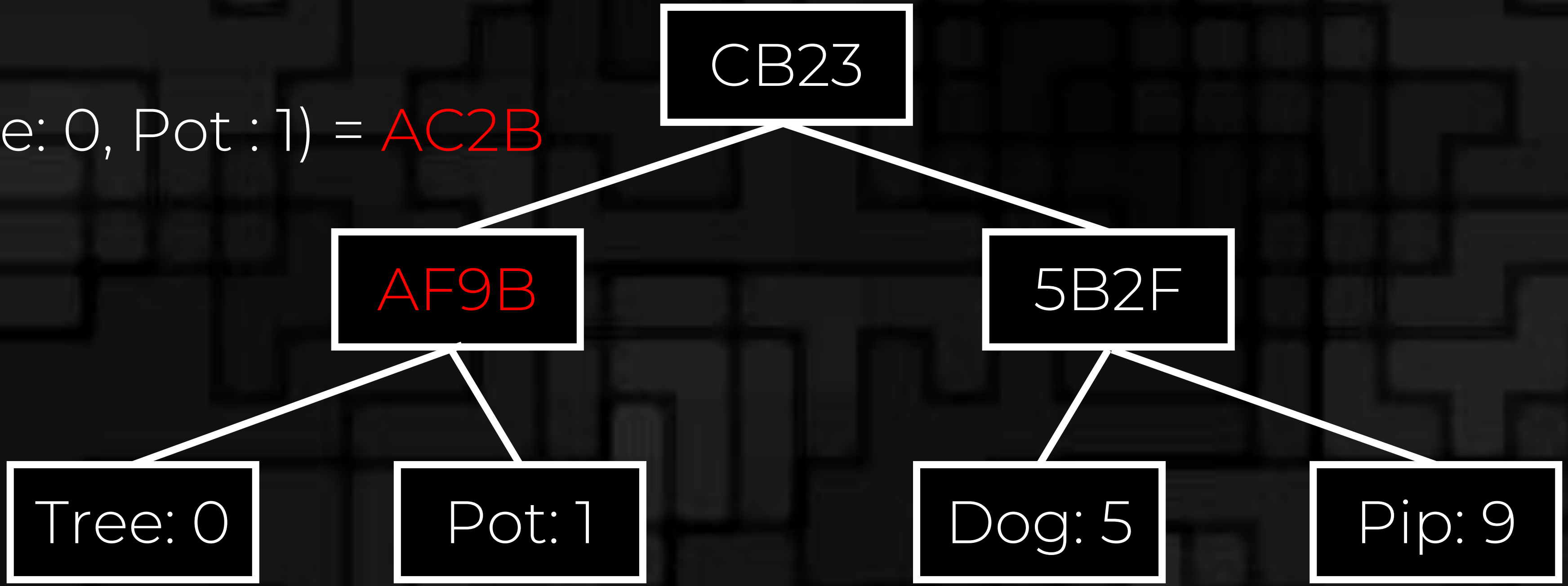
Merkle Tree: Intuition I



5B2F = HASH(Dog: 5, Pip: 9)

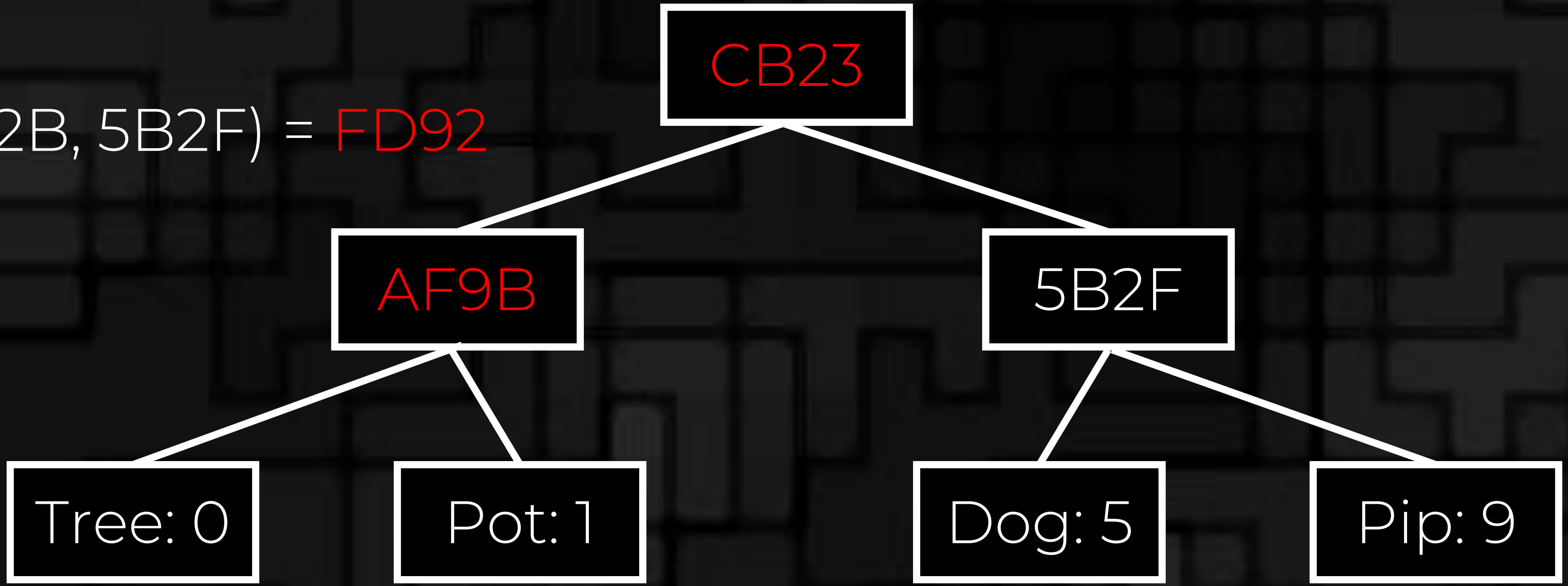
Merkle Tree: Intuition II

Hash(Tree: 0, Pot : 1) = AC2B



Merkle Tree: Intuition III

Hash(AC2B, 5B2F) = FD92



CB23

AF9B

5B2F

Tree: 0

Pot: 1

Dog: 5

Pip: 9

Gas

Gas

- Gas is used to pay for computational power.
- Gas is the unit used to measure amount of fees required per computation.
- Gas price is the amount of Ether you are willing to spend.
- Gas price denominated in gwei (i.e. 1 000 000 000 Wei)

myetherwallet.com/helpers.html // ethgasstation.info

Gas

- Gas Limit: maximum amount of gas you are willing to pay for a tx.

Gas Limit: 21000 * Gas Price: 50 gwei = Cost: 0.00105 ETH

Gas

- Gas is also used to pay for storage.
- Fees exist to prevent DDoS attacks.
- Inadequate pricing of specific operations led to DDoS attack in 2016.

bitfwd

Transactions & Messages

Transactions

- Cryptographically signed instruction generated by an EOA.
- Transactions are how we access the Ethereum network from the outside.
- Contracts talk to each other using “messages”

Messages

- Messages allow contracts to call other contracts in a chain.
- Do not contain gasLimit.
- These are not directly included in the blockchain.

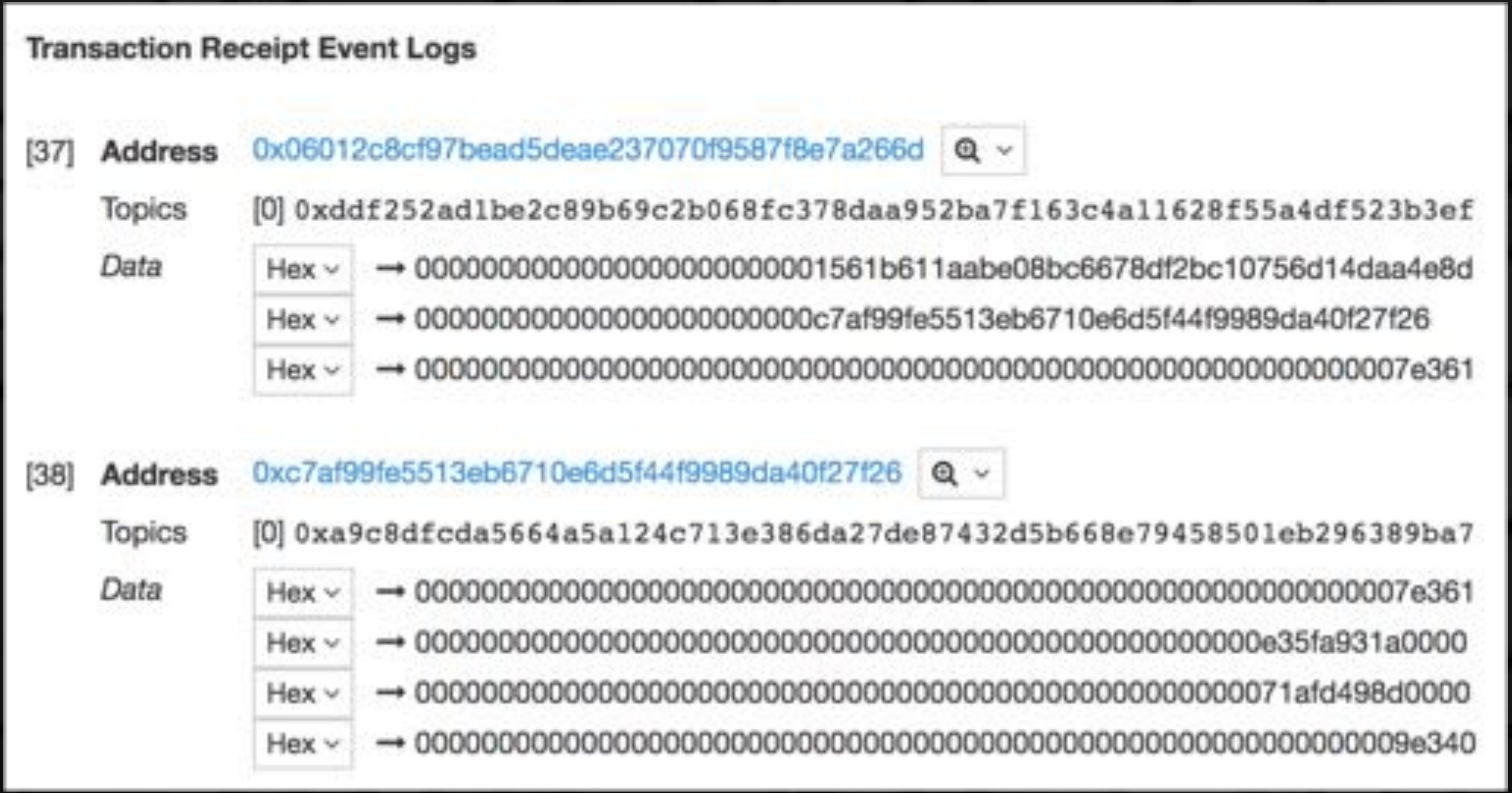
bitfwd

Blocks

Logs

- Allows tracking of various transactions.
- Logs contain
  - Logger address
  - Topics defined by the contract
  - Data associated with these events.

Logs



Transaction Receipt Event Logs

```
[37] Address  0x06012c8cf97bead5deae237070f9587f8e7a266d
     Topics   [0] 0xddf252ad1be2c89b69c2b068fc378daa952ba7f163c4a11628f55a4df523b3ef
     Data     Hex → 0000000000000000000000001561b611aabe08bc6678df2bc10756d14daa4e8d
              Hex → 000000000000000000000000c7af99fe5513eb6710e6d5f44f9989da40f27f26
              Hex → 000000000000000000000000000000000000000000000000000000000007e361

[38] Address  0xc7af99fe5513eb6710e6d5f44f9989da40f27f26
     Topics   [0] 0xa9c8dfcda5664a5a124c713e386da27de87432d5b668e79458501eb296389ba7
     Data     Hex → 000000000000000000000000000000000000000000000000000000000007e361
              Hex → 000000000000000000000000000000000000000000000000000e35fa931a0000
              Hex → 00000000000000000000000000000000000000000000000000071afd498d0000
              Hex → 000000000000000000000000000000000000000000000000000000000009e340
```

Transaction Execution I

Requirements

- Transaction must be formatted correctly (using RLP encoding).
- Transaction signature must be valid.
- Transaction nonce must be valid.
- Gas limit has to be high enough.
- Sender’s balance has to be high enough to pay the gas costs.

Transaction Execution II

Then:

- Deduct upfront cost of execution from sender’s balance.
- Increment sender’s account nonce by 1.
- Calculate gas remaining by subtracting amount used from gas limit.

Transaction Execution III

Begin execution:

- Computations are processed.
- If no invalid state, state is finalized.
- Gas is refunded.

bitfwd

Developing On Ethereum

bitfwd

Tools

IDE: web based IDE remix.ethereum.org, client
Testnets: Ropsten/Rinkeby/Kovan/Ganache
Testing Wallets: Use myetherwallet.com/mycrypto.com/metamask browser extension
Ropsten Faucet: ropsten.bitfwd.xyz
Frameworks: Truffle/Dapple etc.
Remember: interfacing is super important

Getting Started

bitfwd community tutorials on how to deploy your own token contract

- Play with cryptokitties.co (will teach you how metamask works)
- Try to interact with token contracts and send transactions through MEW.
- Write custom contracts/play with them on remix.ethereum.org
- https://github.com/bitfwdcommunity/bitfwd-exercises

bitfwd

Questions