

# PRACTICAL PLASMA: GAMING





# WHY GAMES ON BLOCKCHAIN

- » Real Ownership of Assets
- » Forkability
- » Open Data
- » Play run servers

# NEW WAY TO MONETIZE APPLICATIONS





# **HISTORY COUNTERPARTY - XCP**

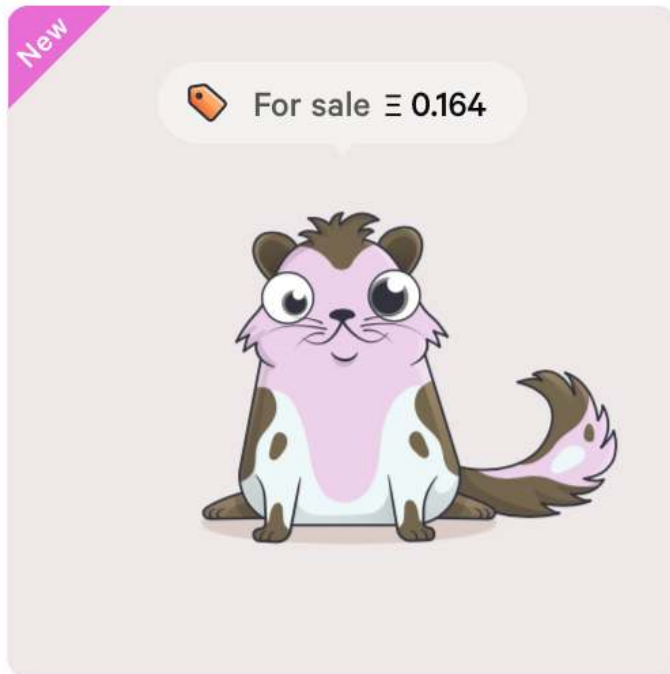
# ETHEREUM

» ERC721

» Smart contracts

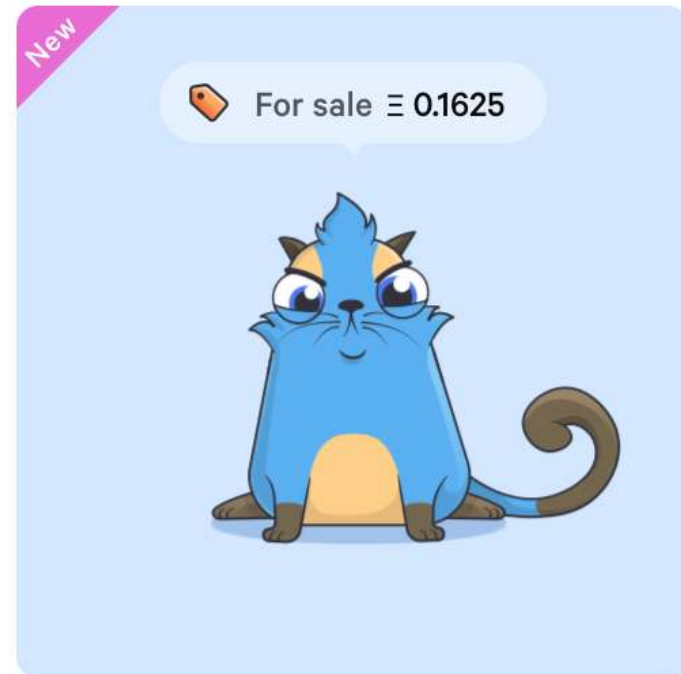


**BEFORE ...**



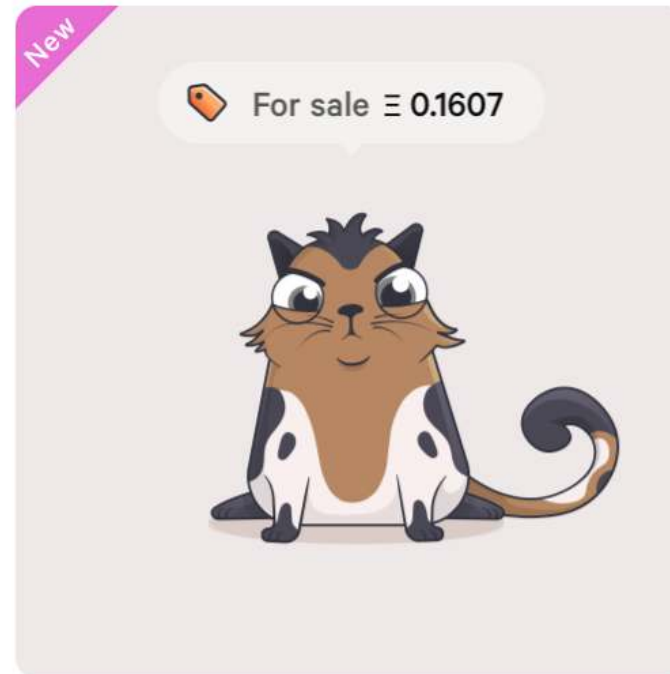
#870646 · Gen 0 · Fast

♡ 0



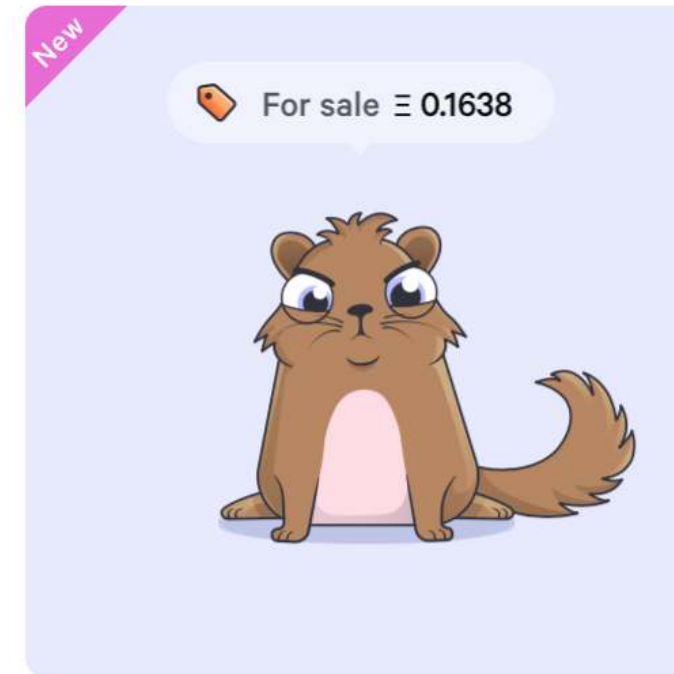
#870616 · Gen 0 · Fast

♡ 0



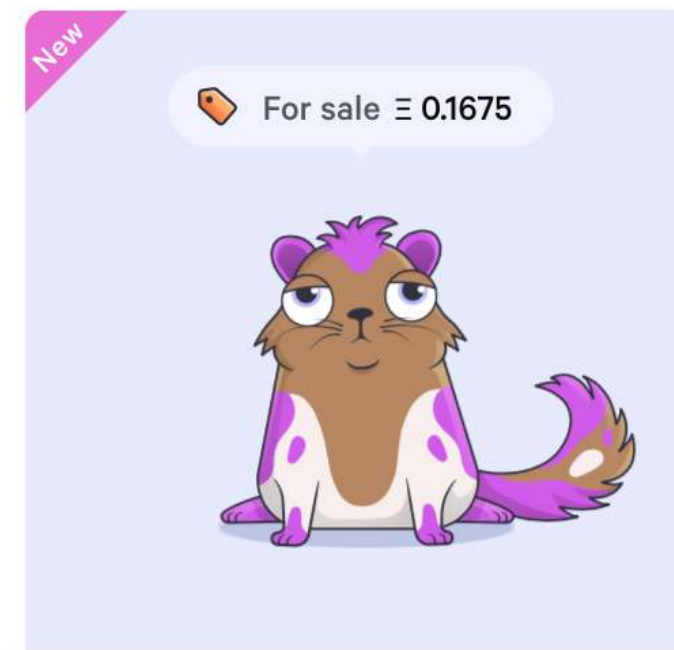
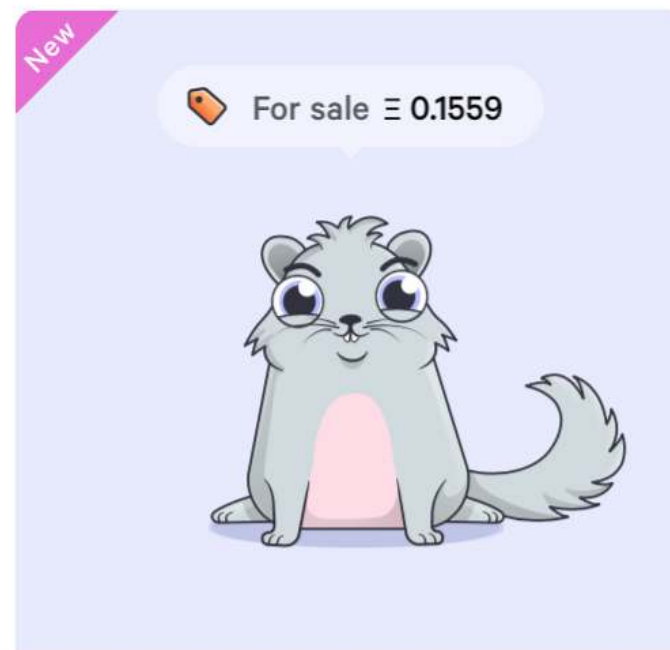
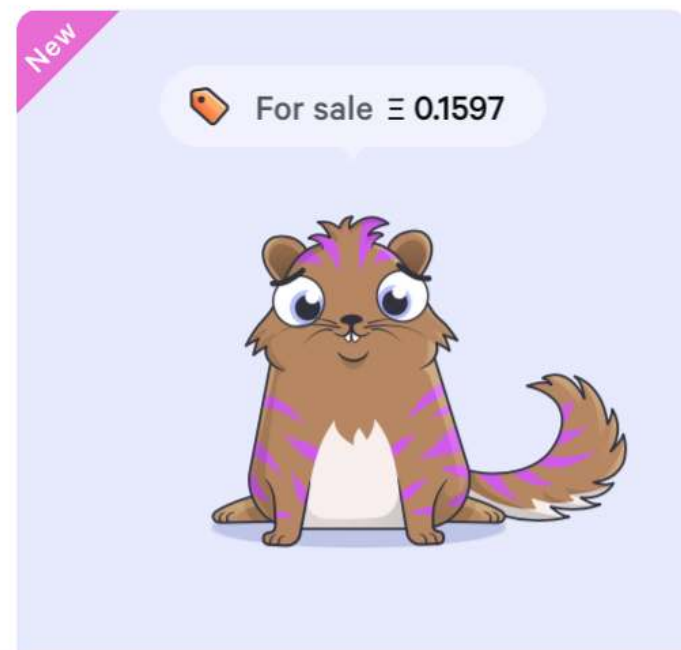
#870569 · Gen 0 · Fast

♡ 0



#870540 · Gen 0 · Fast

♡ 0



# NON FUNGIBLE TOKENS



# PROOF OF WORK CHAINS

# DPOS

Delegated Proof of Stake

**NOW...**





# 2 MILLION CARDS MINTED





# PROBLEM

Securing Assets



# ENTER PLASMA



# 30 SECONDS ABOUT ME

- » Founder Loom Network
- » DigitalOcean
- » Go Developer 5 years
- » Spoken all over the world
- » Rode an elephant at my wedding
- » ชอบพูดไทยเวลาเมา



# WHAT WAS PLASMA



# WHAT IS PLASMA NOW

1. Introduced by Buterin & Poon, 2017
2. Scalability solution for Ethereum via sidechains
3. Multiple off-chain state updates which can be realized on-chain
4. Plasma Chain → Sidechain that interacts with a “Plasma Contract”
5. Plasma Contract → Notifies the Plasma Chain of actions
6. Merkleized block roots get submitted to the Plasma

# PLASMA VARIANTS

- » Plasma Cash
- » Plasma Debit
- » Plasma MVP

**PLASMA CASH IS THE REAL  
PLASMA**

# VITALIK REACHED OUT

[/u/vbuterin](#)

Reaching Out:

[expand all](#) [collapse all](#)

[–] from [/u/vbuterin](#) sent 5 months ago

Hi! Vitalik here.

I'd be happy to chat more, and introduce you to Thomas and Jun (OmiseGo) who are in Bangkok at least some of the time. What's your email? Alternatively feel free to reach out to 

[Permalink](#) [Delete](#) [Report](#) [Block User](#) [Mark Unread](#) [Reply](#)

[–] to [/u/vbuterin](#) sent 5 months ago

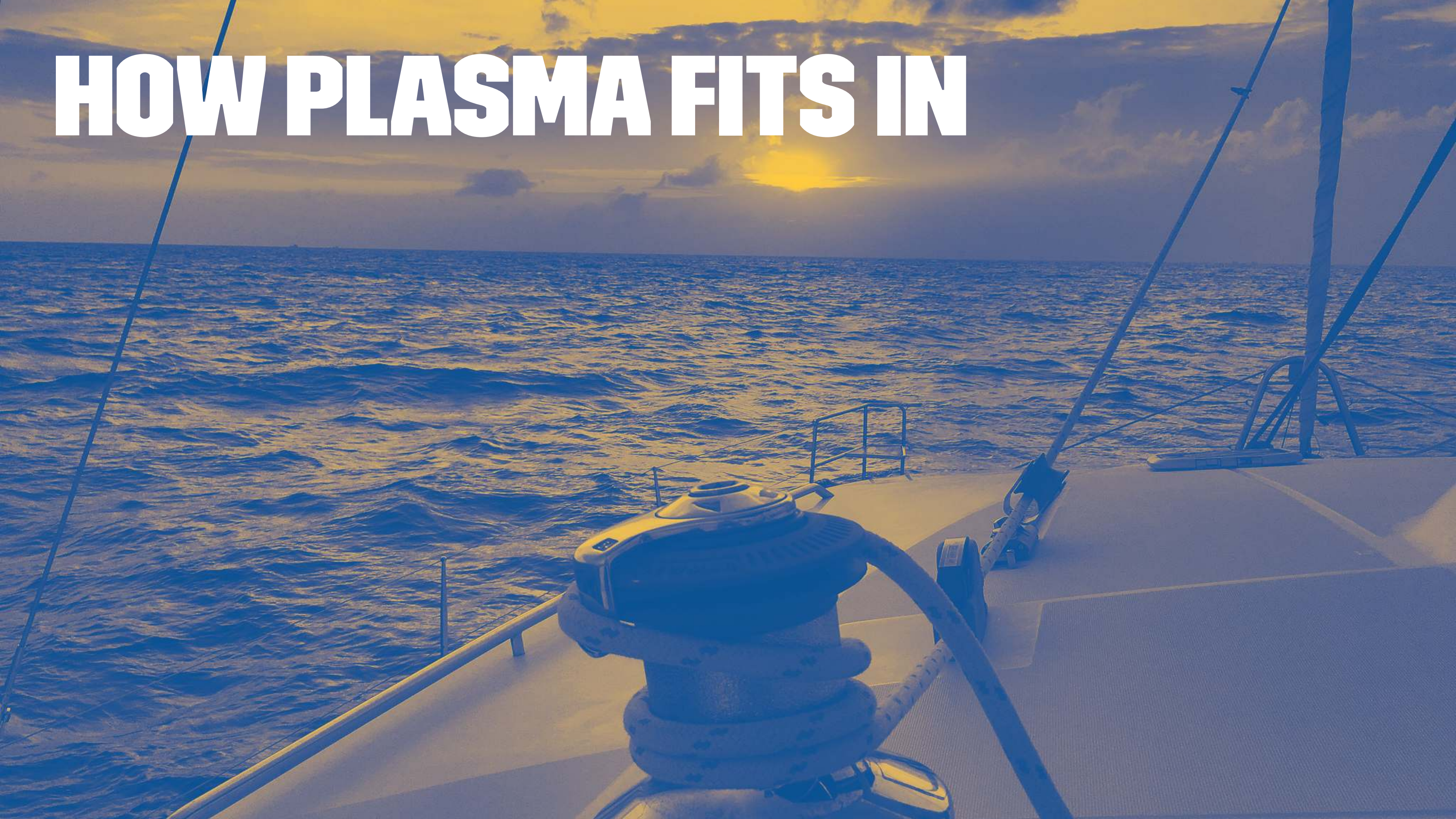
Sure would love to chat [matt@loomx.io](mailto:matt@loomx.io) . I would like to see how plasma could fit into dAppChain tech

[Permalink](#)



# WHAT IS LOOM SDK

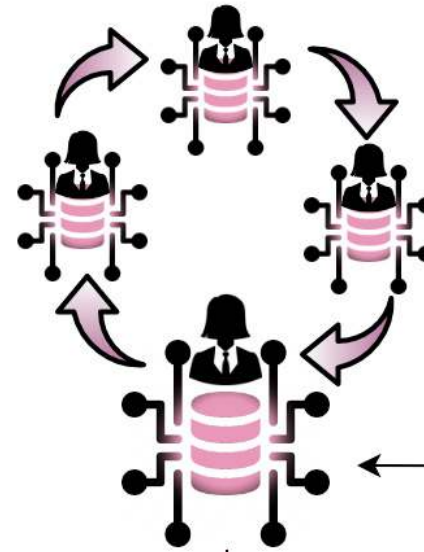
# HOW PLASMA FITS IN



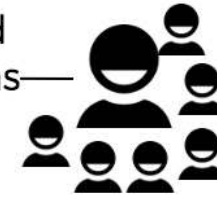
# PoS Plasma Cash

Block Proposers rotate regularly

Block Proposers



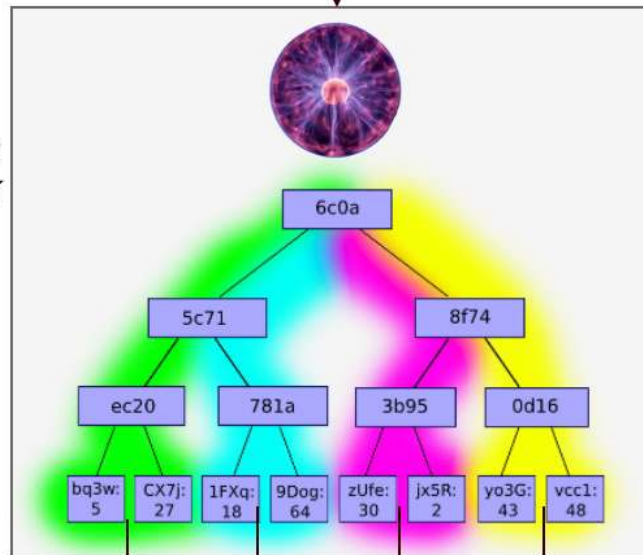
Users send transactions



Users

Create New Large Block

Plasma Cash Block



Proof of Stake Validators



Propagate to users to ensure availability



Users

Sign off on availability & validity

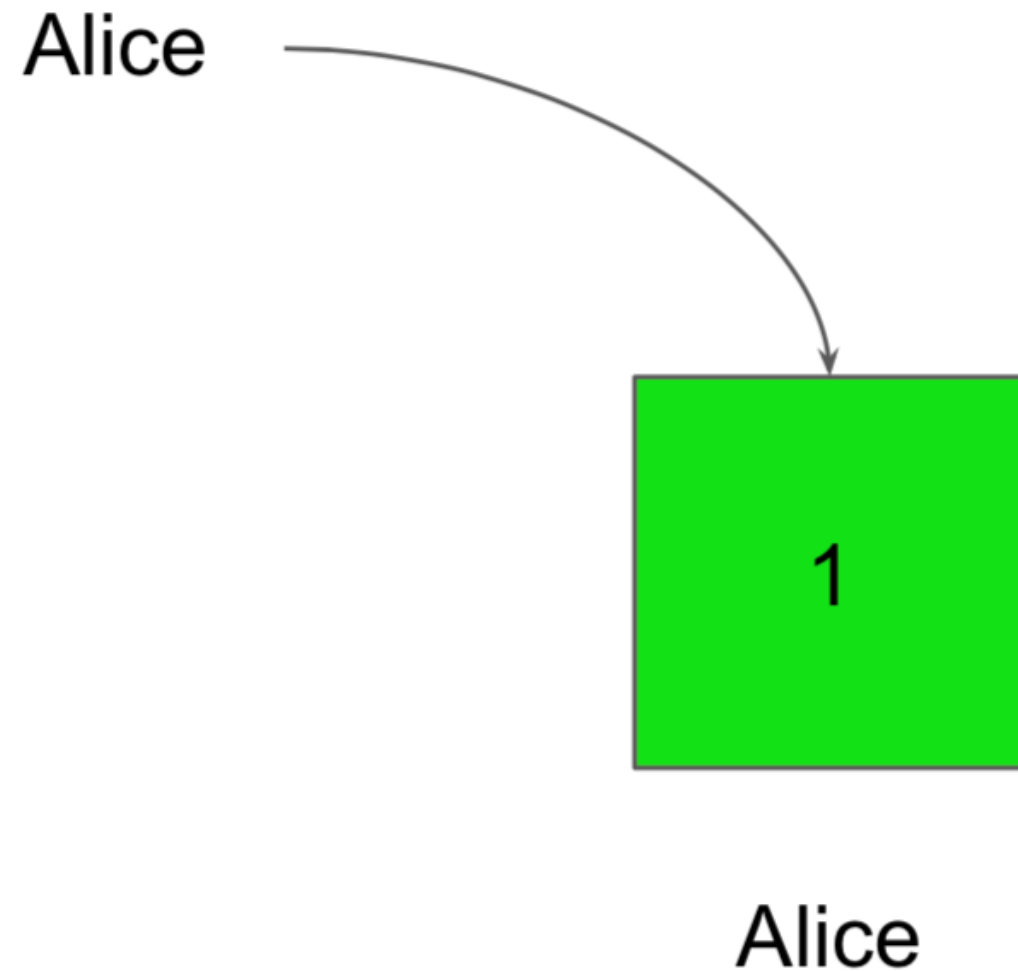
Ethereum Root Chain



Merkle Root and validation signature included in Plasma contract

# Example of Coin History (Deposit 5 ETH)

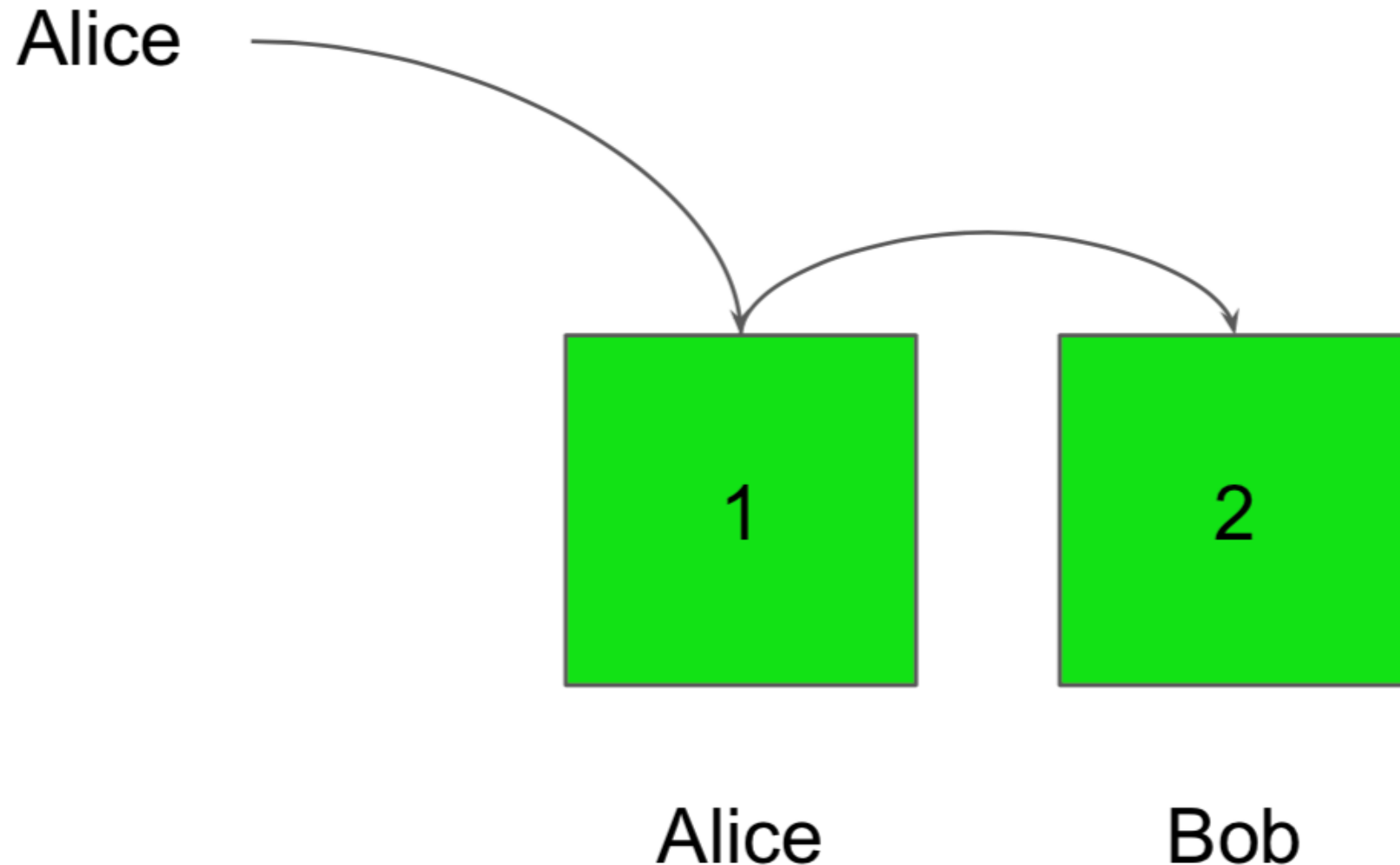
Deposit 5 ETH on Plasma Contract, 5 ETH appears on Plasma “from nowhere”



# Example of Coin History (Deposit 5 ETH)

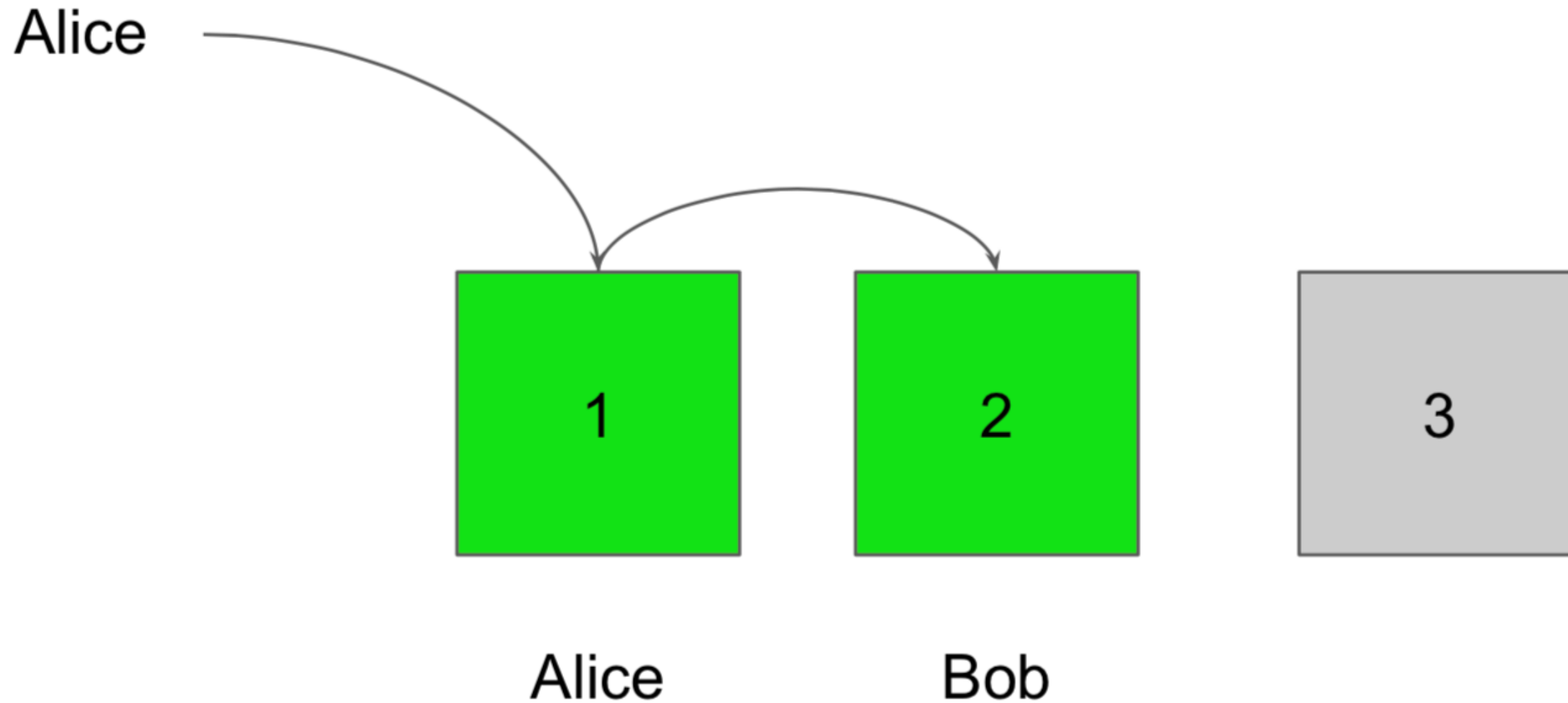
Alice sends coin to Bob + inclusion proof in Block 1.

**Bob must verify that the coin is valid.**



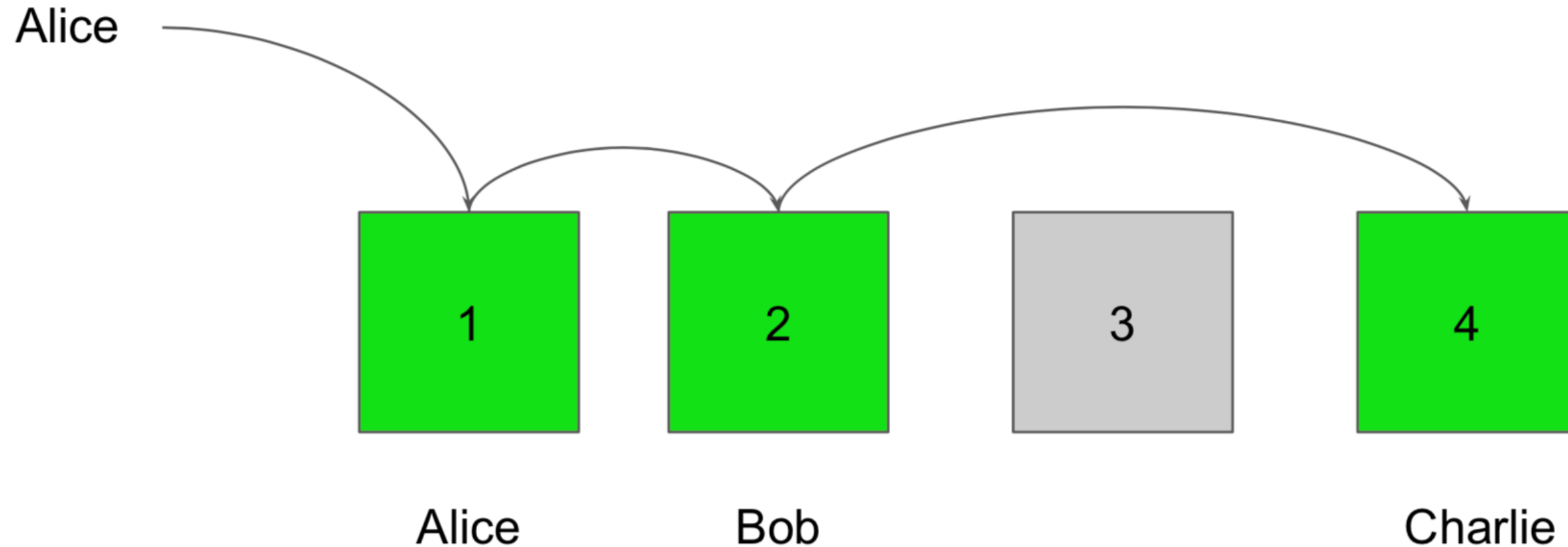
# Example of Coin History (Deposit 5 ETH)

Block 3 gets submitted, the coin was not moved.



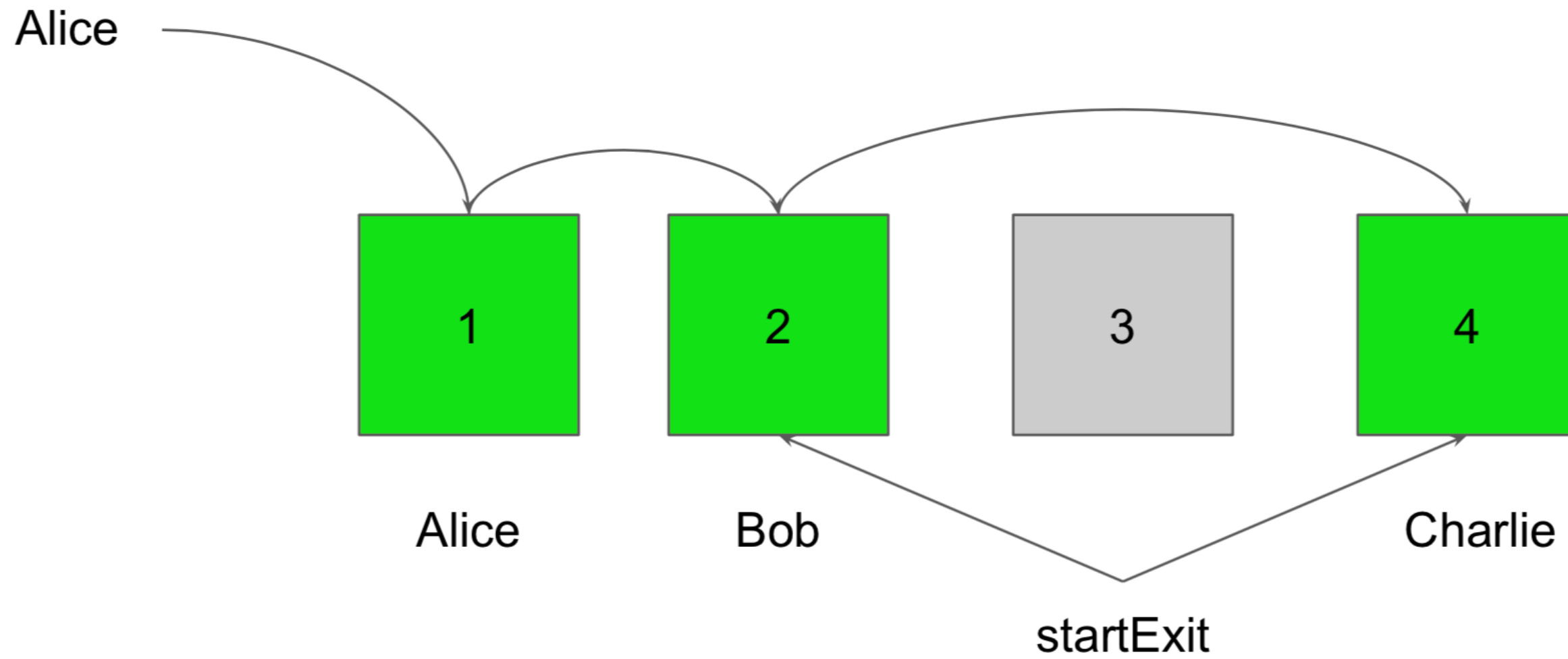
# Example of Coin History (Deposit 5 ETH)

Bob sends the coin to Charlie: Inclusion in blocks 1,2 & exclusion in block 3  
**Charlie must verify that the coin is valid.**



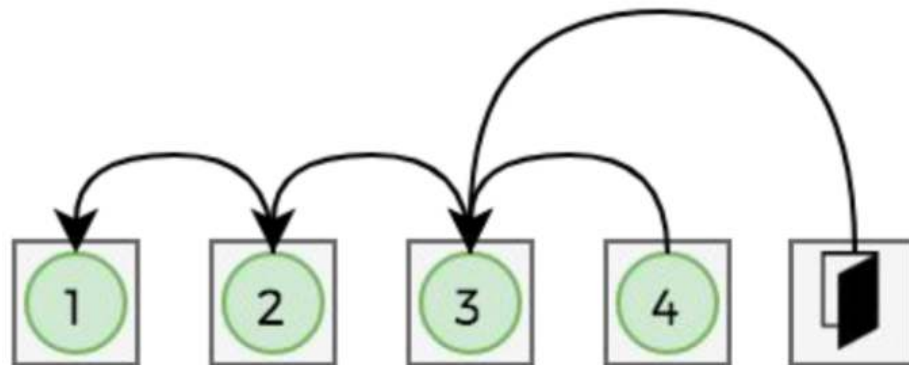
# Example of Coin History (Deposit 5 ETH)

Charlie verifies that the coin was valid. He then exits it by referencing an ancestor



# Challenges

## Exit Spent Coin Challenge



Ethereum block



Valid spend



Invalid spend



Double spend



Exit tx

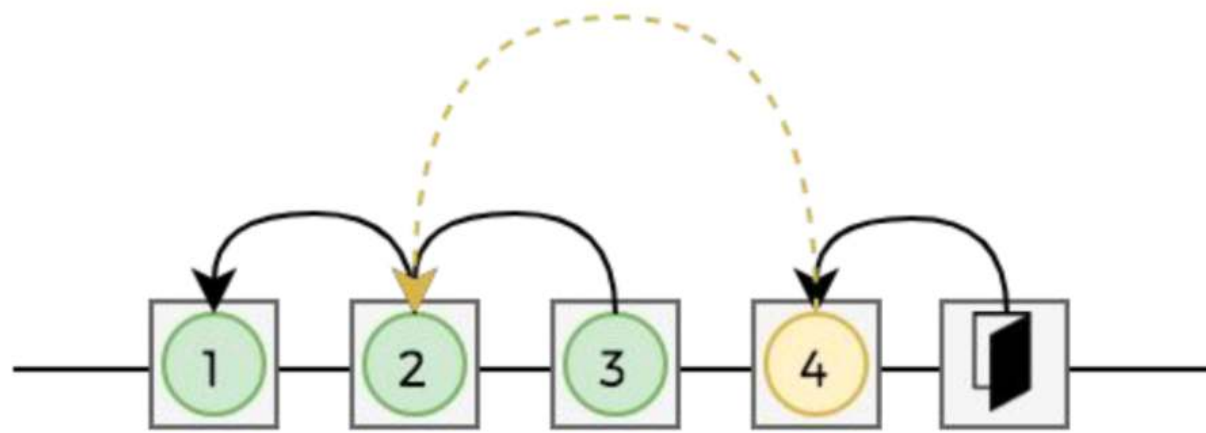


- 1) Exiter sends an exit tx attempting to exit transaction 3.
- 2) Challenger sends a challenge with transaction 4 which cancels exit

source: <https://karl.tech/plasma-cash-simple-spec/>

# Challenges

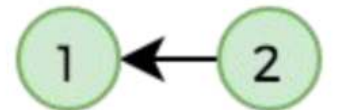
## Exit Double Spend Challenge



Ethereum block



Valid spend



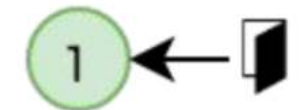
Invalid spend



Double spend



Exit tx

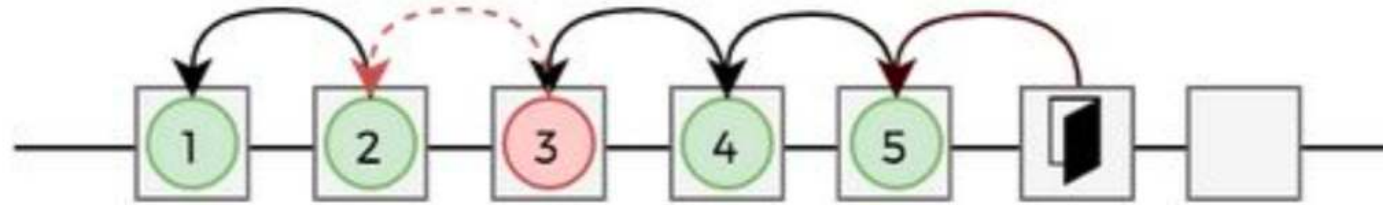


- 1) Exiter sends an exit with tx [(4), (2)], attempting to exit transaction (4).
- 2) Challenger sends a challenge with transaction (3). This token is included before (4) and spends (4)'s parent, which cancels the exit.

source: <https://karl.tech/plasma-cash-simple-spec/>

# Challenges

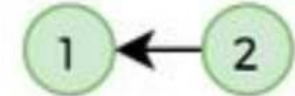
## Exit With Invalid History Challenge



Ethereum block



Valid spend



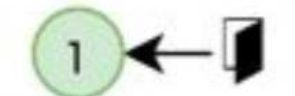
Invalid spend



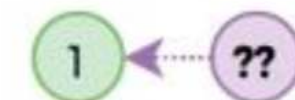
Double spend



Exit tx



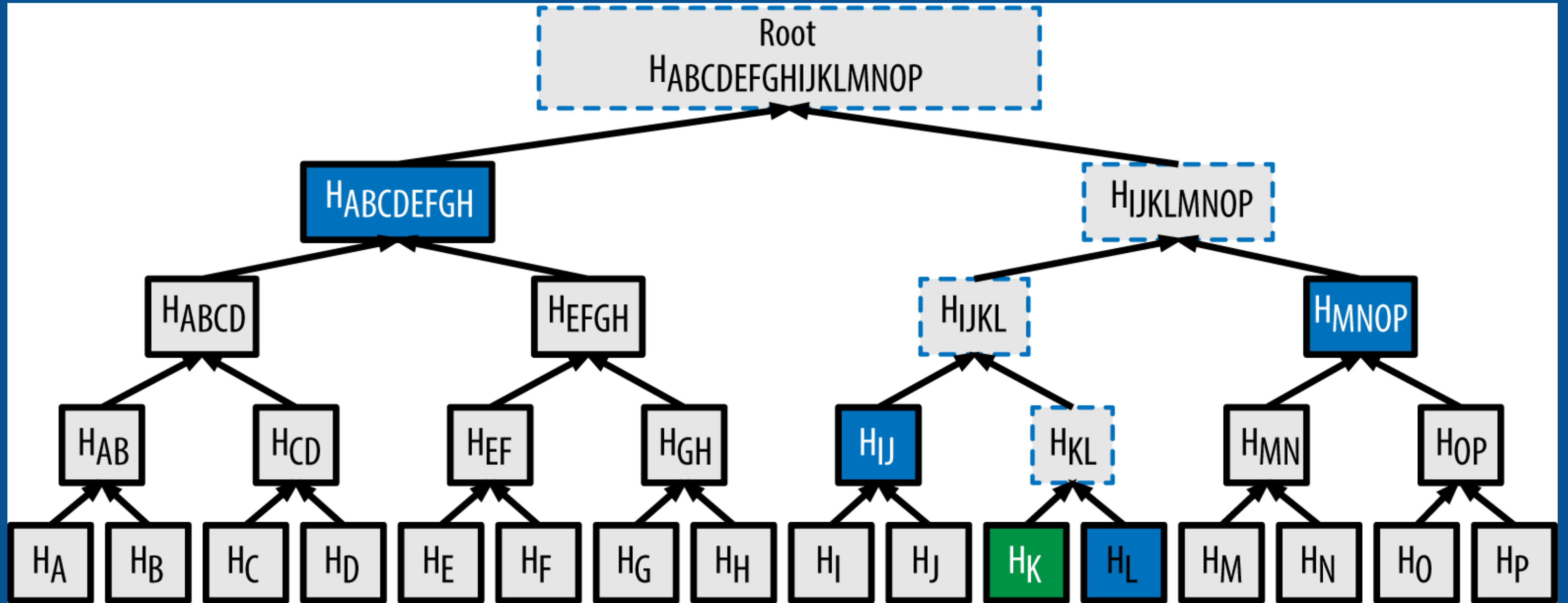
Withheld spend



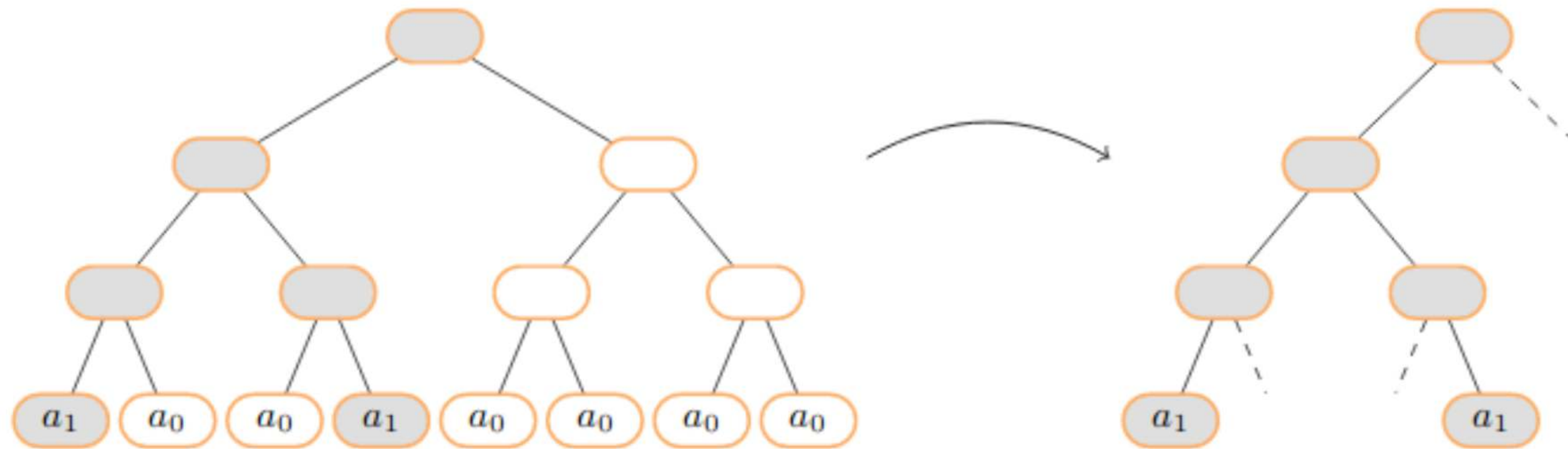
- 1) Exiter sends an exit with tx (5) & (4), attempting to exit transaction (5).
- 2) Challenger sends a challenge with transaction (2) & (1), the last valid transaction
- 3) Exiter must respond with a valid child of tx (2). One does not exist, and so the exit is canceled.

source: <https://karl.tech/plasma-cash-simple-spec/>

# MERKLE TREES



# SPARSE MERKLE TREES



# WHAT DOES THIS LOOK LIKE?



9:41



Your Cards from



CryptoZombies: Battleground



Pushhh

...

Rarity: **Rare**

Type: Walker

Entry: Return a zombie to hand.



Ghoul

...

Rarity: **Rare**

Type: Walker

Entry: Attack: Loses 1 damage



Burrrnn

...

Rarity: **Rare**

Type: Feral

Entry: Feral



Golem

...

Rarity: **Rare**

Type: Heavy

Entry: Heavy

# LIQUIDITY PROVIDERS



# GETTING STARTED



# CRYPTOZOMBIES

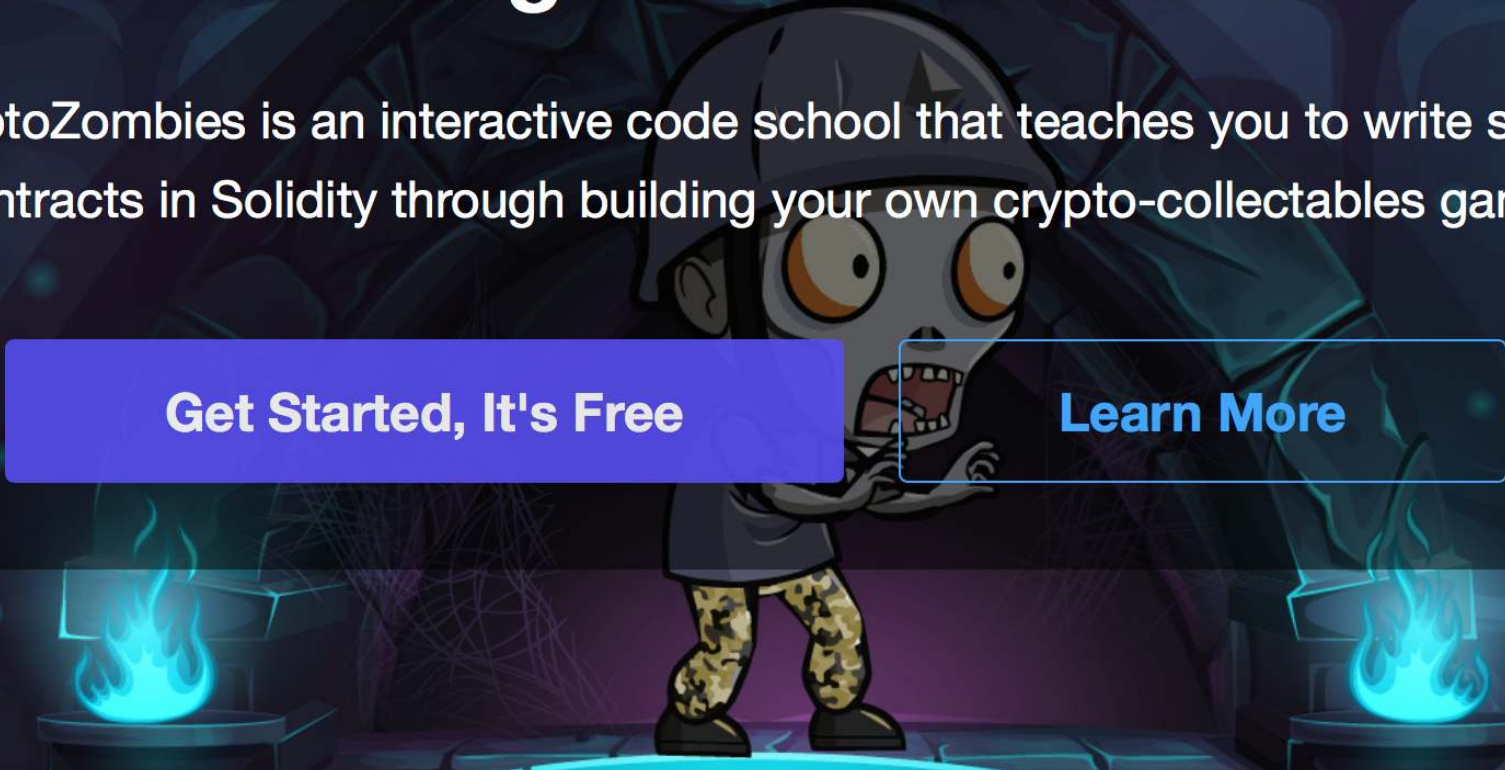


# Learn to Code Ethereum DApps By Building Your Own Game

CryptoZombies is an interactive code school that teaches you to write smart contracts in Solidity through building your own crypto-collectables game.

[Get Started, It's Free](#)

[Learn More](#)



CRYPTOZOMBIES

# github.com/loomnetwork/plasma-cash



Pull requests

Issues

Marketplace

Explore







loomnetwork / plasma-cash

Unwatch

27

Star

161

Fork

32

<> Code

Issues 8

Pull requests 2

Projects 0

Wiki

Insights

Settings

Plasma Cash Contract & Client. ERC721, ERC20, and ETH compatible

<https://loomx.io/developers>

Edit

ethereum

loom

plasma

Manage topics

678 commits

9 branches

0 releases

6 contributors

Branch: master

New pull request

Create new file

Upload files

Find file

Clone or download

 gakonst and enlight

Update docs and dependencies (#114)

Latest commit 6533113 29 days ago

|                |                                                |              |
|----------------|------------------------------------------------|--------------|
| loom_js_test   | Update docs and dependencies (#114)            | 29 days ago  |
| loom_test      | Add misssing dep to Go tests                   | a month ago  |
| plasma_cash    | Update docs and dependencies (#114)            | 29 days ago  |
| server         | Update docs and dependencies (#114)            | 29 days ago  |
| .gitattributes | Initial commit                                 | 4 months ago |
| .gitignore     | Move in the Plasma Cash e2e tests from loom-js | 2 months ago |
| FullSpec.md    | update docs for validators                     | a month ago  |

# COOL THINGS TO BUILD WITH THIS

- » Transaction Networks
- » Liquidity Networks
- » Distributed Exchanges
- » Blockchain Gaming
- » Cross Blockchain communication

# TAKE AWAYS

- » Plasma Cash is here now
- » It helps scale payment networks
- » You can use it for non-fungible tokens

FAIL

# QUESTIONS?

- » Loom Network
- » Loom SDK - <https://loomx.io/developers>
- » Yes we're hiring

