



Optimistic rollups: Offchain Labs Arbitrum

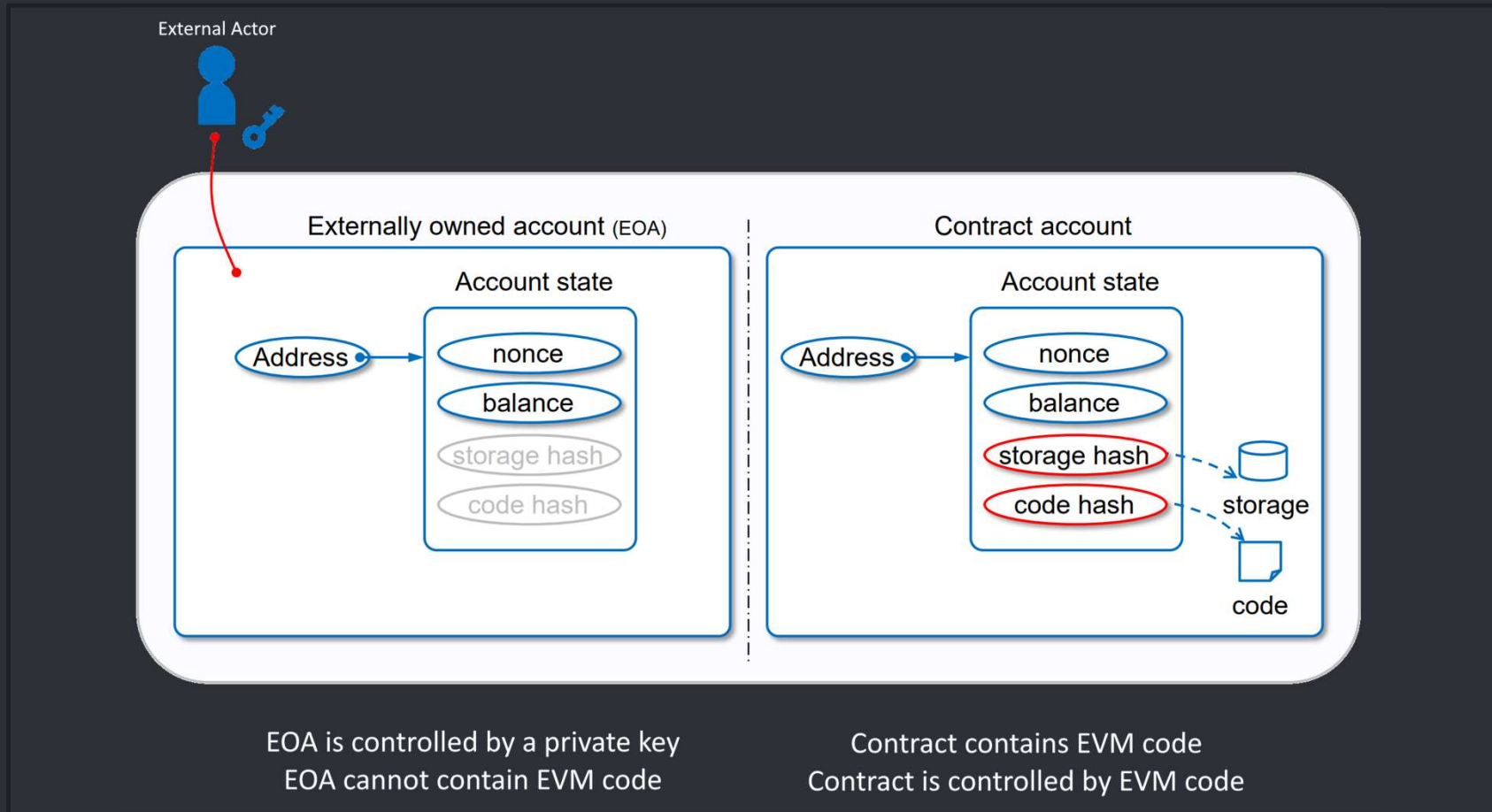
Seminar Cryptography and Data Security

24.11.2021

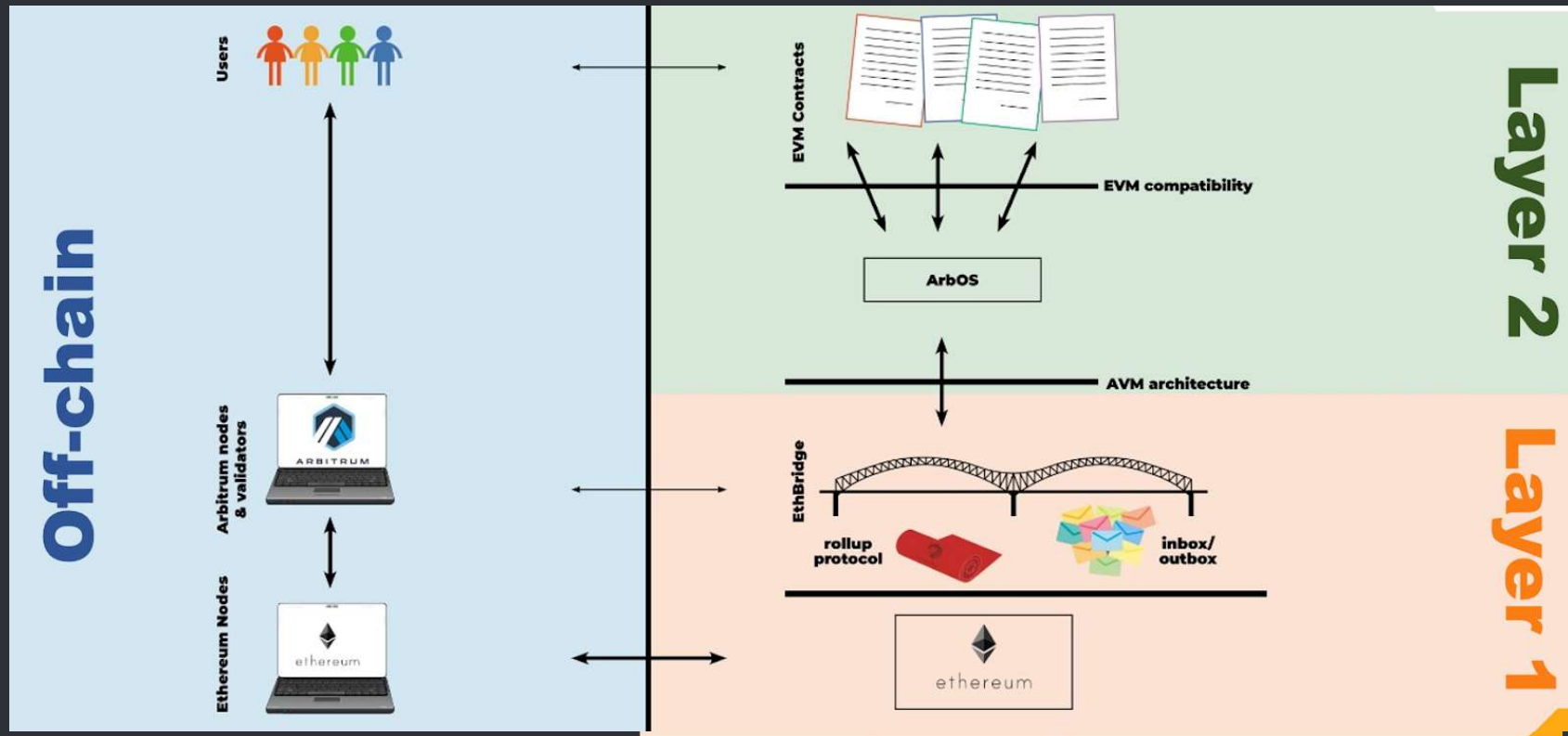
Presentation by:

Marius Asadauskas

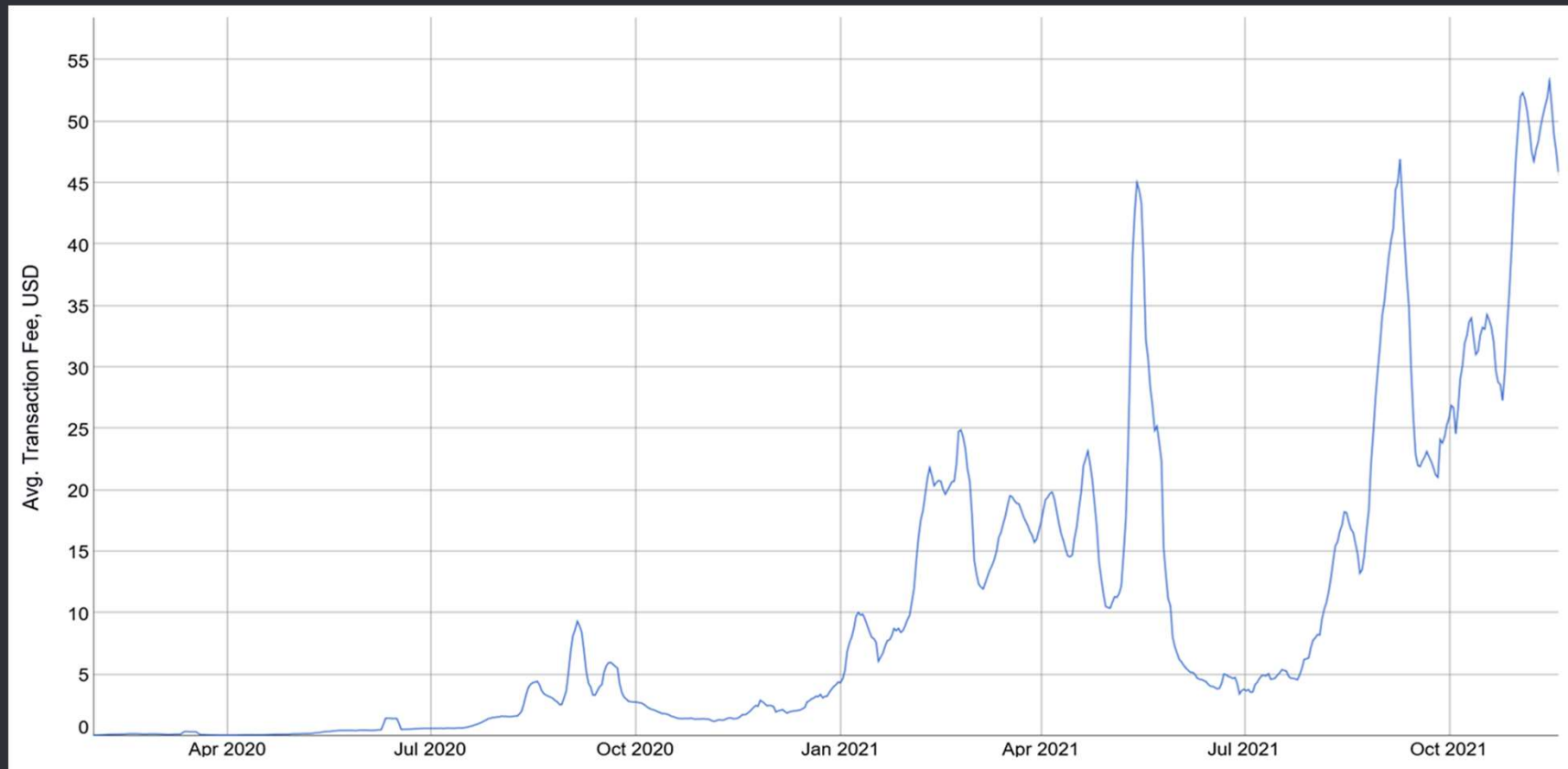
Different Account types



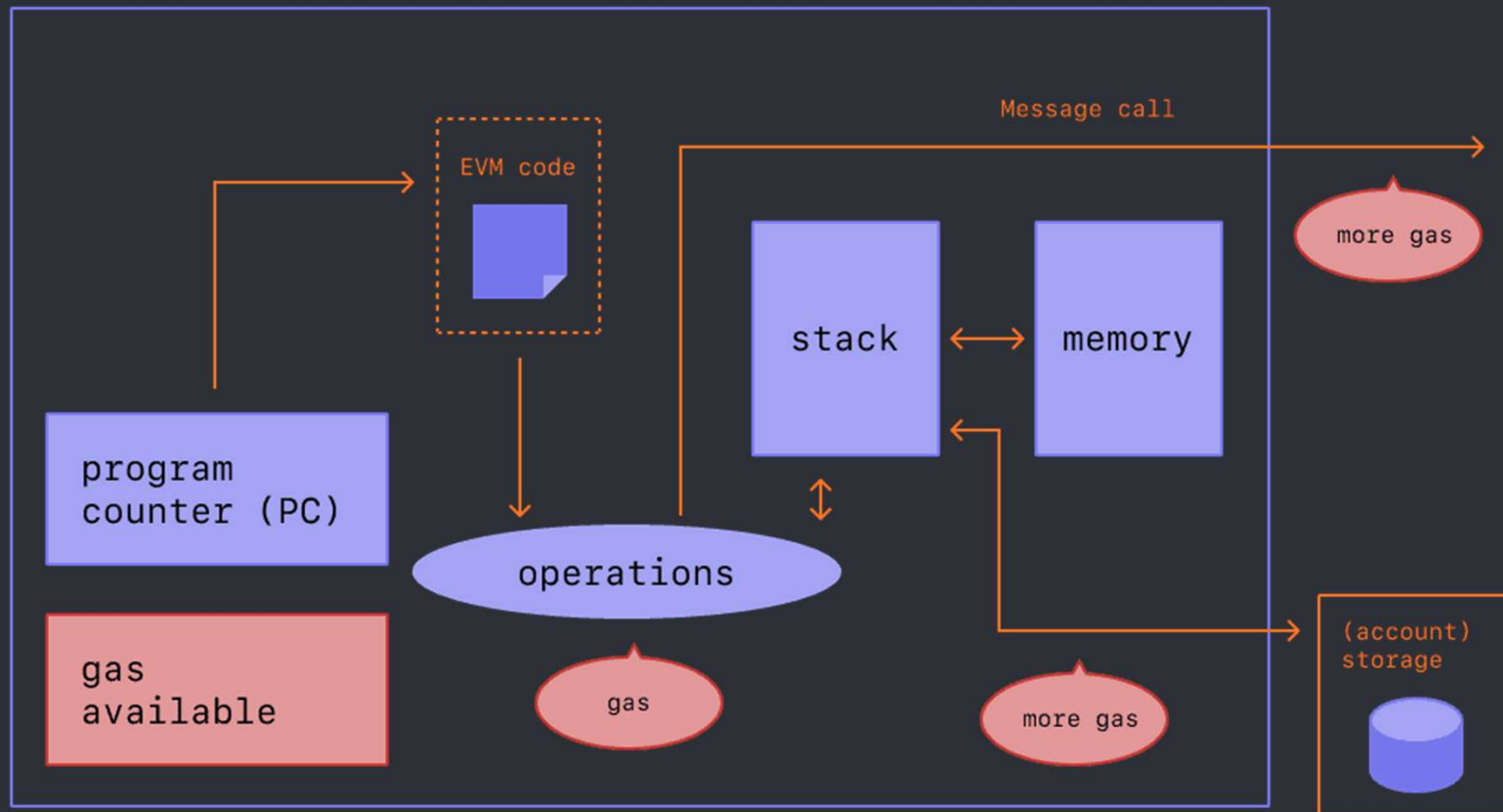
Rollups in Arbitrum



Motivation



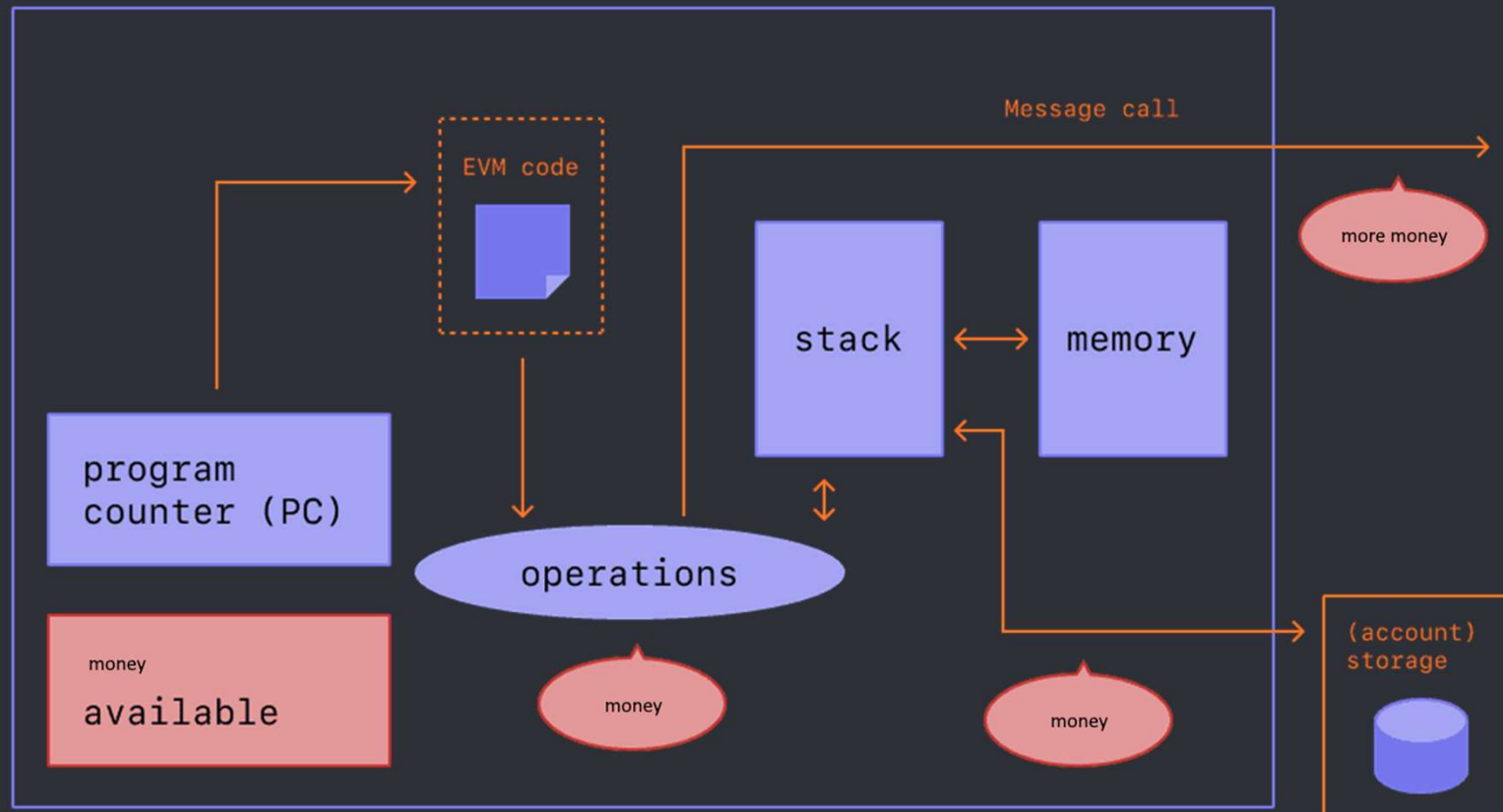
Gas



1 gwei = 10^{-9} ETH

Gas = Gas units * (Base fee + Tip)

Money



The Verifier's Dilemma

1. System works as intended, nobody cheats
2. No point in verifying
3. Opportunity to cheat arises
4. System does not work as intended



- Verifying also puts you behind others

Solution

- Ethereum:
 - Global gas limit
 - Processing at most ~1600 hashes per second
- Arbitrum:
 - Asserter-challenge design pattern
 - Escrow funds



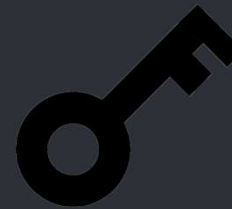
Roles:

Verifier:



- Verifies validity of transactions
- Smart contracts on Ethereum

Key:



- Member in protocol
- Can propose transactions
- Has a private key

VM:



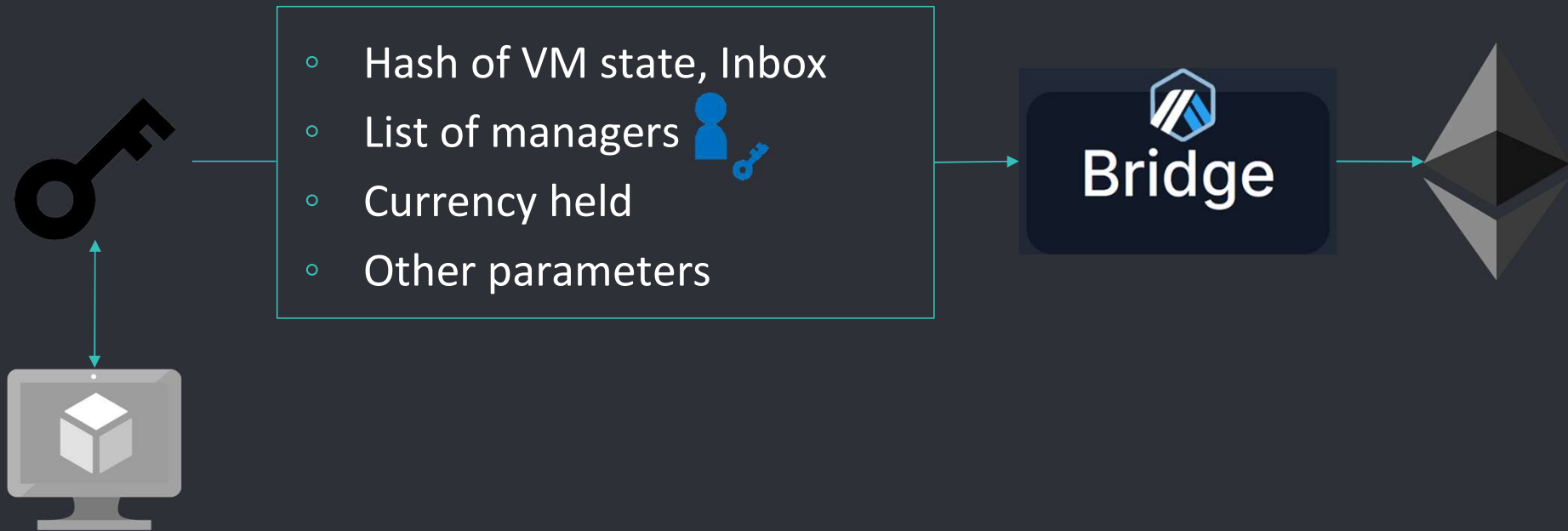
- Code specifies behaviour
- Can own, send and receive currency

Manager:

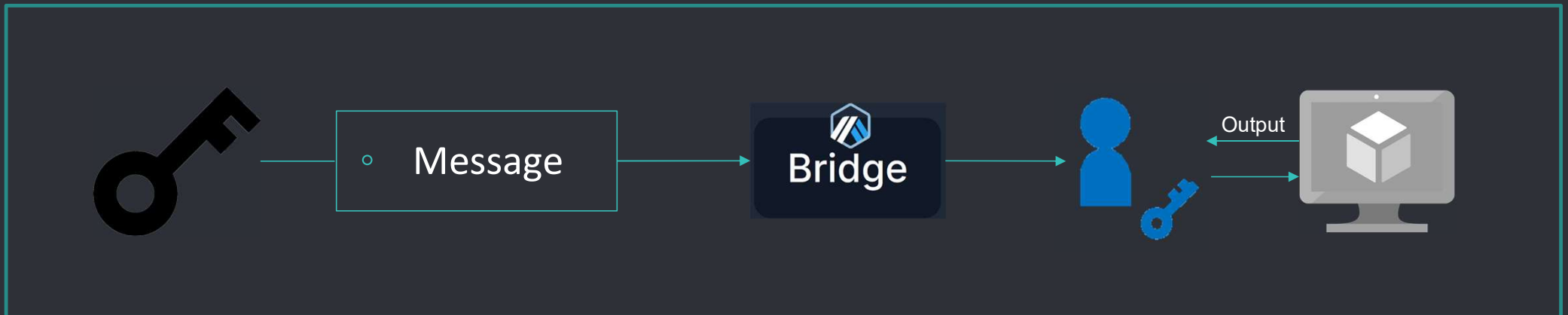


- Is a key
- Monitors progress of VM

Arbitrum VM creation

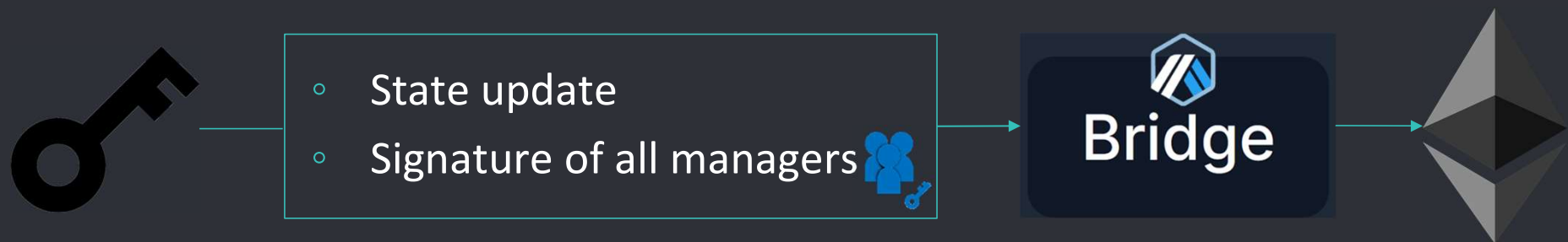


Sending message to VM

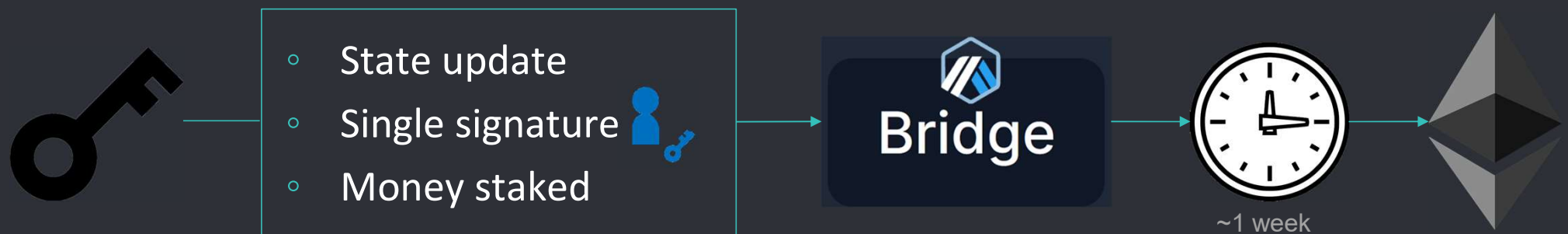


Assertion types

Unanimous assertions:

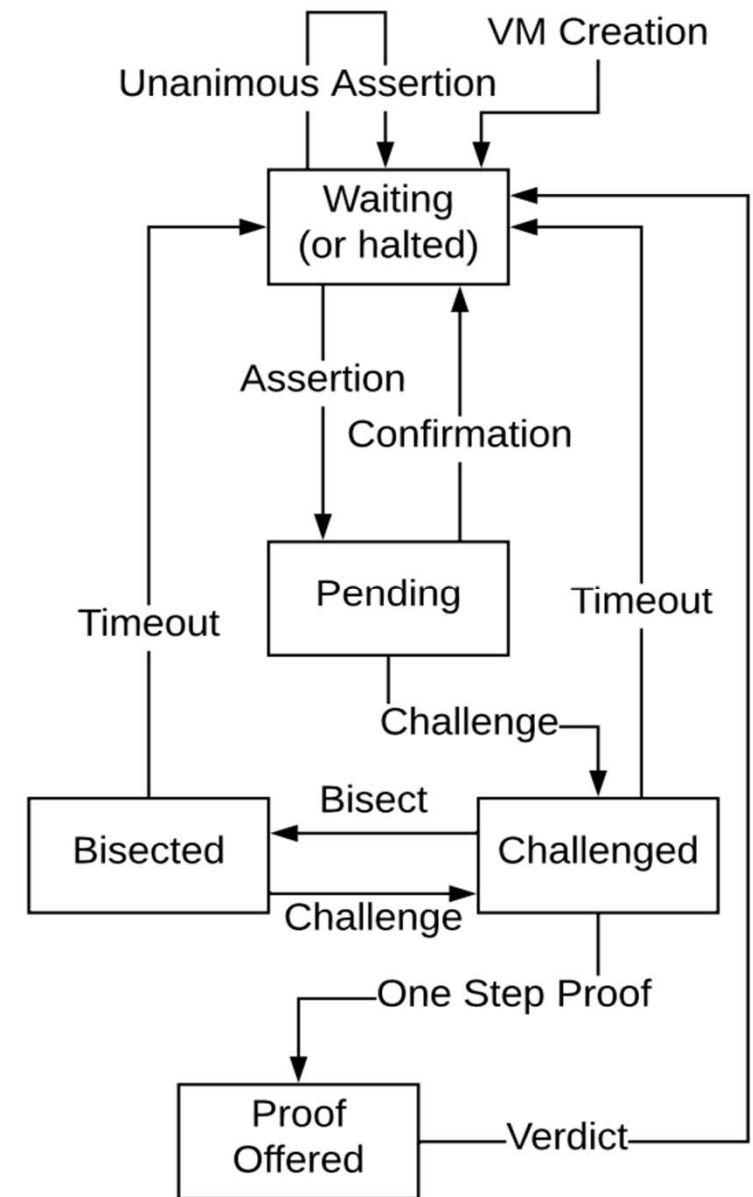


Disputable assertions:



Bisection Protocol

- Bisection means dividing into two
- Relies on interactive proving
- Game with Ethereum contract as the referee.



Bisection Protocol

Alice:

Instruction,	State hash
--------------	------------

A--:	1
------	---

B++:	2
------	---

B--:	1
------	---

A++:	0
------	---

Receives $3 \neq 0$,

Challenges assertion

Bob:

Instruction,	State hash
--------------	------------

A--:	1
------	---

B++:	2
------	---

B--:	2
------	---

A++:	3
------	---

Sends DA with hash 3

Bisection Protocol

Bob bisects instructions

Instruction,	State hash
1-2:	2
3-4:	3

Alice chooses

Instruction,	State hash
1-2:	2
3-4:	0

Alice challenges 3-4

Bisection Protocol

Bob bisects instructions

Instruction,	State hash
3:	2
4:	3

Alice chooses

Instruction,	State hash
3:	1
4:	0

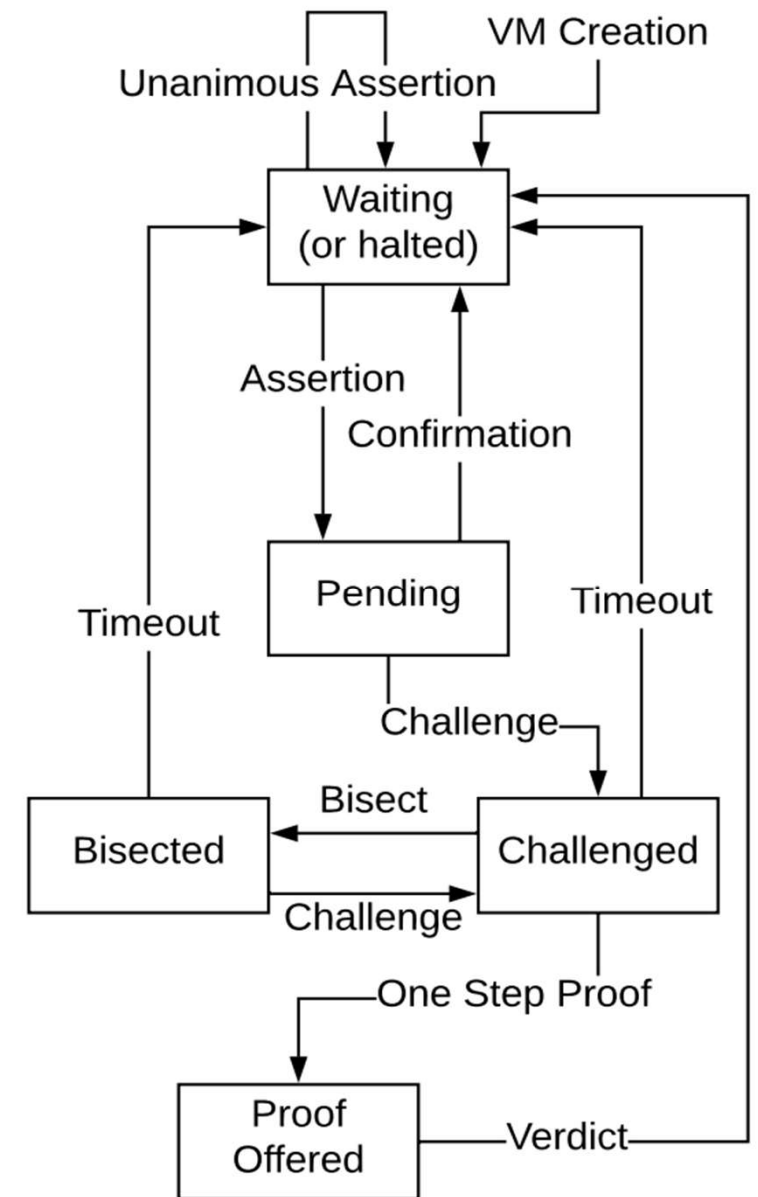
Alice challenges 3

Bisection Protocol



Bisection Protocol

- Bisection means dividing into two
- Relies on interactive proving
- Game with Ethereum contract as the referee.



Arbitrum History

Mainnet for Everyone



Offchain Labs Aug 31 · 6 min read



Today's the day! We've opened up Arbitrum One for everyone and couldn't

Uniswap on Arbitrum



Uniswap

Learn how this Layer 2 network lowers the cost of transactions on the Uniswap protocol

Arbitrum One Outage Report



Offchain Labs




















Follow



Sep 14 · 2 min read



Layer 2 ranking

No.	Name	Value Locked	7 days change	Market share	Purpose	Technology
1.	 Arbitrum	\$2.67B	-5.07%	43.67%	Universal	Optimistic Rollup
2.	 dYdX 	\$975M	+0.67%	15.91%	Exchange	ZK Rollup
3.	 Boba Network	 \$863M	+889.98%	14.08%	Universal	Optimistic Rollup
4.	 Loopring	 \$580M	+18.61%	9.47%	Payments, Exchange	ZK Rollup
5.	 Optimism	\$461M	-5.62%	7.53%	Universal	Optimistic Rollup
6.	 ZKSwap V2	 \$218M	-16.01%	3.56%	Payments, Exchange	ZK Rollup
7.	 ImmutableX 	 \$215M	+22.70%	3.51%	NFT, Exchange	Validium
8.	 DeversiFi 	 \$62.15M	+23.46%	1.01%	Exchange	Validium
9.	 zkSync	\$33.90M	+15.46%	0.55%	Payments	ZK Rollup
10.	 Sorare 	\$24.06M	+5.70%	0.39%	NFT, Exchange	Validium



ArbiNyan



ArbiNyan

- Arbitrum's skyrocketing growth in total value locked was largely triggered by the launch of a yield farm called ArbiNYAN. Currently, the project contains 439,262.5 ETH worth about \$1.4 billion.

Pros/Cons

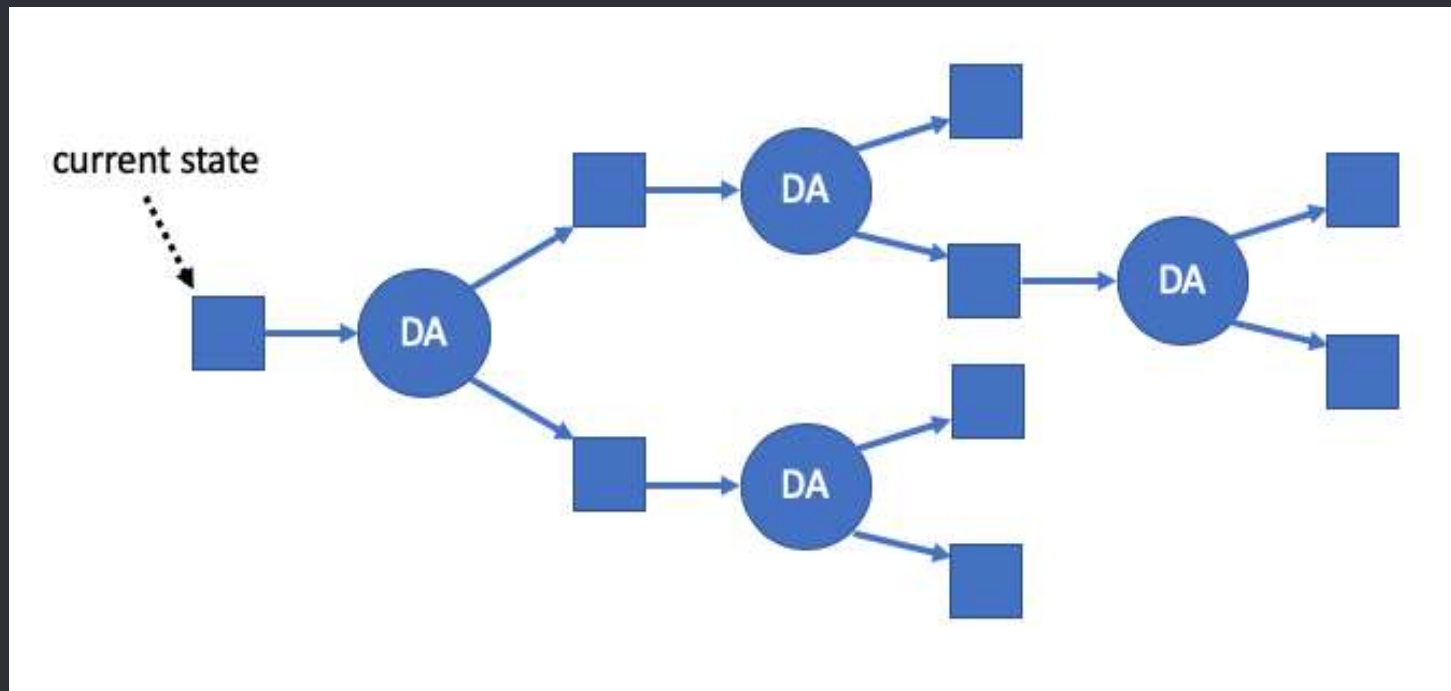
Pros:

- EVM compatible
- Much lower cost
- Allows contract modification
- Higher privacy
- Security of layer 1

Cons:



- Long waiting time till on-chain confirmation
- Central authority Arbitrum

Mainnet Implementation



Future work

- Analyse promises of Arbitrum

💡 Transaction Action:	▶ Approved  USDC For Trade On  Uniswap V3: Router
❓ Value:	0 ETH (\$0.00)
❓ Transaction Fee:	0.00103155154469 ETH (\$4.47)

- “ArbOS also adds a 15% markup and deposits those funds into the network fee account, to help cover overhead and other chain costs.”

✅ Contract Source Code Verified (Exact Match)	
Contract Name:	UniswapV2Router02
Compiler Version	v0.6.12+commit.27d51765

Alternatives

- ZK-Rollups
- TEEs
- State Channels



Thank you for your attention

Any questions?