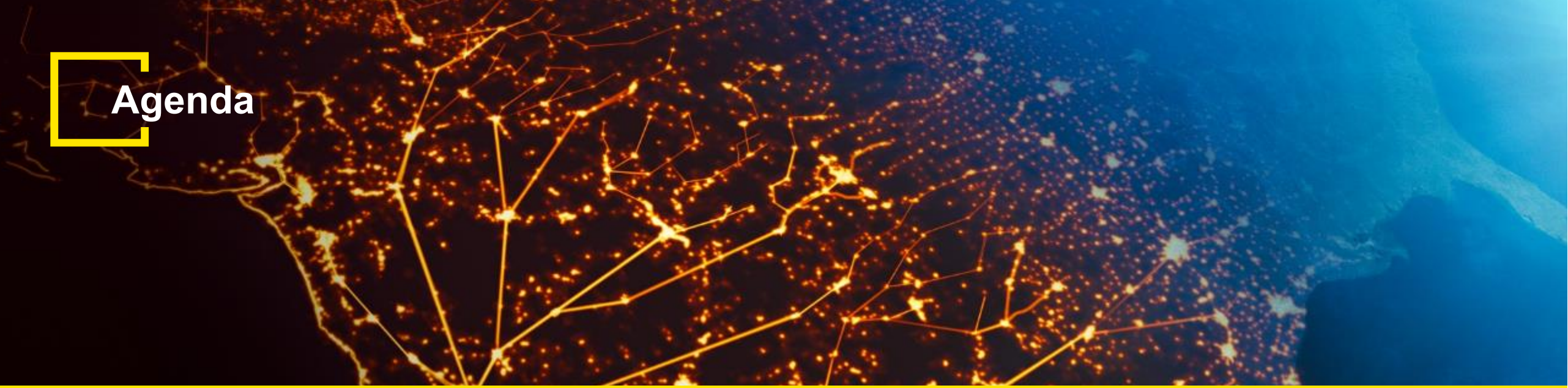
Nightfall

Private transactions on Ethereum using zk-SNARKs.

Devcon 2019

EY
Building a better working world

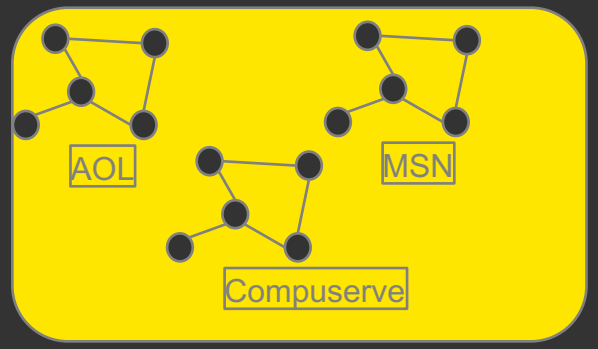


Agenda

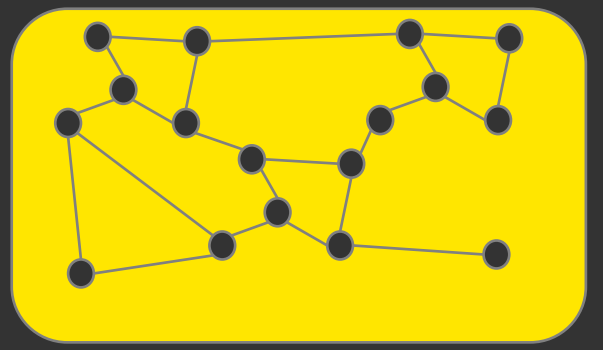
1. Motivation for Nightfall
2. High Level Architecture
3. Nightfall protocols
4. Architecture detailed
5. What next?

Blockchain development is analogous to the development of the internet

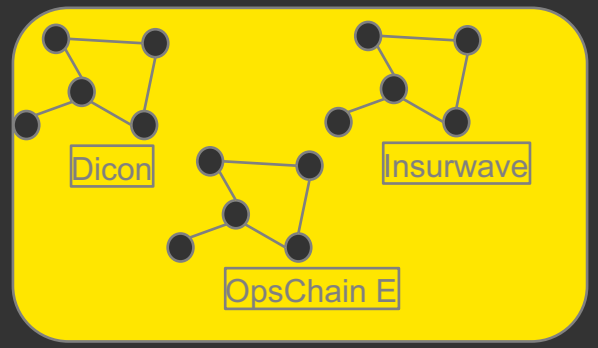
Yesterday: multiple independent and 'owned' networks brought some benefits



Today: frictionless communication via the internet supports e-commerce transactions

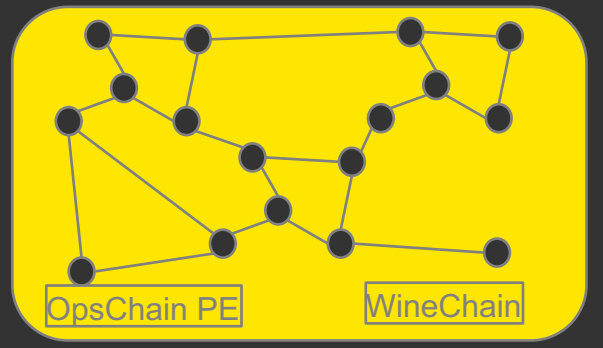


Today: multiple independent private blockchains bring some benefits



ZKPs

Tomorrow: frictionless value exchanges via public blockchain ARE the e-commerce transactions



What is Nightfall?

Public blockchain is great...

...but transaction data is public

What is Nightfall?

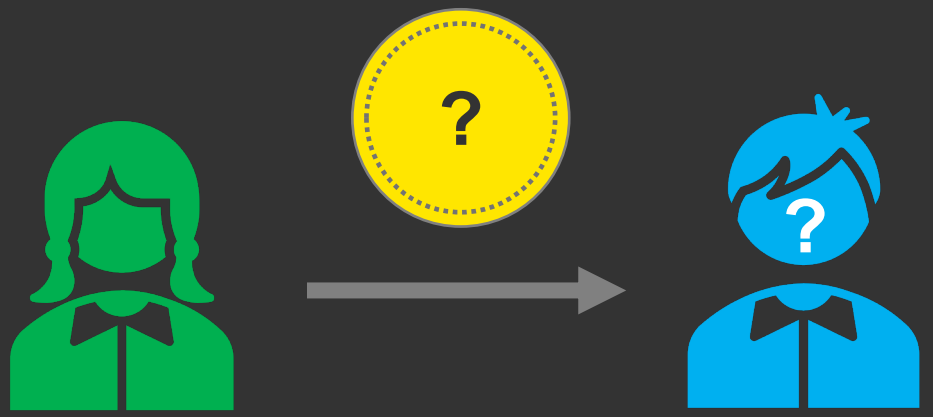
Businesses need transaction privacy

Nightfall enables privacy

What is Nightfall?

Nightfall enables transfer of *fungible* and *non-fungible* tokens between parties such that:

- the value/token id of the token remains **confidential**
- the recipient remains **anonymous**



What is Nightfall?

- Open source
- Public domain
- Ideas & contributions welcome
- See github.com/EYBlockchain/nightfall

What is Nightfall?

Nightfall includes...

- UI
- APIs
- Smart Contract Templates
  - Shield contracts
  - zk-SNARK verifier contracts
  - ERC contracts
- zk-SNARK generator (via ZoKrates)
- DB's for private data management
- Private messaging

What is Nightfall?

Nightfall can be subdivided in to 6 sub-protocols

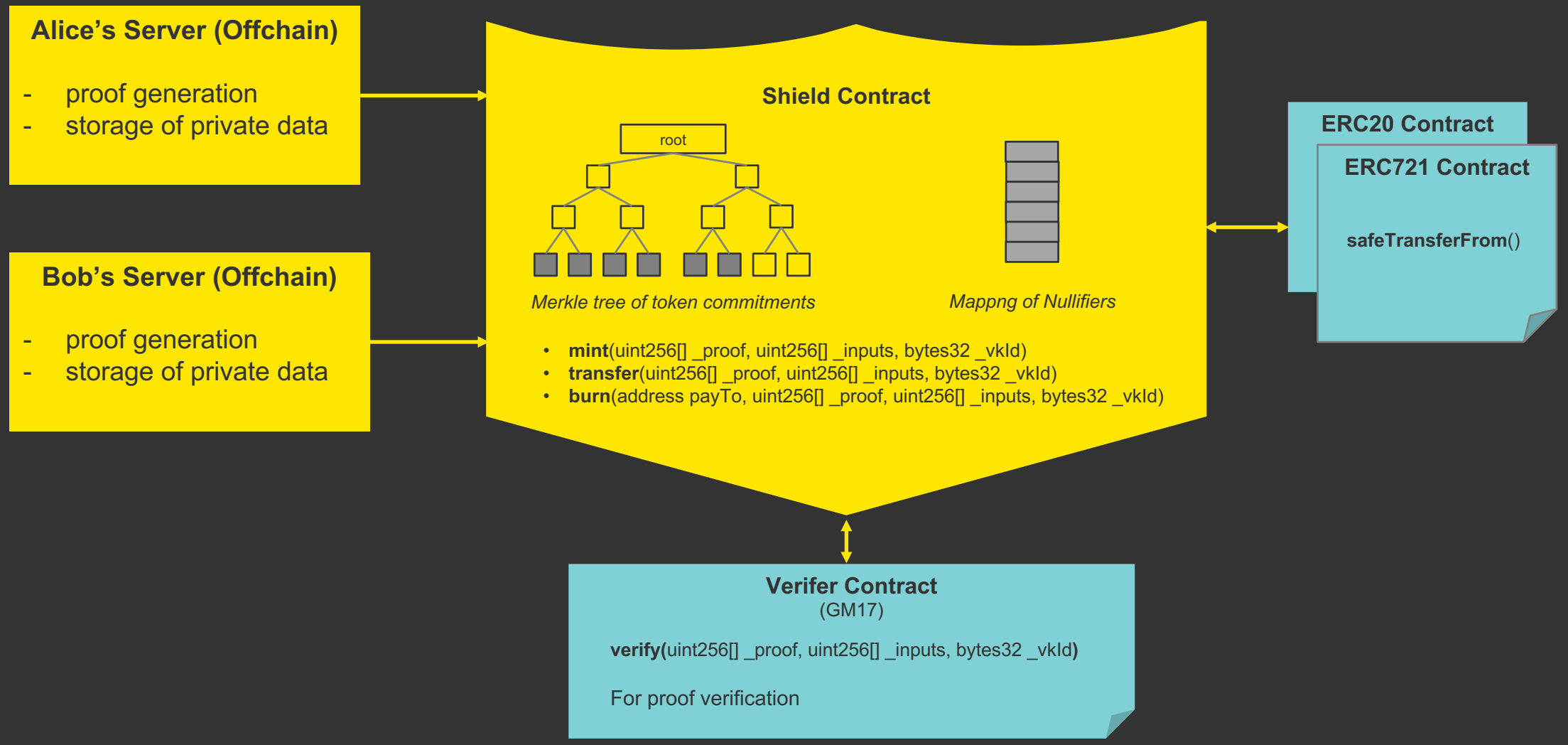
ERC-20 Token Commitments:

- **Mint**
- **Transfer**
- **Burn**

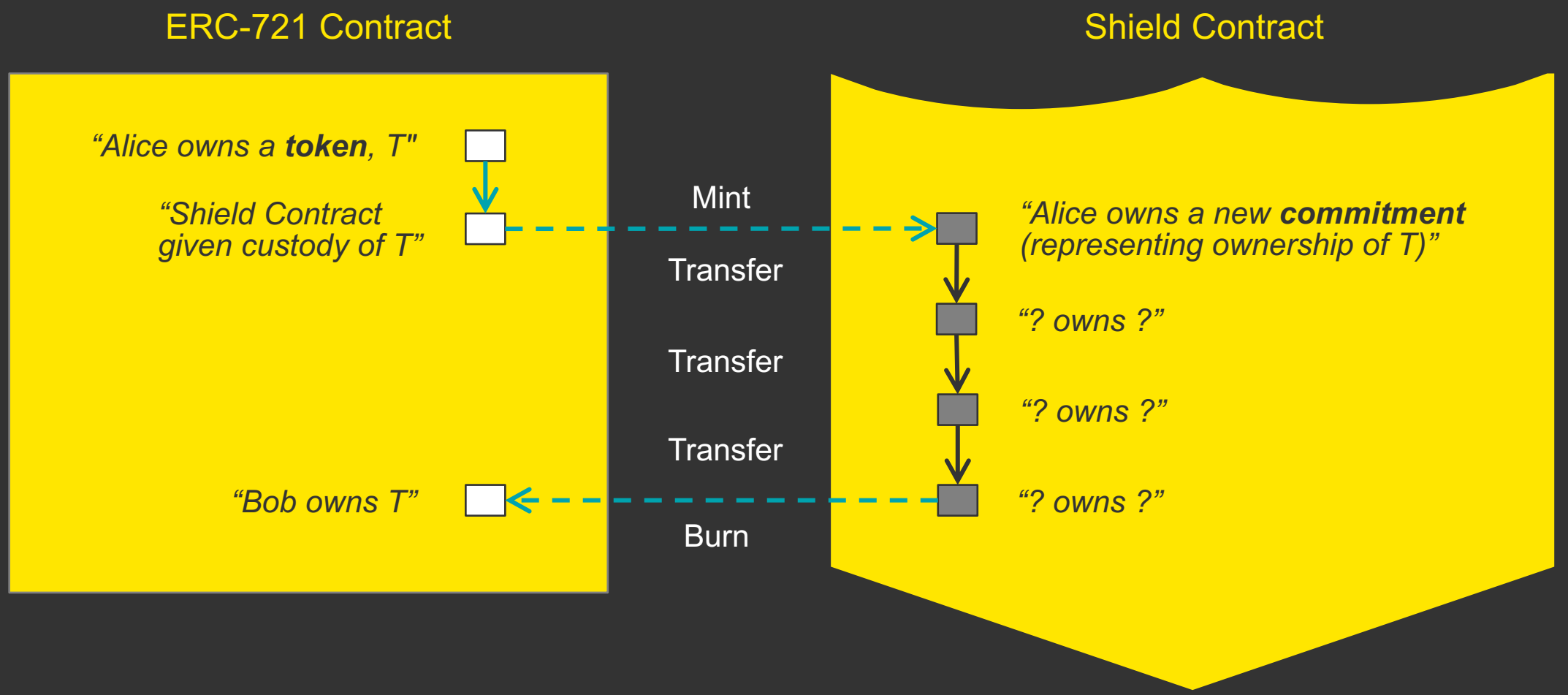
ERC-721 Token Commitments:

- **Mint**
- **Transfer**
- **Burn**

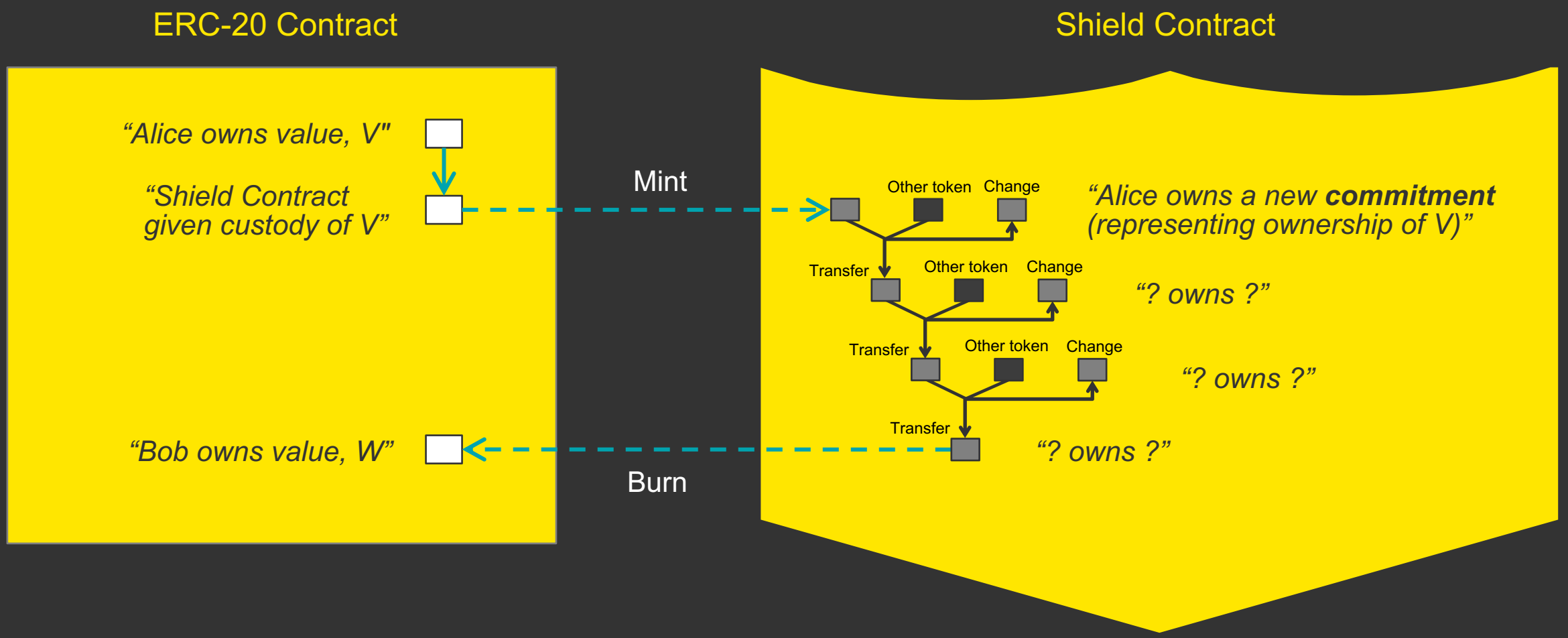
High Level Architecture



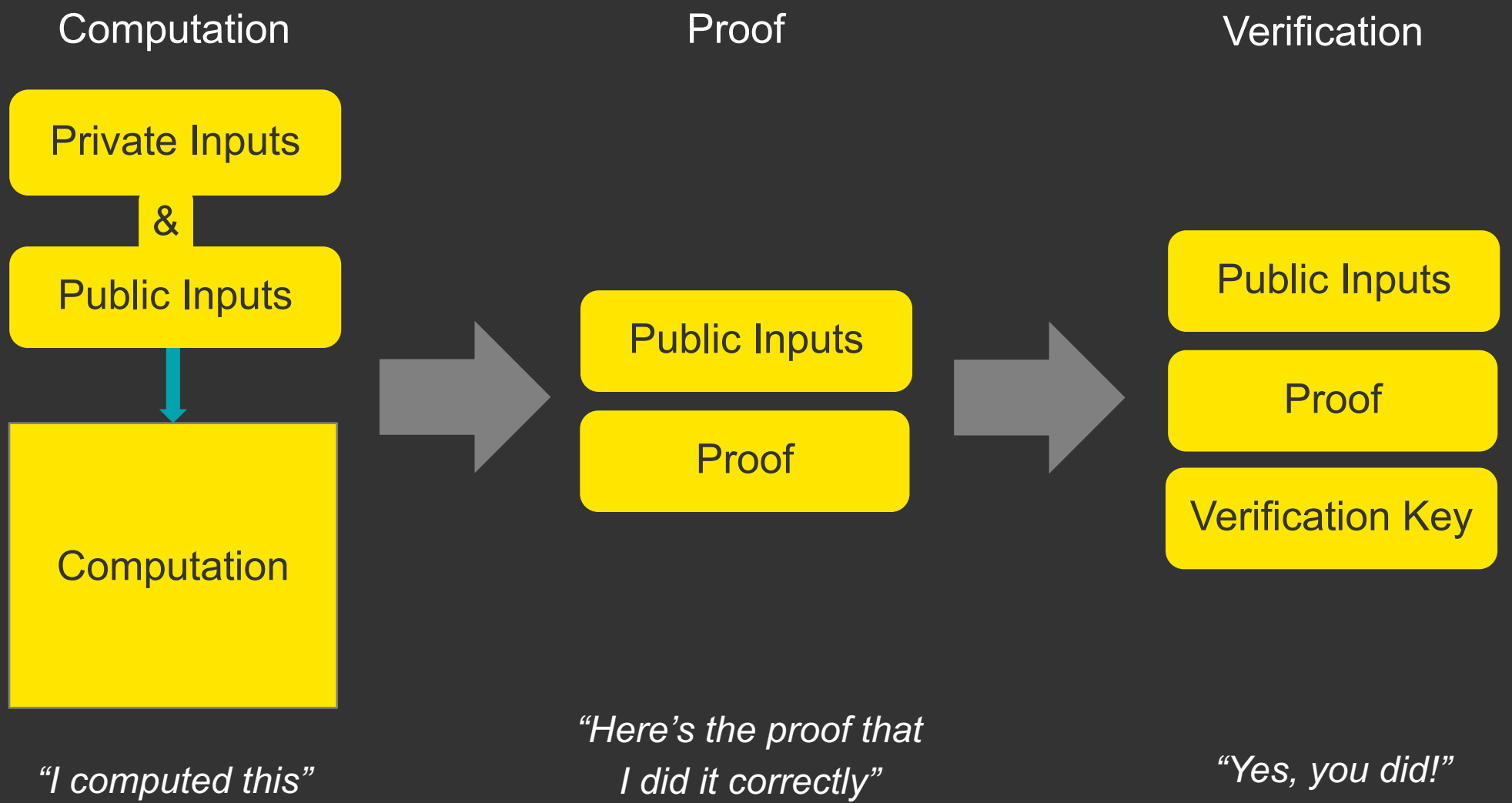
ERC-721 shielding



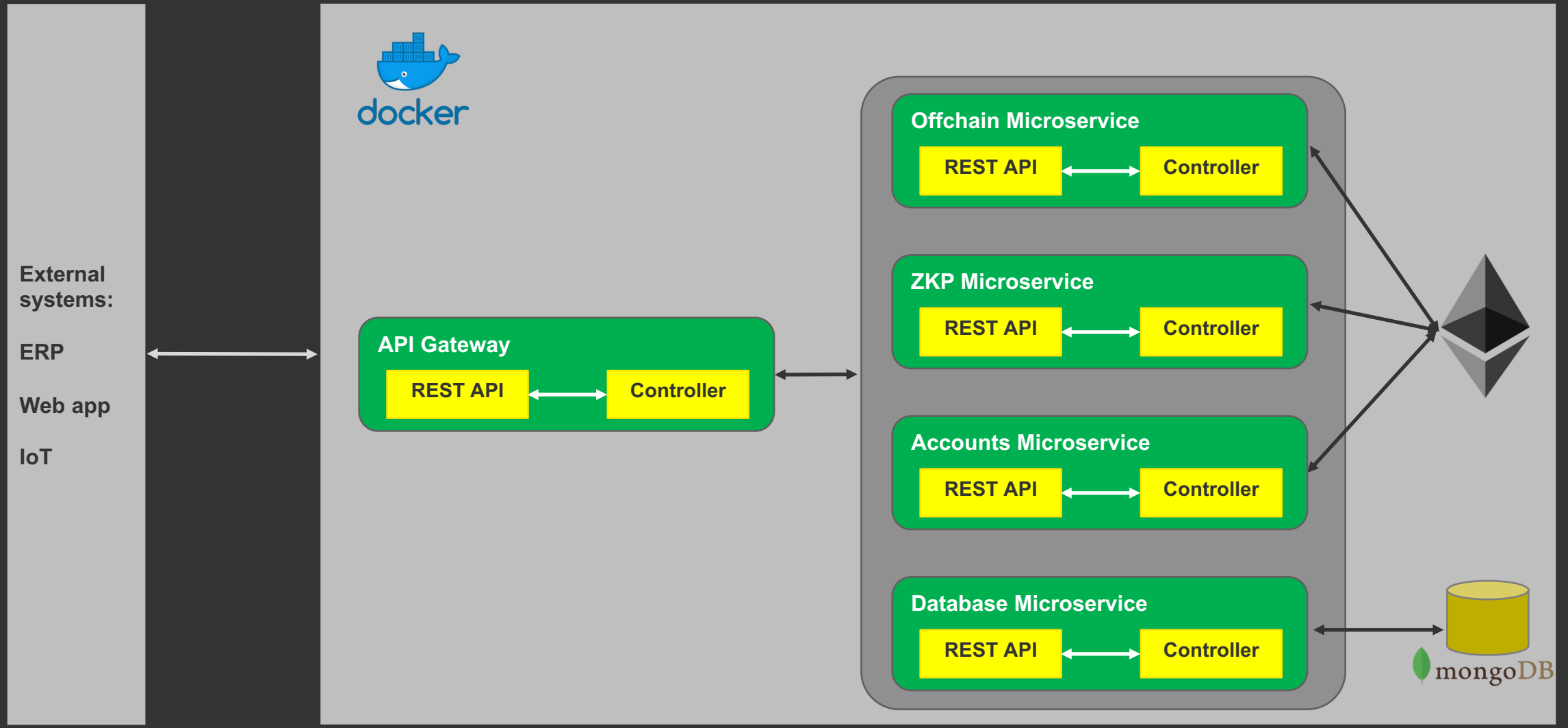
ERC-20 shielding



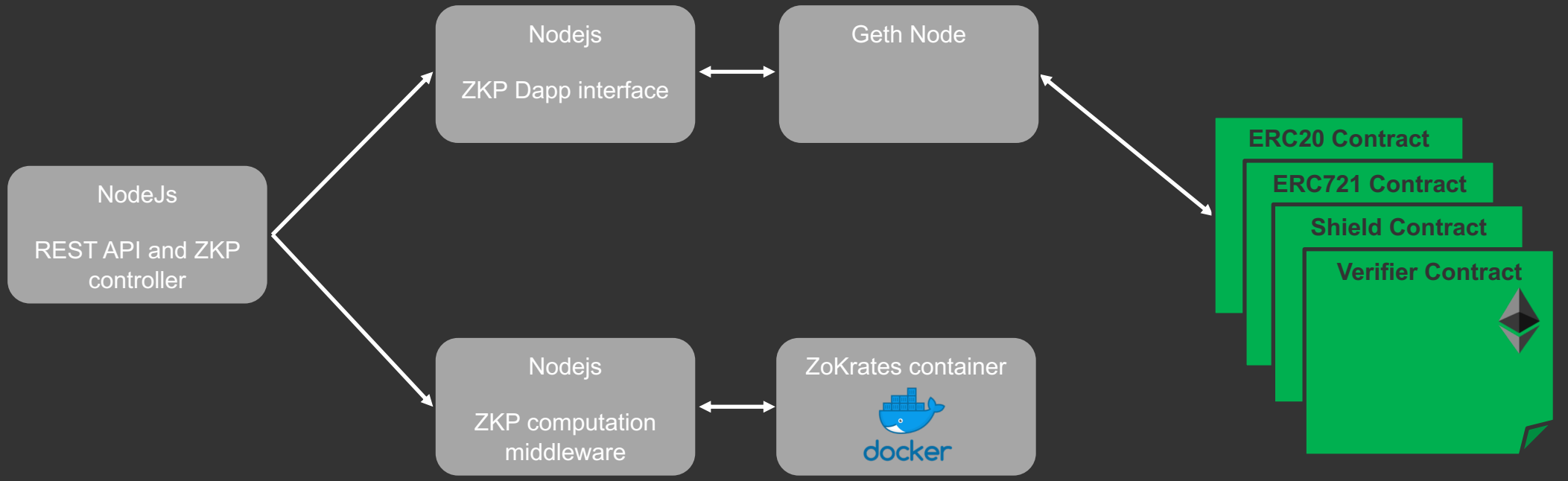
zk-SNARKs


Computation
Proof
Verification
Private Inputs
&
Public Inputs
Computation
Public Inputs
Proof
Public Inputs
Proof
Verification Key
"I computed this"
"Here's the proof that I did it correctly"
"Yes, you did!"

Architecture



ZKP Microservice



What next?
Contributions welcome!

- More developer tools
  - Requests welcome!
- Reduce the cost of private transactions
  - Batching zk-SNARKs
  - Smart contract logic
  - Verification scheme
- Anonymity of the transactor (token sender)
  - Transaction relayers
- zk-SNARK circuit efficiency
- One Shield Contract
  - For all ERC-20 / ERC-721 tokens
- Setup - trusted / trustless schemes?

Batching proofs

Performing ZKP-based private transactions is costly as it requires on chain verification of ZKP

For enhancing adoption, we need to improve performance

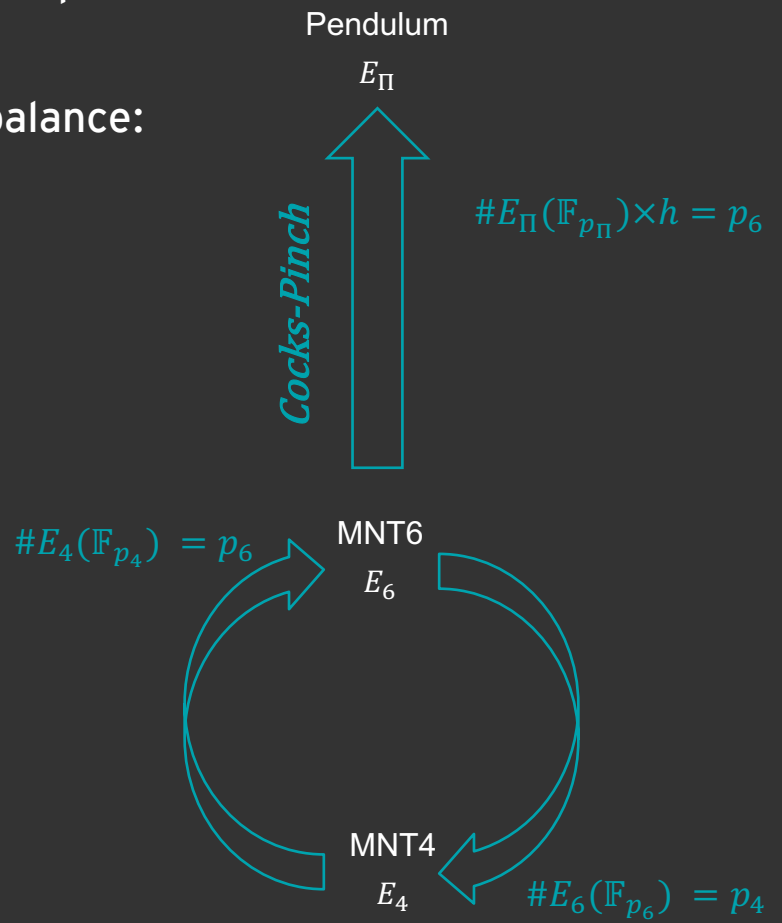
We've developed a prototype for batching proofs and are working on integrating into Nightfall

How to batch proofs ?

The most generic way to batch different zero-knowledge proofs relies on recursive proof composition via pairing-friendly cycles of elliptic curves

As of today the existing solutions do not offer an optimal security/performance balance:

Cycle	Security vs. speed[1,2]	Recursion depth
MNT4 / MNT6	Security — Speed	$+\infty$
MNT4753 / MNT6753 (Coda)	Security — Speed	$+\infty$
BLS12_377 / SW6 (Zexe)	Security — Speed	1



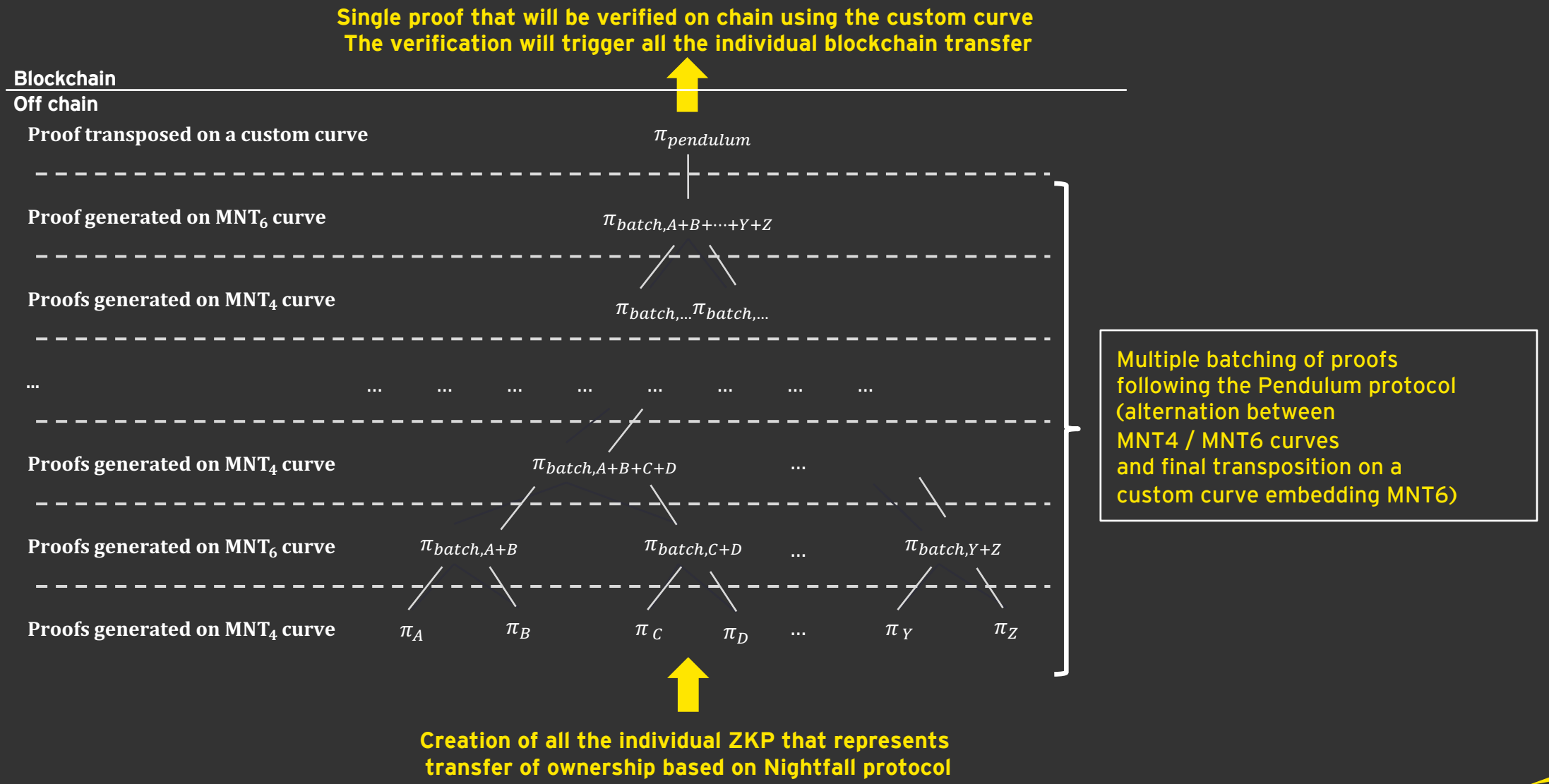
Leveraging on these approaches, we designed the **Pendulum protocol** that can achieve both secure and fast aggregation

Pendulum protocol

Use faster and less secure MNT4/MNT6 curves offchain + **Find a new elliptic curve on top of MNT6 for the final stage of proof composition** + **Combine the new curve with the MNT4/MNT6 curves**

Sources:
(1) https://eprint.iacr.org/2014/595.pdf
(2) https://eprint.iacr.org/2018/962.pdf

General overview of the batching protocol



Code released

ZoKrates

- Exposing off chain proof verification on ZoKrates
- Generate unitary proofs targeting MNT4/MNT6 curves
- Batching MNT4/MNT6 proofs on ZoKrates

libsnark

- Expose the verification circuit gadget to build a proof of proof

libff

- Support MNT4753, MNT6753, BLS12-381, BLS12-377, SW6, SW6-BIS, Pendulum curves

https://github.com/EYBlockchain

Going to the main net ?

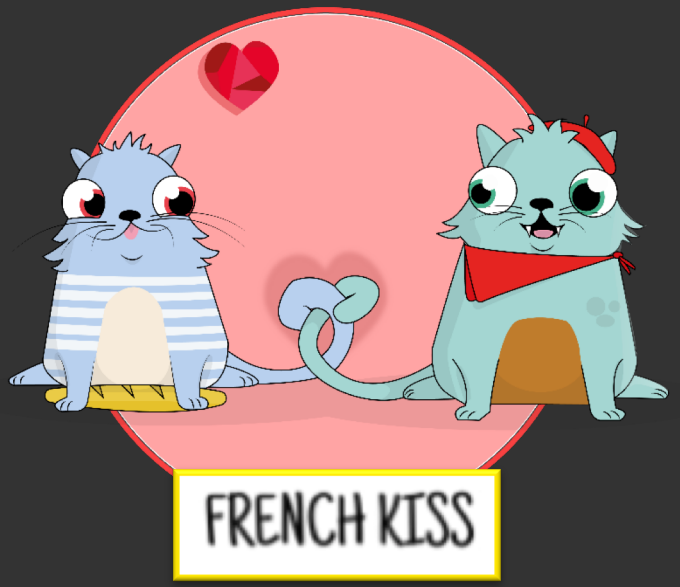
It would be great to do it on the main net !

Waiting for community decision on EIP1962 from Matter Labs

https://github.com/ethereum/EIPs/blob/master/EIPS/eip-1962.md

French Kiss under Nightfall

#Privacy #Swap #ZKP



Useful Links

- https://github.com/EYBlockchain/nightfall - ALL CONTRIBUTIONS WELCOME!
- https://github.com/EYBlockchain/nightfall/blob/master/doc/whitepaper/nightfall-v1.pdf
- https://medium.com/@chaitanyakonda/nightfall-makes-token-transactions-on-ethereum-private-how-does-it-work-acf2ffd0aa7a

Thank you

EY | Assurance | Tax | Transactions | Advisory

About EY
EY is a global leader in assurance, tax, transaction and advisory services. The insights and quality services we deliver help build trust and confidence in the capital markets and in economies the world over. We develop outstanding leaders who team to deliver on our promises to all of our stakeholders. In so doing, we play a critical role in building a better working world for our people, for our clients and for our communities.

EY refers to the global organization, and may refer to one or more, of the member firms of Ernst & Young Global Limited, each of which is a separate legal entity. Ernst & Young Global Limited, a UK company limited by guarantee, does not provide services to clients. For more information about our organization, please visit ey.com.

EYG no. XXXXXX
1801-2543904

ED None

ey.com