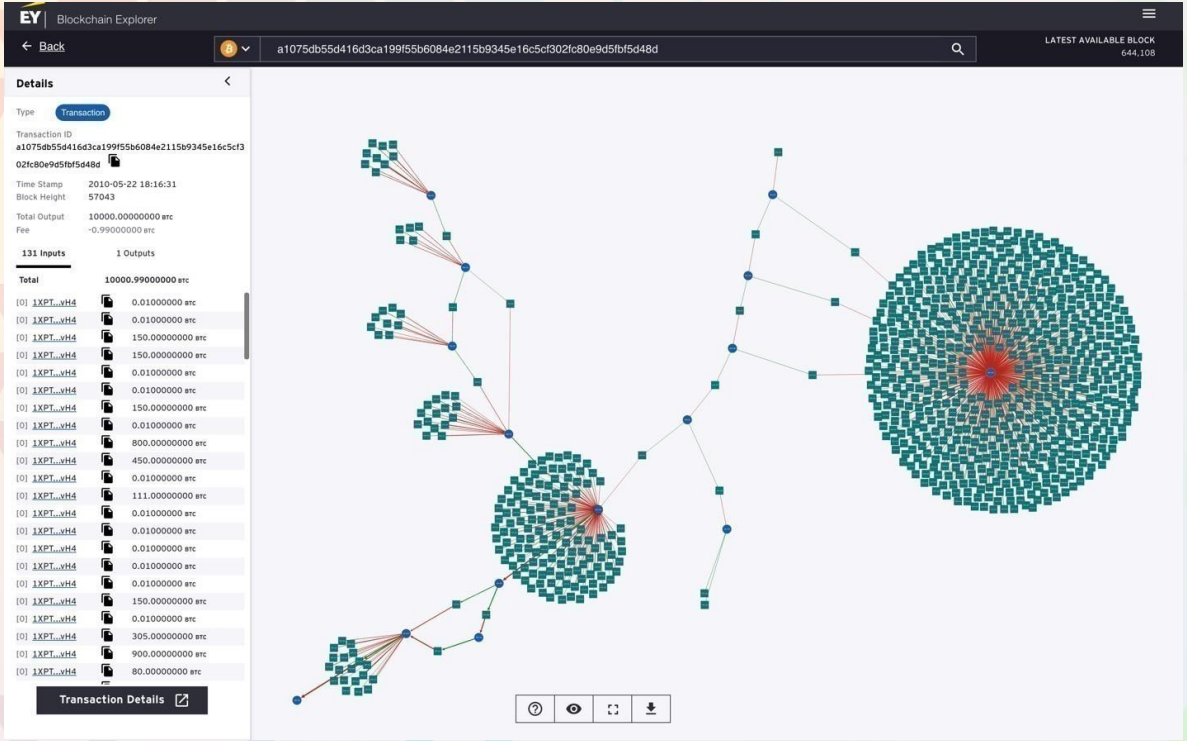
blockchain.ey.com

The New Era of Blockchain Privacy

Paul Brody

EY Global Blockchain Leader

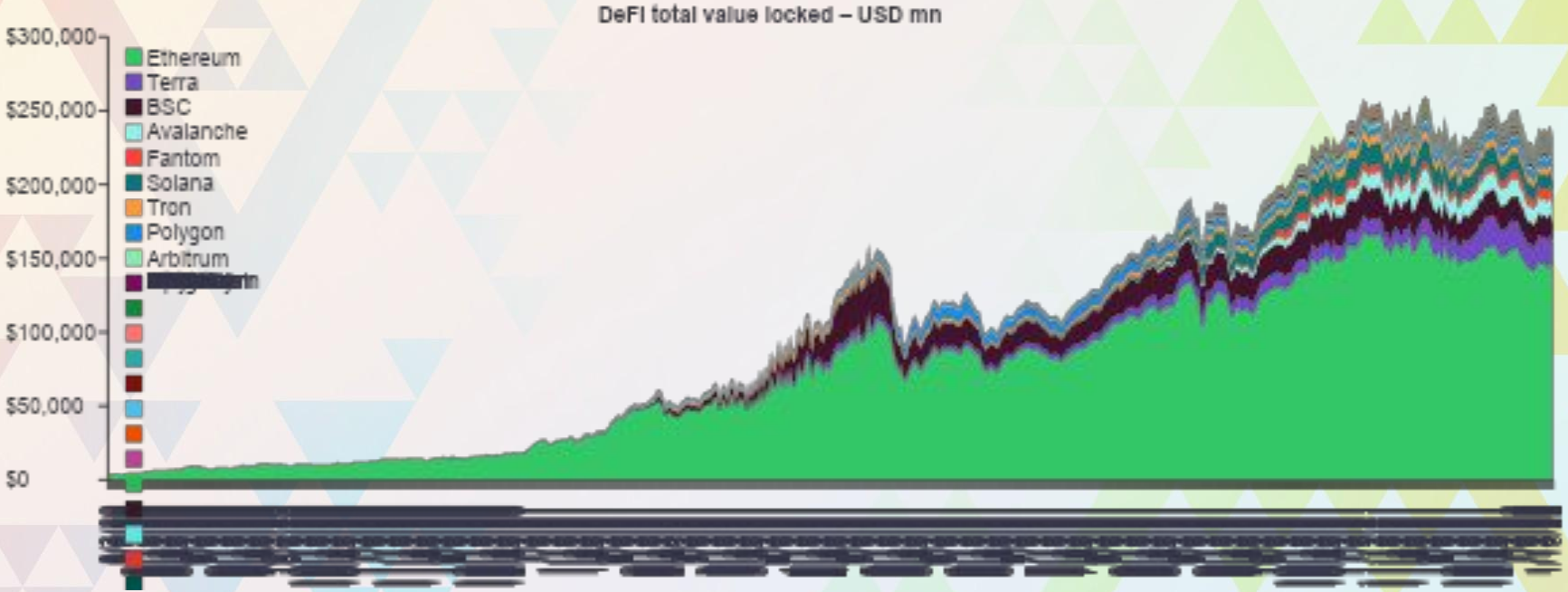
There isn’t much in the way of blockchain privacy today, though many are not bothered.



- Nearly all transaction data is readable in the clear
- Swaps, exchanges and mixers and liquidity pools all provide an element of pseudo-anonymity for individual users
- Large scale traders find their moves impossible to conceal

The lack of privacy hasn’t stopped the growth of some very powerful use cases.

The DeFi ecosystem is nearing $300bn in value



Source: DeFi LLAMA

For many financial & industrial use cases, however, privacy is essential

- Money and products are easily represented by digital tokens
- Most enterprise assets are unique to the enterprise – so they're too easy to follow around on the blockchain
- Enterprise purchases are not swaps – they are often complex smart contracts that contain unique and sensitive business information

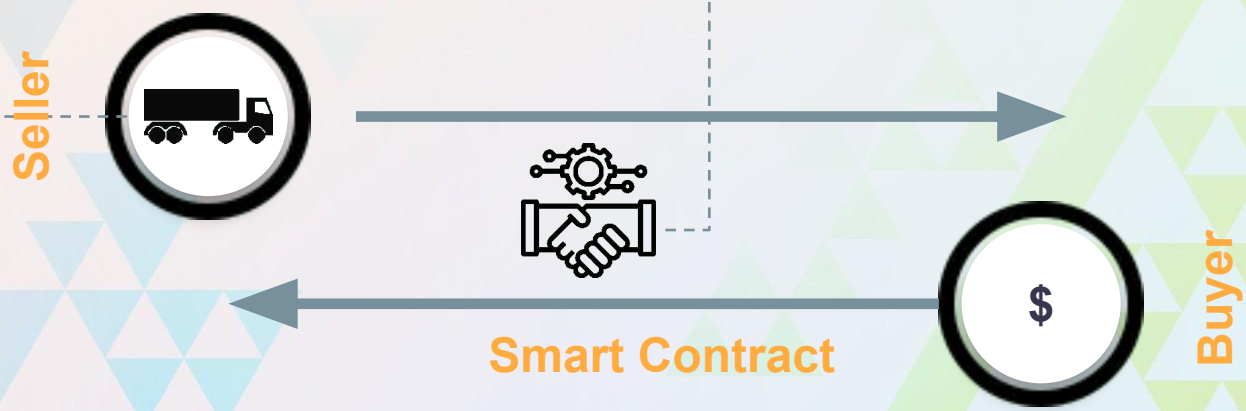
More than one kind of privacy tool is needed to unlock the universe of business applications

1 Asset Transfers and Payments

- Critical to keep what you're buying and how much you are paying overall, as well as when you buy and where it goes a secret from your competition

2 Smart Contract Terms

- The contract logic – the major terms & conditions, are also sensitive information because they usually contain price and rebate information based on expected volumes



Once we can handle both assets and logic, we can handle pretty much every transaction

1 Tokens

Asset tokens

Commodities

Currency tokens

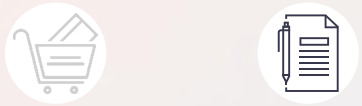
Rights tokens

Insurance tokens

Loans and leases

What items of value are being exchanged?

2 Contracts



Procurement contracts

Loans

Royalties

Sales

Securities

Retail promotions

What are the rules that govern this process?

3 Analytics

Transaction history

Fraud detection

Product traceability

Tax liability

How do we gain insight from this process?

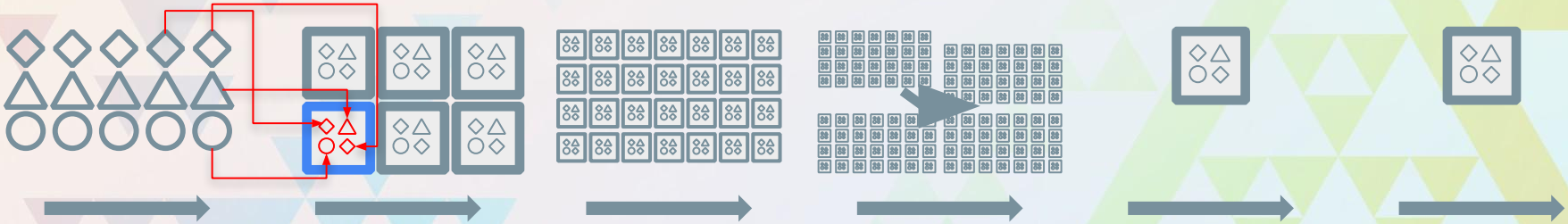
Polygon Nightfall gets us down the first half of this path, around asset transfer privacy

- Once you have assets inside of Polygon Nightfall, there is no external visibility to how it moves to external viewers
- Assets can be put in and cashed out
- Auditable histories can be prepared but requires the cooperation of the sender or receiver
- Many new business models are unlocked by this

Polygon Nightfall is in production beta. Polygon Nightfall is a product of Polygon Technology, not EY. EY developed the original nightfall code and has contributed that code into the public domain. EY does not control or manage Polygon Nightfall and retains no ownership over the Nightfall code. Nightfall is a public domain, open-source initiative to which any person or firm can contribute and EY continues to contribute new ideas and code as well based on our own thinking about how privacy technology needs to develop to support widespread adoption. You can find the original Nightfall information at https://github.com/eyblockchain/ . If you want to learn about Polygon Nightfall, please visit https://polygon.technology

EY OpsChain Supply Chain Manager is our first product that leverages privacy for industrial users

Raw materials	Manufacture	Transport	Warehouse	Sell	Support
• Purchase raw materials • Create digital tokens to represent those assets	• Integrate items together into manufacturing output • New digital token incorporates the materials	• Put finished goods into an in-transit status	• Move into warehouse with a distributor • Unload container and truck	• Transfer to a retailer • Transfer ownership first to retailer and then to end customer	• Build true end-to-end traceability for product history



With privacy enabled, you can now track end-to-end multi-company value chains without disclosing sensitive business information to your competition

Nightfall remains public domain and open source and we believe there is more work to be done

It's been a very long haul:

2017 Work Started

2018 Nightfall Prototype

2019 Nightfall Version 2

2020 Timber & Batching

2021 Nightfall Version 3

2022 Polygon Nightfall Production Beta

*Avg Per Tx Costs***

$100

$5

$2.5

$1.00

Delivered as public domain code free from any restrictions or conditions

Mainnet Beta Now Live as Polygon Nightfall

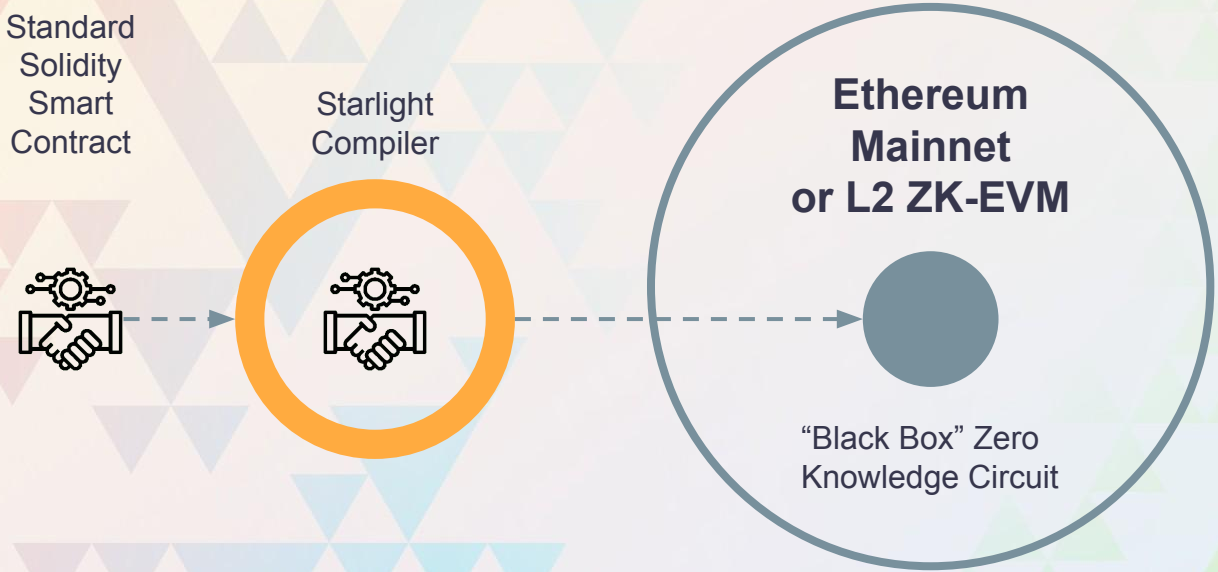
And there's a lot more to do:

- Regulatory compliance tools
- Improved audit integrations
- Privacy-enabled swaps
- NFT theft protection
- Metadata masking

** Transaction prices are approximate and will vary with network congestion and gas fees.

Polygon Nightfall is in production beta. Polygon Nightfall is a product of Polygon Technology, not EY. EY developed the original nightfall code and has contributed that code into the public domain. EY does not control or manage Polygon Nightfall and retains no ownership over the Nightfall code. EY does continue to contribute to the Nightfall code base and we develop new features in consultation with any member of the blockchain community that wishes to contribute. Other people and companies are free to contribute to this open source, public domain initiative. You can find the original Nightfall information at https://github.com/eyblockchain/ . If you want to learn about Polygon Nightfall, please visit https://polygon.technology

The next big challenge is making business logic private, a task we're focused on with Starlight



- Starlight enables on-chain logic that's not externally de-codeable
- Business relationships with specific terms & conditions can then be applied without disclosing them to the wider public
- Still subject to limitations of metadata "leakage" as transactions take place

eCommerce didn’t take off without encryption and blockchain won’t scale without privacy.

- SSL certificates became available starting in 1994 on the Netscape browser.
- Prior to that time, online credit card transactions were done in the clear, leading to low levels of consumer trust.
- The actual rate of online fraud in the early days was very low

Thank you!

Paul R. Brody

Principal, Ernst & Young LLP

EY Global Blockchain Leader

paul.brody@ey.com

@pbrody

blockchain.ey.com

Starlight

Devcon VI

Chaitanya Konda

Applied Cryptographer, Blockchain

Agenda

1. Intro to Starlight
2. How does the transpiler work?
3. zApp Architecture
4. Example

Zero Knowledge Applications, or zApps are Awesome but …..

They have a **steep learning curve**

Experience with **zero-knowledge proofs** (ZKPs)

Take **time** to build

Specialist ZKP devs need to be hired

Starlight was born to solve all these problems.

Zero Knowledge Applications, or zApps are awesome but …..

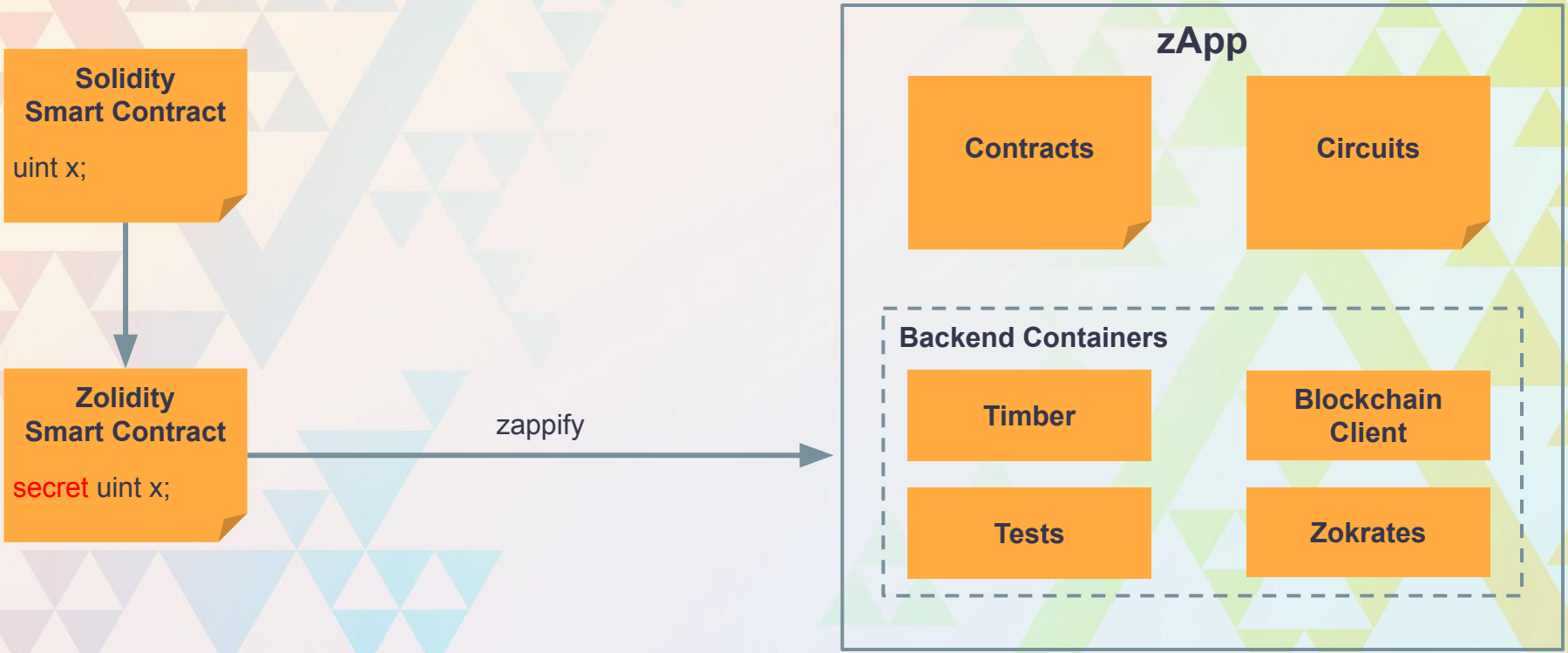
Ordinary smart contract myContract.sol

Decorated smart contract myContract.zol

Transpiler

Complete, working zApp

How does transpiler work?



Decorators – Secret

- What it does?
  - Contents of the variable remain confidential
- For
  - State variables
  - Function parameters
  - Functions (future enhancement)
- Not for
  - Local stack memory declarations
- How it works?
  - Create a commitment for this state variable that binds and hides the value

```
contract Example {

  secret uint x; // owned by the contract deployer

  function add(secret uint y) public {
    known x += y;
  }

}
```

Decorators – Known

- What it does?
  - Only the secret state variable owner can update it
- For
  - Incrementation statements of secret state variables
- How it works?
  - Proof of knowledge of existence of old commitment
  - Proof of knowledge of secret key of the public key in commitment
  - Nullifies old commitment
  - Create new commitment

```
contract Example {

  secret uint x; // owned by the contract deployer

  function add(secret uint y) public {
    known x += y;
  }

}
```

Decorators – Unknown

- What it does?
  - Anyone can increment this secret state variable
- For
  - Incrementation statements of secret state variables
- How it works?
  - Create a new ”part” commitment to hold only the value by which to update the amount
  - Secrete state variable is a partitioned variable whose value is a summation of all it’s “part” commitments

```
contract Example {

  secret mapping(address => uint)  balances;

  function deposit(uint amount) {
    balances[msg.sender] += amount;
  }

  function transfer(secret uint amount, secret
address recipient) {
    balances[msg.sender] -= amount;
    unknown balances[recipient] += amount;
  }

}
```

Commitment structure

Normal State Variable

hash(stateVarId, stateValue, ownerPublicKey, Salt)

- Unique state ID applied by solc
- Value state represents
- ZKP public key of the owner
- Random salt

Mapping State Variable

Secret mapping(address => uint256) balances;

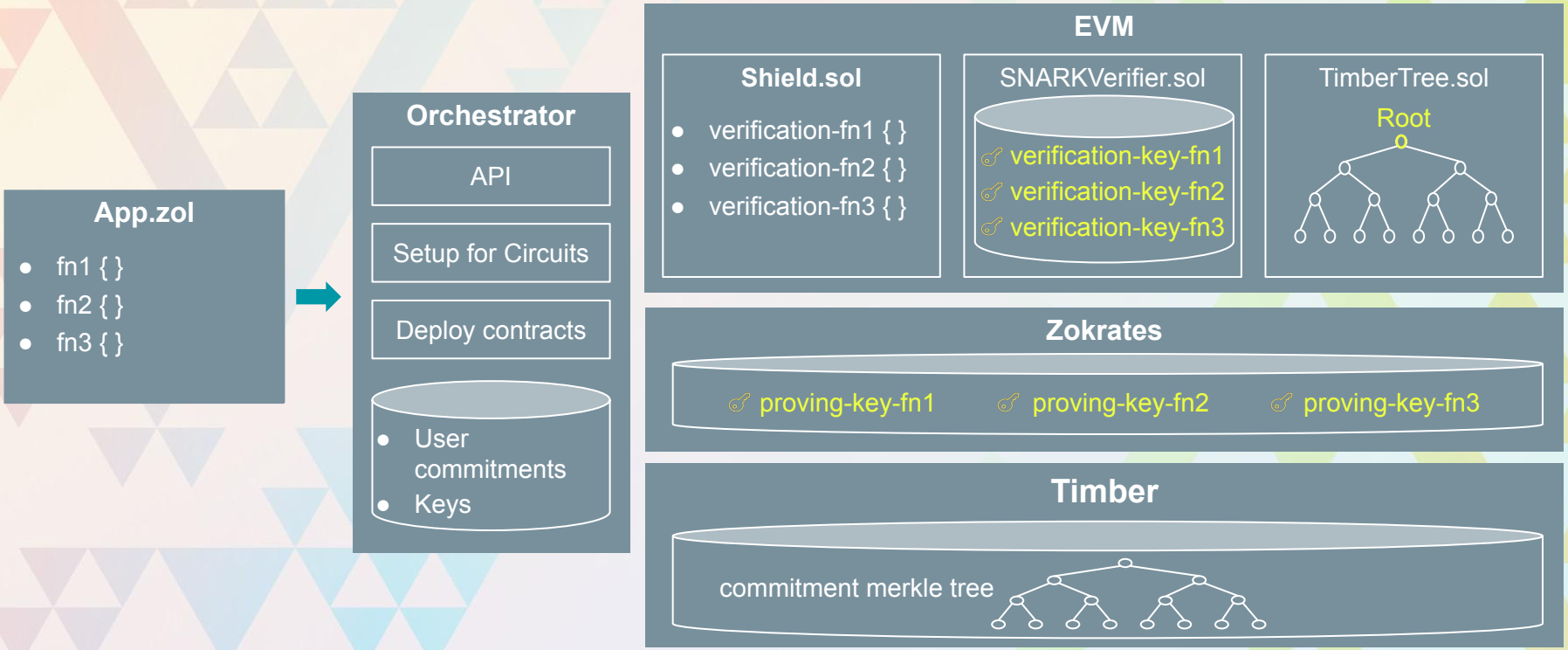
hash(hash(stateVarId, mappingKey), stateValue, ownerPublicKey, Salt)

- Mapping key (e.g., Alice's address) or array index

Transpilation Steps

1. Syntax verification
2. Dedecoration
3. Solc compilation
4. Redecoration
5. Generate Abstract Syntax Tree
   a. Circuits
   b. Shield contract
   c. Orchestrator
   d. Test
6. Code generation

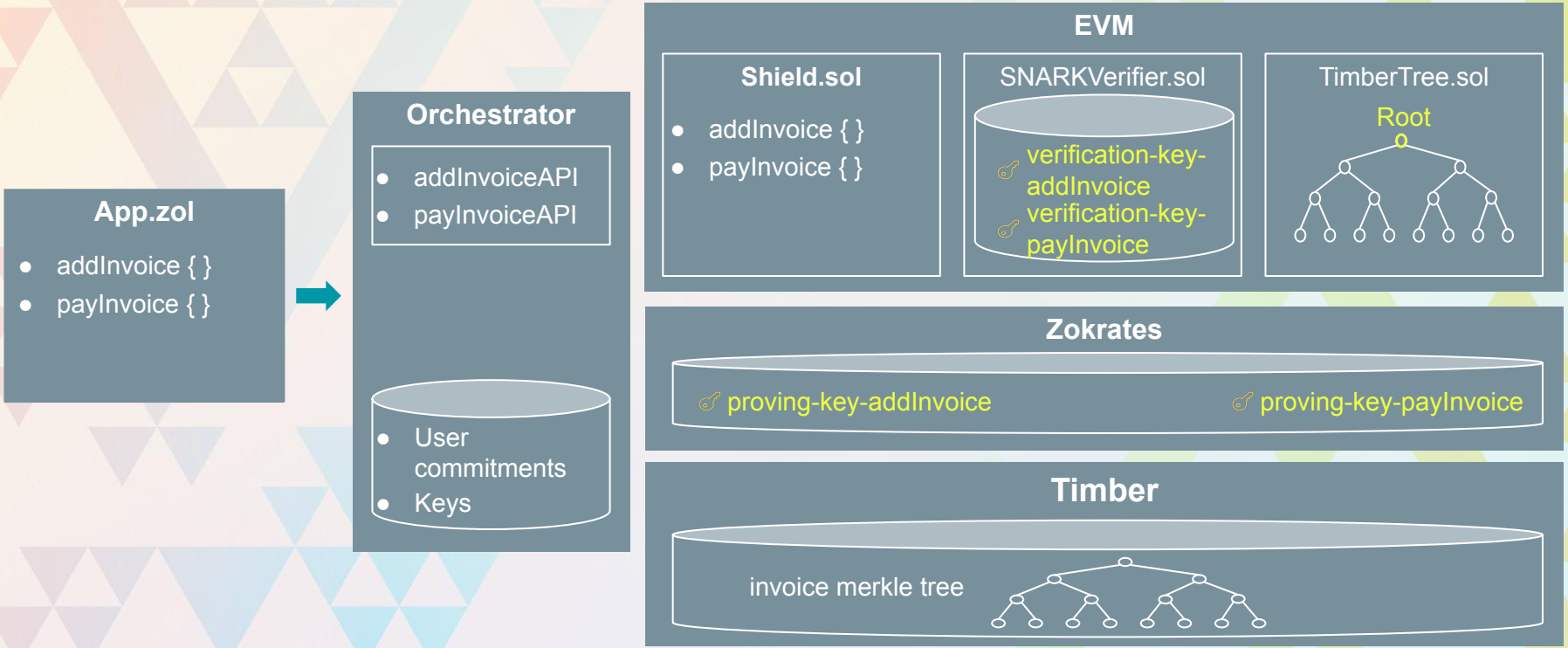
zApp Architecture



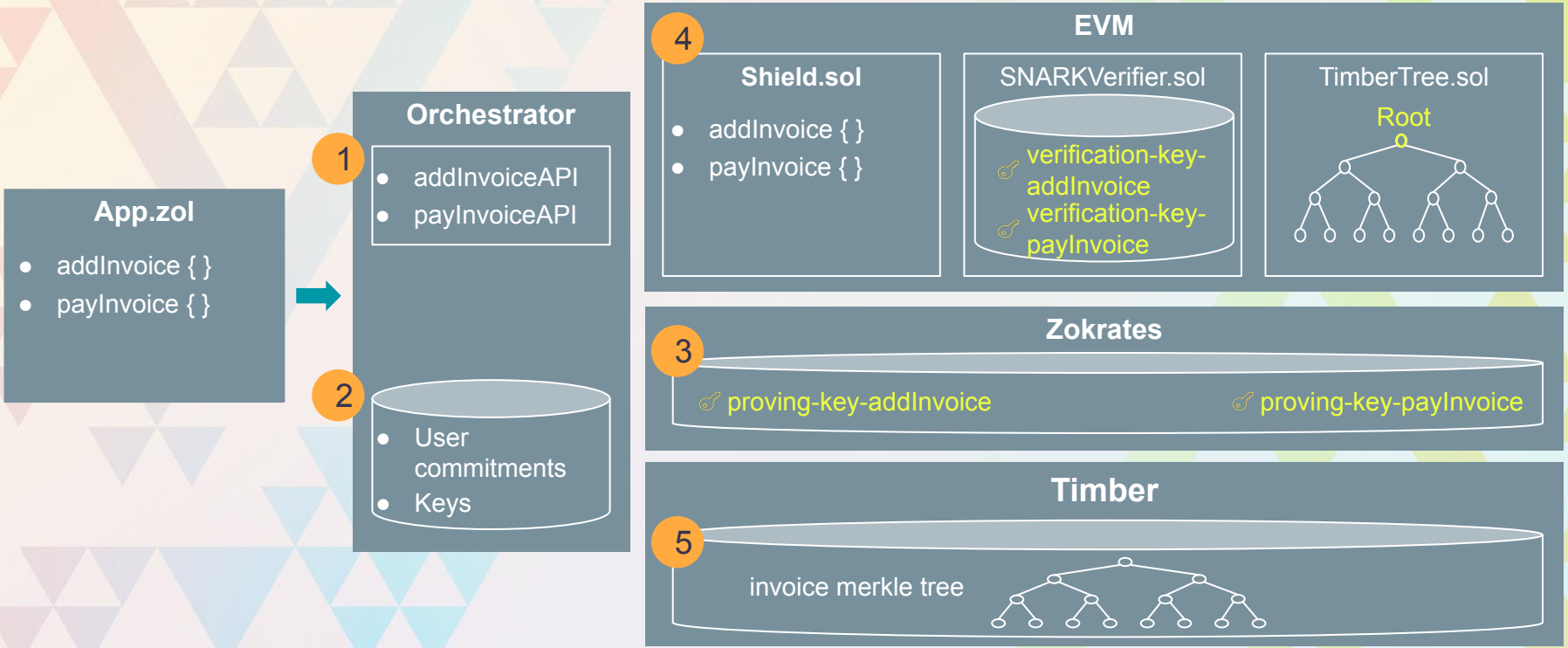
Example – Invoice.zol

```
contract Invoice {

  secret mapping(address => uint256) invoices;
  address contractOwner;


  function addinvoice(secret address owner, secret uint256
amount) public {
    require(invoices[owner] == 0);
    unknown invoices[owner] += amount;
 }


  function payInvoice(secret uint256 amount, secret address
owner) public {
    require(msg.sender == contractOwner);
    // imagine some payment here
    invoices[owner] – = amount;
 }

}
```

Calling ./zappify on Invoice.zol



When user calls addInvoiceAPI



Thank you!

Chaitanya Konda

Assistant Director, Ernst & Young LLP

EY Global Blockchain

ckonda@uk.ey.com

EY | Building a better working world
EY exists to build a better working world, helping create long-term value for clients, people and society and build trust in the capital markets.
Enabled by data and technology, diverse EY teams in over 150 countries provide trust through assurance and help clients grow, transform and operate.
Working across assurance, consulting, law, strategy, tax and transactions, EY teams ask better questions to find new answers for the complex issues facing our world today.
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. Information about how EY collects and uses personal data and a description of the rights individuals have under data protection legislation are available via ey.com/privacy. EY member firms do not practice law where prohibited by local laws. For more information about our organization, please visit ey.com.

EYG no. 007978-22Gbl
EYG no. 008839-22Gbl

ED None
This material has been prepared for general informational purposes only and is not intended to be relied upon as accounting, tax, legal or other professional advice. Please refer to your advisors for specific advice.
ey.com