Smart Contracts with Privacy

A Case Study With Renewable Energy

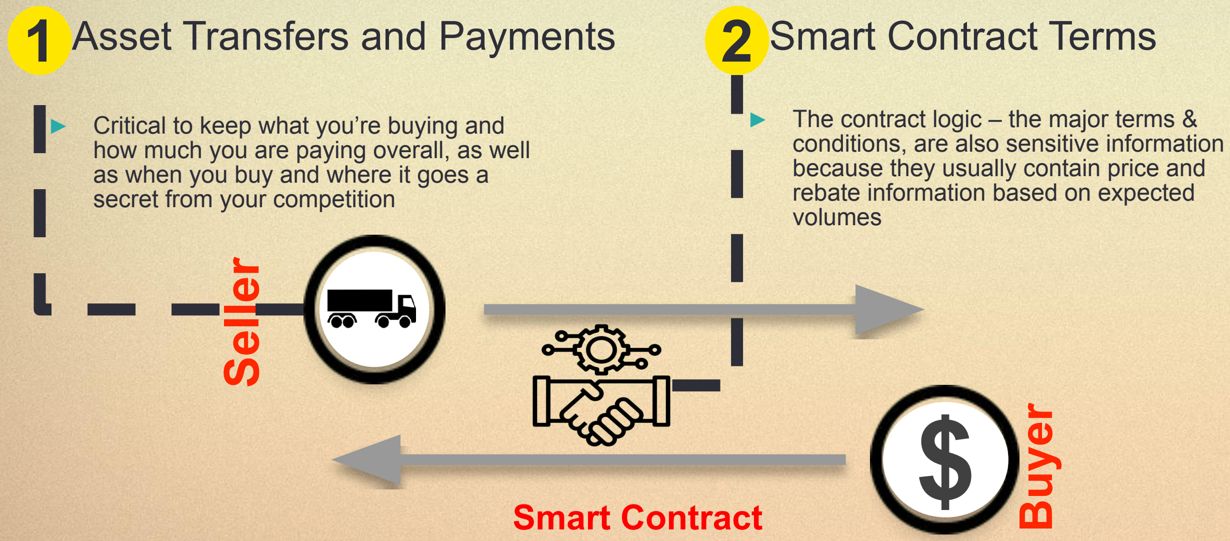
Paul Brody

Ernst & Young

Section 1

The Business Case for Privacy

Business users typically need two types of privacy. Neither of them are easy to execute.



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

- ❖ Privacy is a prerequisite for business users.
- ❖ Pseudo-privacy isn't good enough, neither is anonymity
- ❖ Hard to design without leaking data

Privacy may be difficult, but the return on investment is very high. Case example: Automating business contracts.

Microsoft's xBox network uses smart contracts for automation. Without privacy, systems like this can never migrate to public networks.

Less time needed to calculate rights and royalties owed

-99%

- From 45 days to less than 4 minutes to complete statements of account

Less cost to administer the entire system

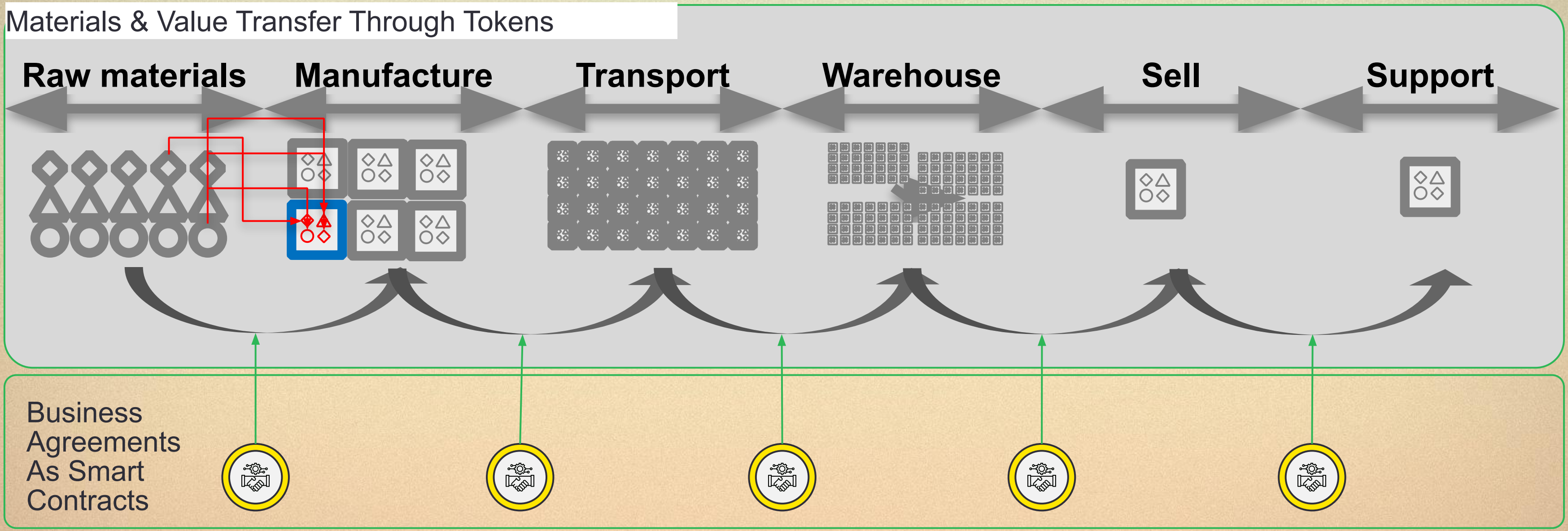
-40%

- Reduction in the cost to administer the system

Full transparency for all leading to less litigation

- Increased trust from all parties being allowed to examine the transaction logs and business logic in detail

When you put the pieces together, you can build an entire Enterprise business model on chain. That's the



Materials & Value Transfer Through Tokens
Raw materials
Manufacture
Transport
Warehouse
Sell
Support
Business Agreements As Smart Contracts

With their rigorous handling of inventory and assets, we estimate that many companies can cut up to 20% of their inventory simply by having a much more accurate picture of the end-to-end supply chain and movement of goods.

Section 2

Renewable Energy Case Example

Our roadmap to full privacy consists of several incremental steps rather than a single big leap.

Nightfall

- ❖ Layer 2 ZK roll-up for privacy
- ❖ For transferring tokens under privacy

Since 2018

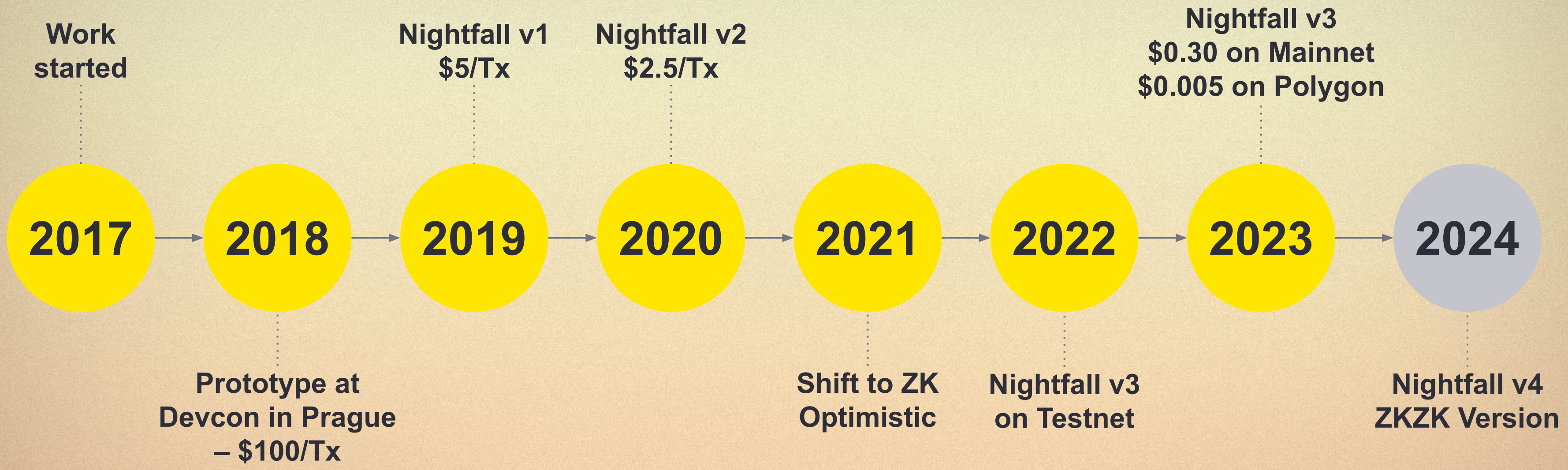
Starlight

- ❖ Transpiler for converting solidity contracts into zero knowledge circuits

May 2021

- ❖ Get each individual component working
- ❖ Enable very low cost asset transfers & payments
- ❖ Enable low cost business logic
- ❖ Integrate both Starlight and Nightfall together in Nightfall Version 5 using new ZK / Folding algorithms

This is part of a relatively long journey we have been on with a strong focus enterprise use cases.



2017
Work started

2018
Prototype at Devcon in Prague – $100/Tx

2019
Nightfall v1
$5/Tx

2020
Nightfall v2
$2.5/Tx

2021
Shift to ZK Optimistic

2022
Nightfall v3 on Testnet

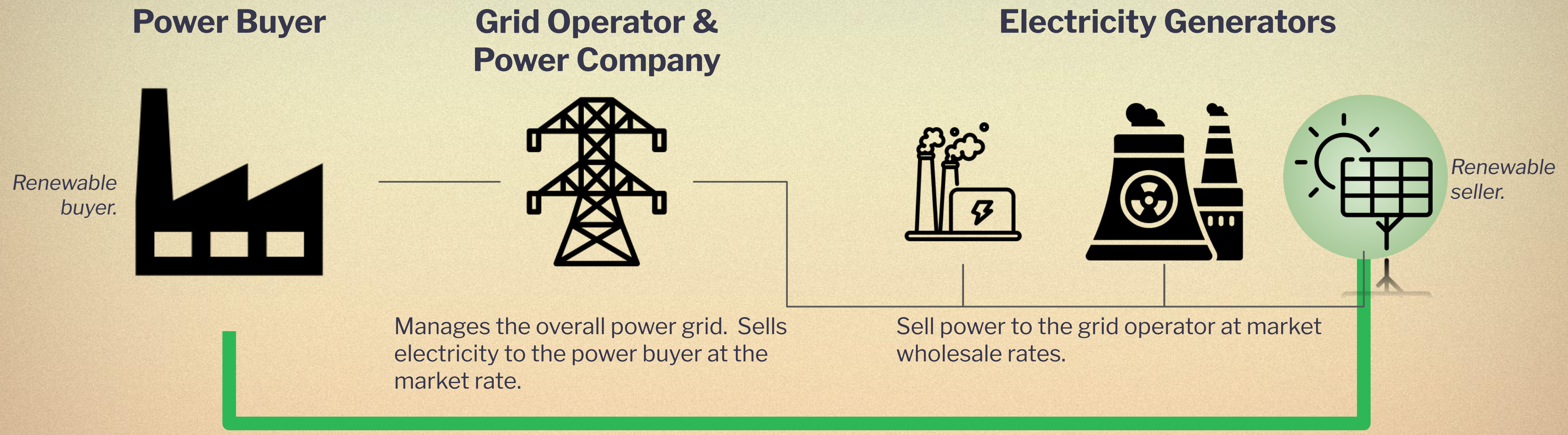
2023
Nightfall v3
$0.30 on Mainnet
$0.005 on Polygon

2024
Nightfall v4
ZKZK Version

Note: Efficiency calculation is based on gas consumption per transaction. The price per transaction is also affected by the cost of Eth, so even though the calculation is more than 1,000 times more efficient, the price of Eth has increased by around 1,000% since the original prototype debuted. Nightfall is in production. Nightfall is a public, decentralized Layer 2 network. EY developed the original nightfall code and has contributed that code into the public domain. EY does not control or manage 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 public domain code repository for Nightfall at https://github.com/eyblockchain/ .

Renewable energy contracts are critical to funding renewables infrastructure. Theyr’e aslo complicated.

Simplified version:



Power Buyer

Renewable buyer.

Grid Operator & Power Company

Manages the overall power grid. Sells electricity to the power buyer at the market rate.

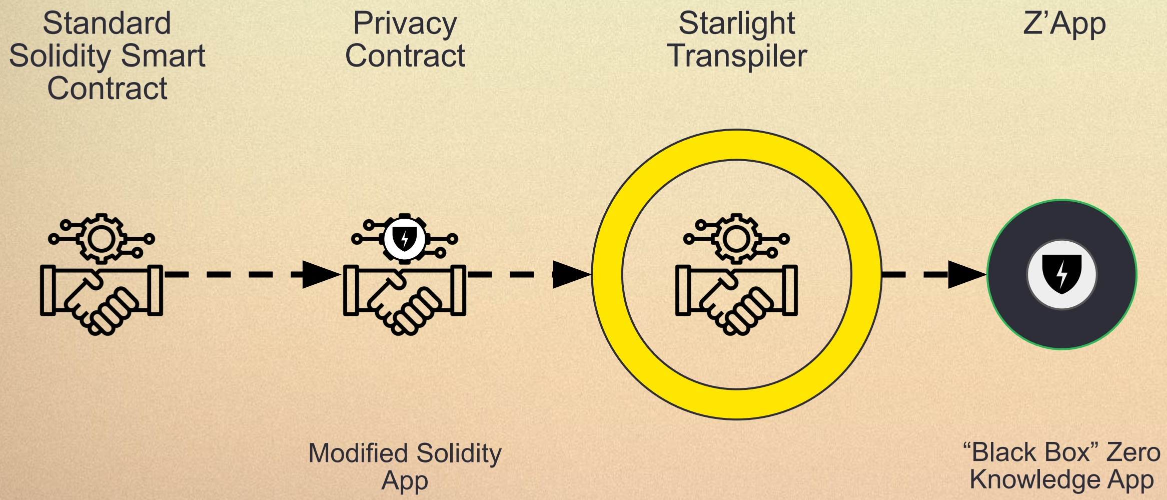
Electricity Generators

Renewable seller.

Sell power to the grid operator at market wholesale rates.

- ❖ Renewables company and our power user have a long-term power purchase agreement. These commitments are important for getting financing to build green energy facilities.
- ❖ However, green energy companies cannot build and run their own grid or sell directly to power buyers, they must sell through the grid at market prices.
- ❖ Renewables company and power user settle up after the fact based on their commitments for minimums and an agreed upon average price.
- ❖ Lots of variations on this by country and regulatory model

To build our zero knowledge circuit, we started with a public version in a plain solidity contract.


Standard Solidity Smart Contract
Privacy Contract
Starlight Transpiler
Z'App
Modified Solidity App
"Black Box" Zero Knowledge App

- ❖ 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
- ❖ Starlight allows anyone to build their own privacy-enabled applications.

Starlight is a public domain, open-source contribution to the Ethereum ecosystem. The Starlight repository contains work from us and others. The Starlight repository can be found at https://github.com/eyblockchain/.

Once deployed on-chain, the contract receives data from external sources to determine the amounts due

Current Iteration:

- Data comes from external sources including consumption and prices
- Smart contract calculates amount owed
- Current iteration is stateless
- Tx cost is about 0.06 ETH
- Best location is on a layer 2 for lower cost

Future Path:

- Integration to tokenized on-chain payment done under privacy
- Off-chain data storage with commitments to track payments, consumption

Please join us in maturing the state of on-chain privacy.

Our tools are public domain and open source.

GitHub.com/eyblockchain/

Swati Rawal - Research
Jiaje Zhang - Research
Lydia Garms - Research
Michael Livesey - Research

Dattatray Jhadav - Engineering

Talk with our team here today. We're ready to help you build privacy applications.

Thank you!

Paul Brody

Global Blockchain Leader
paul.brody@ey.com
@pbrody