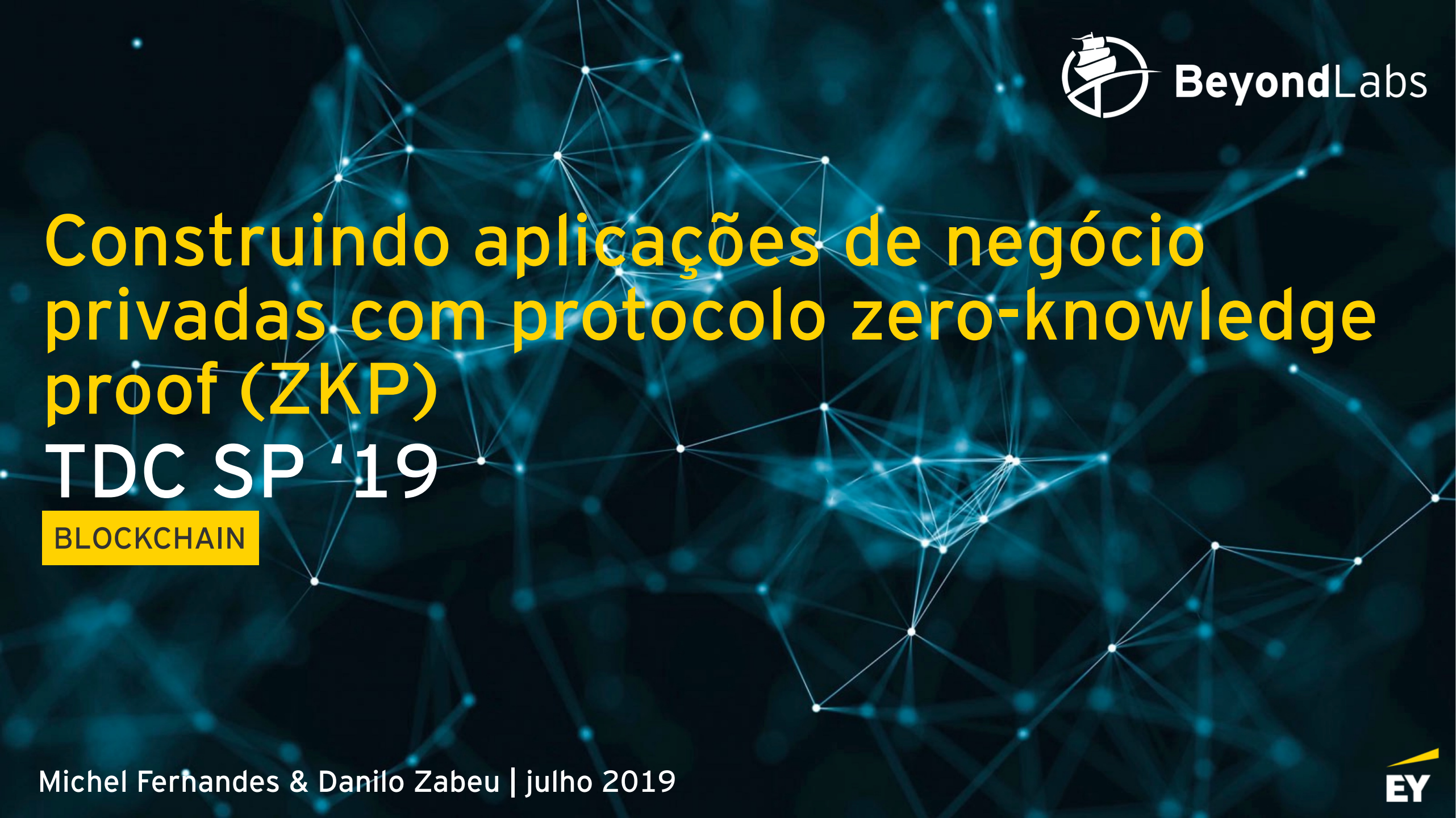

BeyondLabs
Construindo aplicações de negócio privadas com protocolo zero-knowledge proof (ZKP)
TDC SP '19
BLOCKCHAIN
Michel Fernandes & Danilo Zabeu | julho 2019
EY

DANILO ZABEU

BLOCKCHAIN LEAD

MICHEL FERNANDES

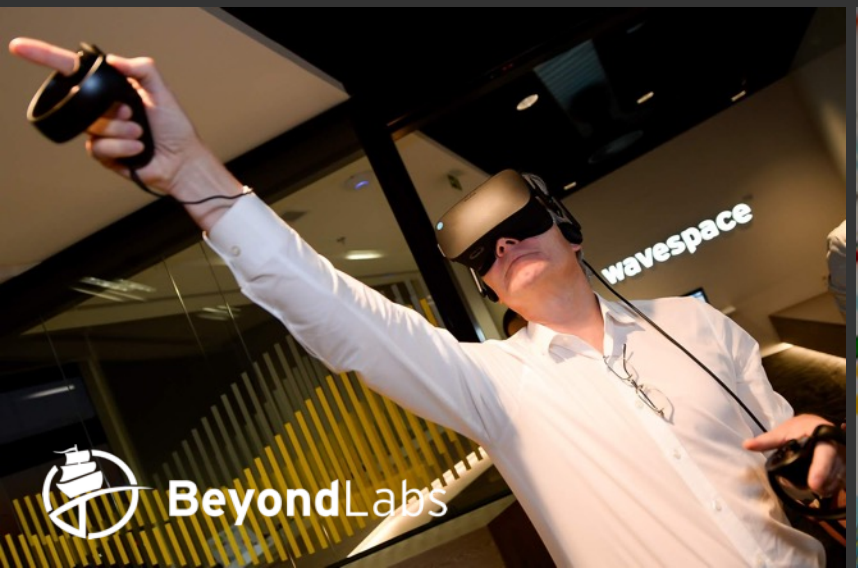
CHIEF ENGINEER

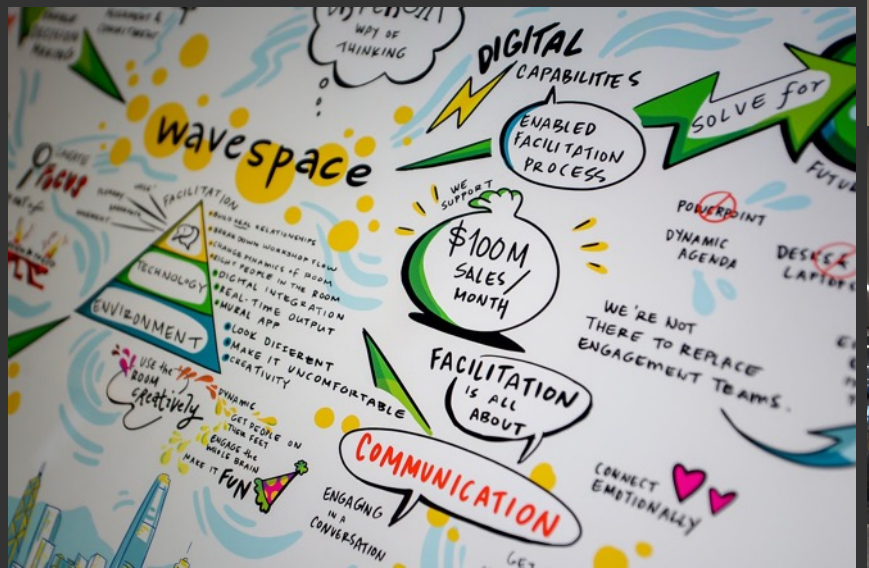

EY
Building a better working world
#bewavespace
BeyondLabs
EY


wavespace™


#beWavespace


wavespace


wavespace
BeyondLabs


wavespace
DIGITAL CAPABILITIES
ENABLED FACILITATION PROCESS
SOLVE FOT
$100M SALES/MONTH
POWERPOINT
DYNAMIC AGENDA
WE'RE NOT THERE TO REPLACE ENGAGEMENT TEAMS.
FACILITATION IS ALL ABOUT
COMMUNICATION
CONNECT EMOTIONALLY
ENGAGING IN A CONVERSATION
TECHNOLOGY
ENVIRONMENT
MAKE IT FUN


space™
EY

ECOSISTEMA

CRYPTOECONOMICS

BUSINESS APPLICATIONS
aka SMART CONTRACTS

ETHEREUM | QUORUM | HYPERLEDGER FABRIC | CORDA

PUBLIC | PERMISSIONED

DISTRIBUTED LEDGER TECHNOLOGY BACKED BY BLOCKCHAIN

BeyondLabs

EY

SMART CONTRACT

- STANDARDIZED TOKENS
- RULES
- DESIGN PATTERNS
- AUDIT & SECURITY
- PUBLICITY

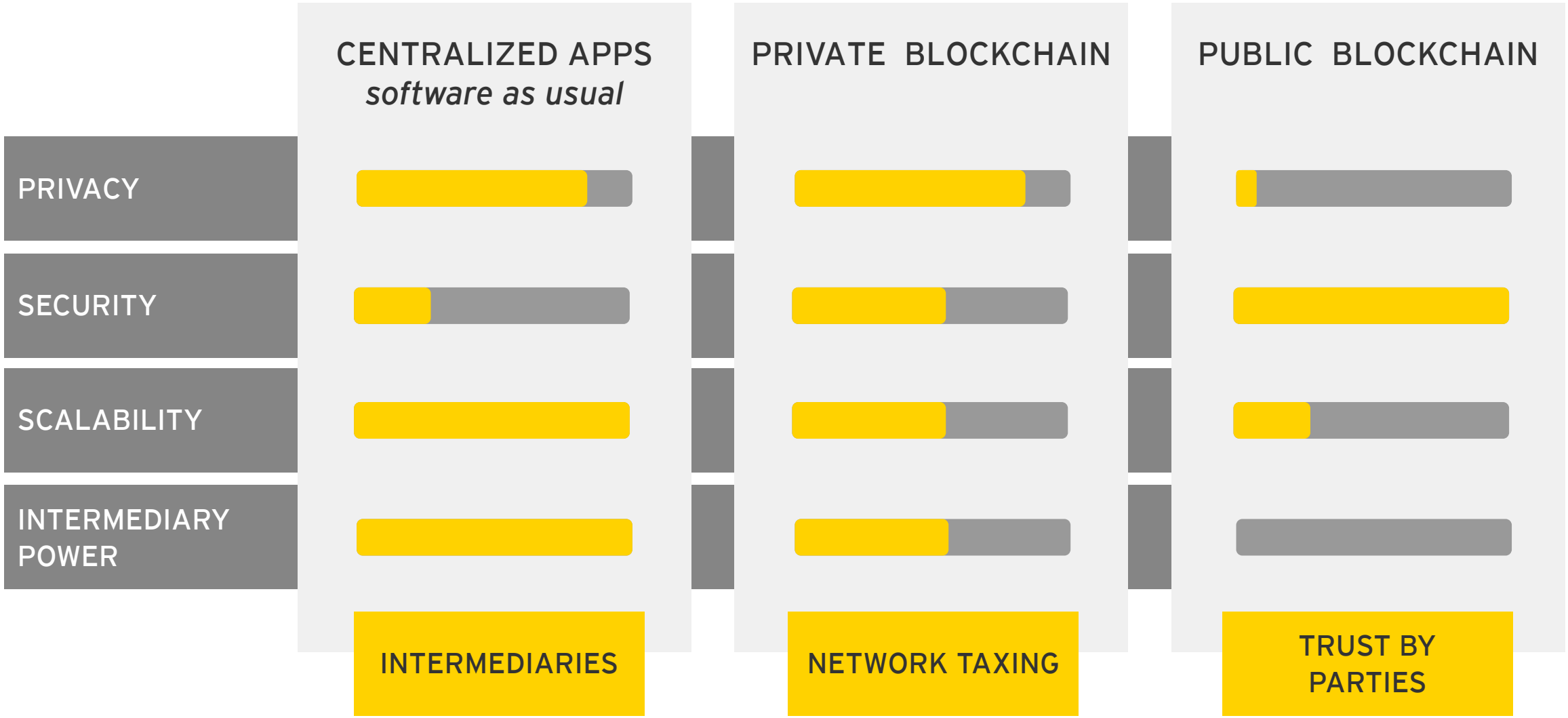
MUST FOLLOW PRINCIPLES AND PATTERNS IN THE SAME WAY OF APPLICATION DEVELOPMENT

USING STANDARDIZED TOKENS ENABLES INTEROPERABILITY AND PORTABILITY BETWEEN PARTICIPANTS

PUBLIC = UNIVERSAL APPS
PRIVATE = SPECIALIZED APPS

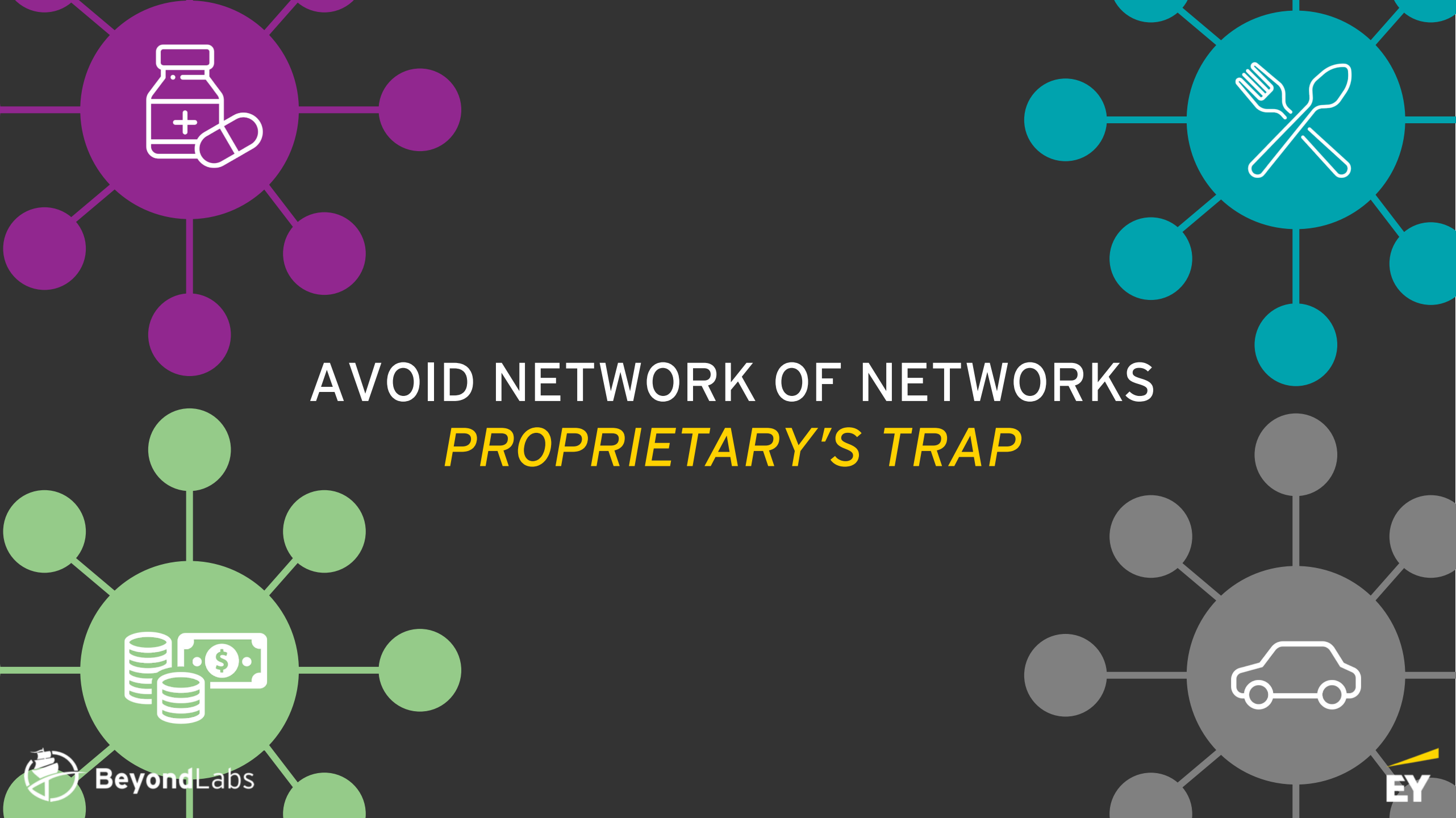
CHOOSE A PLATFORM THAT WILL ENABLE FRICTIONLESS MIGRATION FROM PRIVATE TO PUBLIC

PLATAFORMAS PÚBLICAS E PRIVADAS



BeyondLabs

EY


AVOID NETWORK OF NETWORKS
PROPRIETARY'S TRAP
BeyondLabs
EY

BUSINESS INTEGRATION

CONTRACT

Paper contracts

ORDER

Purchase order sent by email through ordering app against contracts

FULFILL

Shipment and email sent through tracking logistics app

INVOICE

Invoice sent by email through the seller's ERP app

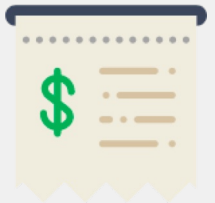
PAY

Bank transfer after 60 days sent by the buyer through the buyer's ERP app

BeyondLabs

EY

BUSINESS INTEGRATION

CONTRACT	ORDER	FULFILL	INVOICE	PAY
				
Paper contracts	Purchase order sent by email through ordering app against contracts	Shipment and email sent through tracking logistics app	Invoice sent by email through the seller's ERP app	Bank transfer after 60 days sent by the buyer through the buyer's ERP app
SMART CONTRACTS	SIGNAL	NON-FUNGIBLES TOKENS	SIGNAL	FUNGIBLE TOKENS

ONE PUBLIC BLOCKCHAIN PLATFORM: **ETHEREUM**

BeyondLabs

EY

ONE TO RULE THEM ALL

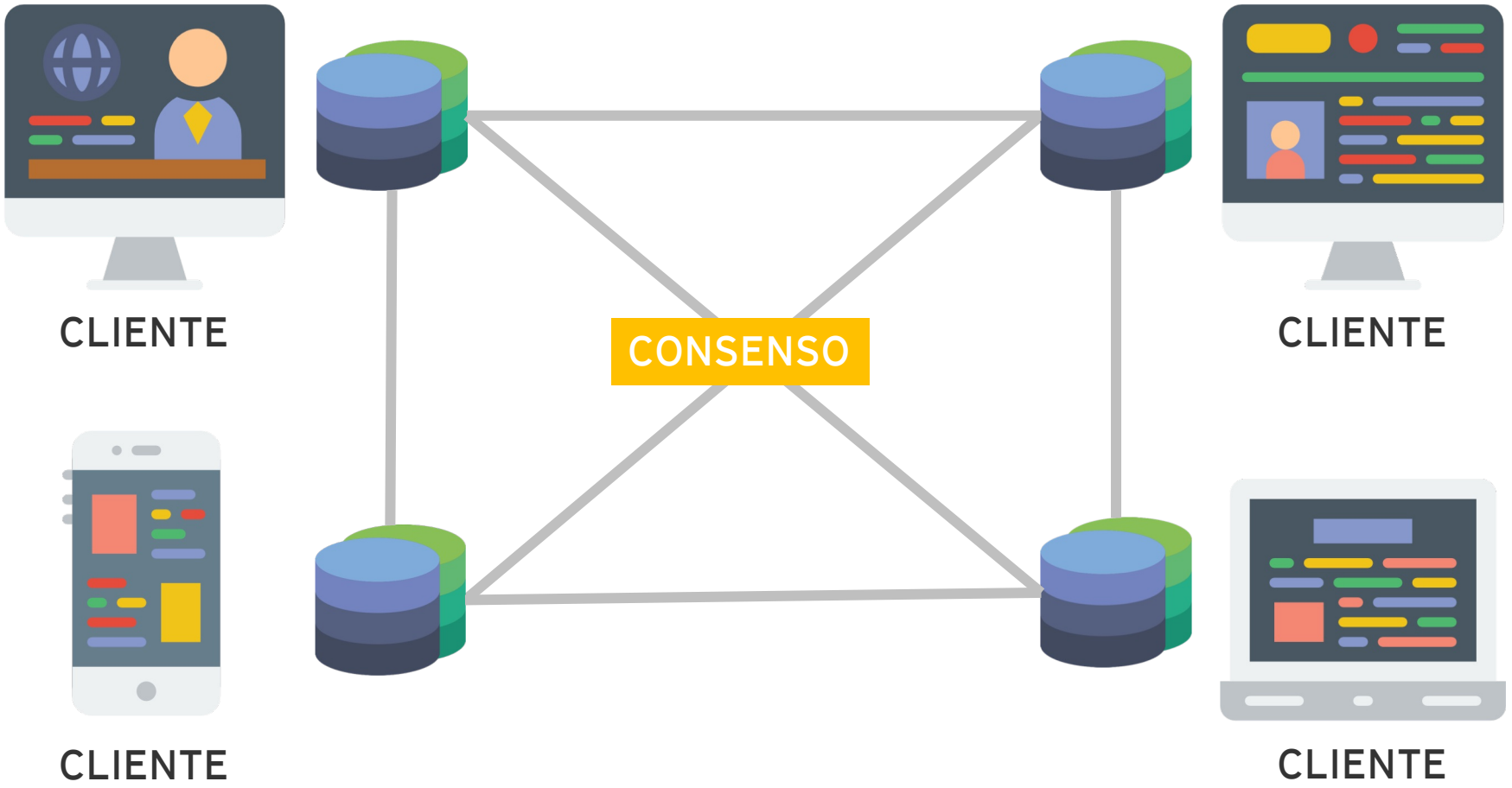
"One day you get a call from a very large buyer saying, 'Would you like to join my private blockchain?' You say, 'Okay.' And then you get the same call from your wholesaler, your suppliers, your shipper, your insurance company and maybe even your bank...or several of each of these! Suddenly you are spending all your time – and a lot of money – juggling dozens of blockchains. When the next partner calls, you say, 'Just fax me the order.' "

Paul Brody

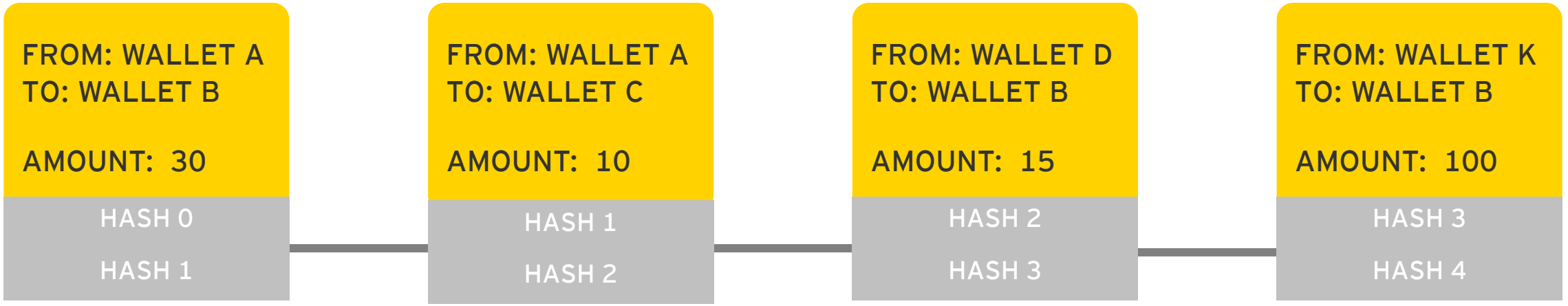
BeyondLabs

EY

BLOCKCHAIN ATUAL PÚBLICO



CUSTO DO DESIGN



Token BNB

Binance | Exchange

Buy | Earn Interest | Crypto Credit

Overview [ERC-20]

PRICE
$33.9027 @ 0.116999 Eth (-5.84%)

FULLY DILUTED MARKET CAP
$562,089,763.32

Total Supply: 16,579,517.055253... BNB

Holders: 317,739 addresses

Profile Summary

Contract: 0xB8c77482e45F1F44dE1745F52C74426C631bDD52

Decimals: 18

Official Site: https://www.binance.com/

Social Profiles:

Announcement: Binance Chain Mainnet Swap

FILTERED BY TOKEN HOLDER
0xe1743b9f9b65e41b51970befdf5a60f3161f536a

BALANCE
369.5018675 BNB

VALUE
$12,527.10 (~43.2312 Eth) [0.0022%]

Transfers | Info | Exchange | Read Contract | Write Contract | Analytics

0xe1743b9f9b65e41b5197...

A total of 6 transactions found

First | < | Page 1 of 1 | > | Last

Txn Hash	Age	From		To	Quantity
0xe5b394f1eeb4bd...	17 mins ago	0xe1743b9f9b65e4...	OUT	0x74bee08fd2ce34a...	50

PRIVACIDADE

BeyondLabs

EY

ZKP

ZERO KNOWLEDGE PROOF

BeyondLabs

EY

A CAVERNA DO ALI BABA

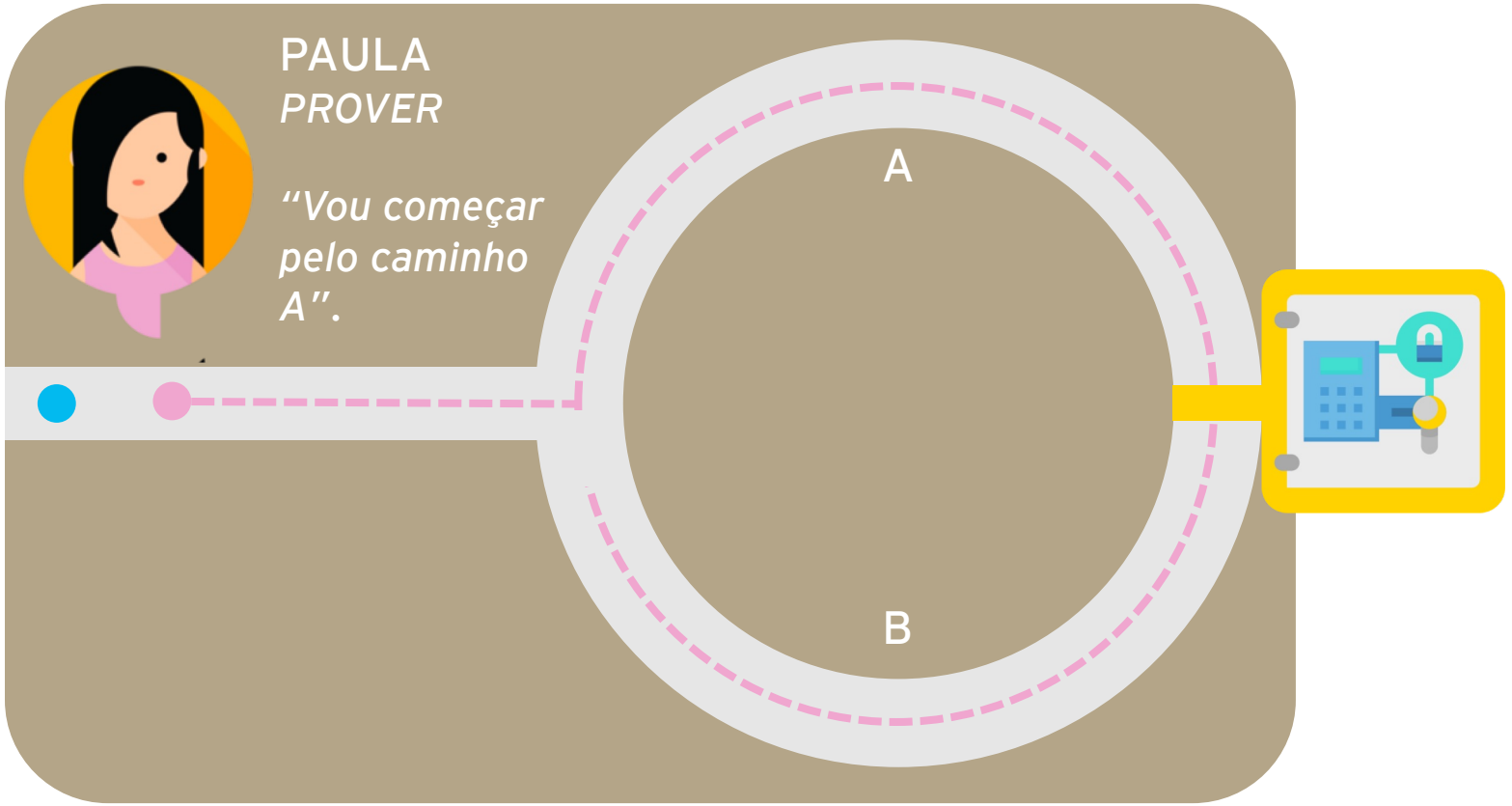
BeyondLabs

EY

PROVA DE ZERO CONHECIMENTO

VICTOR
VERIFIER

"Se você tem o código, vá pelo caminho A."



PORTA
CODIFICADA
KNOWLEDGE

BeyondLabs

EY

COMPLETUDE
COMPLETENESS

UM PROVADOR HONESTO SEMPRE SERÁ CAPAZ DE CONVENCER UM VERIFICADOR

SOLIDEZ
SOUNDNESS

UM PROVADOR MALICIOSO NÃO DEVERÁ SER CAPAZ DE CONVENCER UM VERIFICADOR

ZERO CONHECIMENTO
ZERO-KNOWLEDGE

NÃO SERÁ REVELADO NENHUMA INFORMAÇÃO

PROVA DE ZERO CONHECIMENTO

"Eu sei **x**, tanto que **y = F(x)**".

PROVER

- **F** *function*
- **y** *claimed output*
- **x** *private input*

VERIFIER

- **F** *function*
- **y** *claimed output*

BeyondLabs

EY

zk-SNARKS

ZERO-KNOWLEDGE SUCCINCT NON-INTERACTIVE ARGUMENT OF KNOWLEDGE PROOFS

ARGUMENTO
ARGUMENT

SOLIDEZ ALCANÇADA POR UM VERIFICADOR POLINOMIAL ASSOCIADO

NÃO INTERATIVO
NON-INTERACTIVE

SEM INTERAÇÃO ENTRE O PROVADOR E O VERIFICADOR

SUSCINTO
SUSCINT

VERIFICAÇÃO RÁPIDA, NÃO DEPENDE DO TEMPO DE EXECUÇÃO DA FUNÇÃO

BeyondLabs

EY

FUNCIONAMENTO DO ZK-SNARKS

SETUP DOS PARES DE CHAVES PRIVATE/PUBLIC PARA GERAR CHAVES DE PROVA E VERIFICAÇÃO SEQUÊNCIA NUMÉRICA LAMBDA

COM A CHAVE DE PROVA, ENTRADA PÚBLICA (*ENDEREÇO DO ETHEREUM*) E A *PRIVATE WITNESS* (INFORMAÇÃO) É GERADO UMA **PROVA**

VERIFICAÇÃO REALIZADA A PARTIR DA CHAVE DE VERIFICAÇÃO, ENTRADA PÚBLICA E PROVA, SENDO UMA FUNÇÃO BOOLEANA PARA O RESULTADO.


TRUSTED SETUP
TOXIC WASTE
BeyondLabs
EY

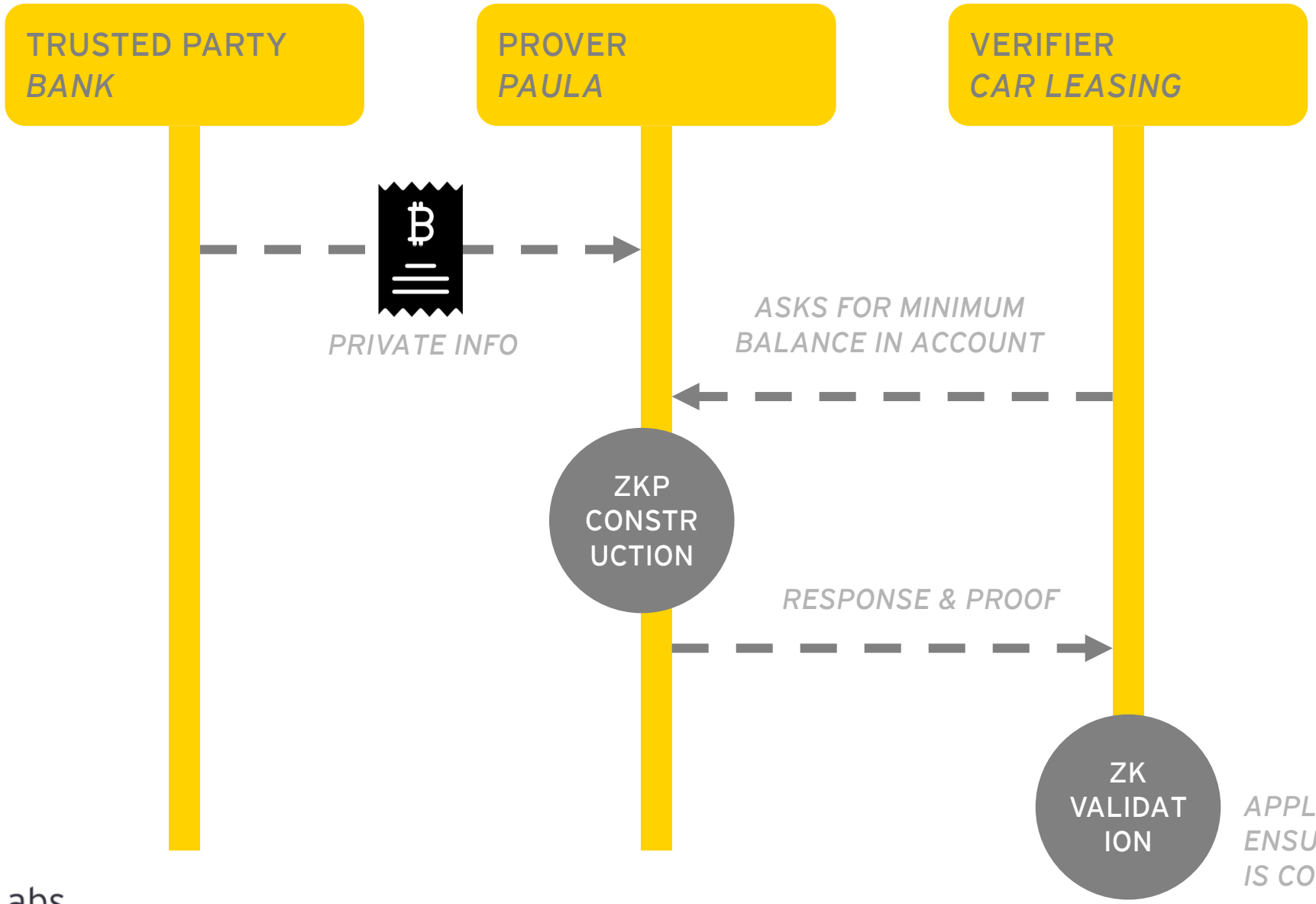
TAU CERIMONY

ZCASH

BeyondLabs

EY

SIMPLE DATA EXCHANGE EXAMPLE



BeyondLabs

EY

APLICAÇÕES

VALIDAÇÃO DE ID

AUTENTICAÇÃO

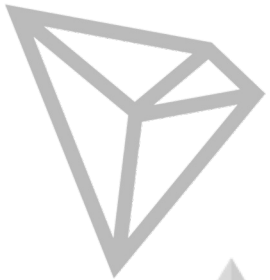
VOTAÇÃO

MENSAGENS

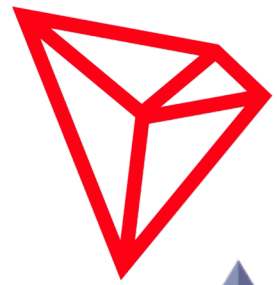
BeyondLabs

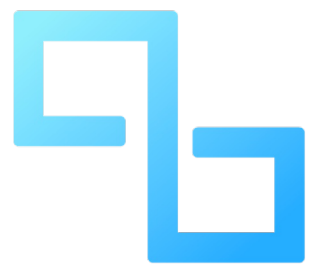
EY

EMPRESAS E PLATAFORMAS QUE USAM ZKP



EMPRESAS E PLATAFORMAS QUE USAM ZKP





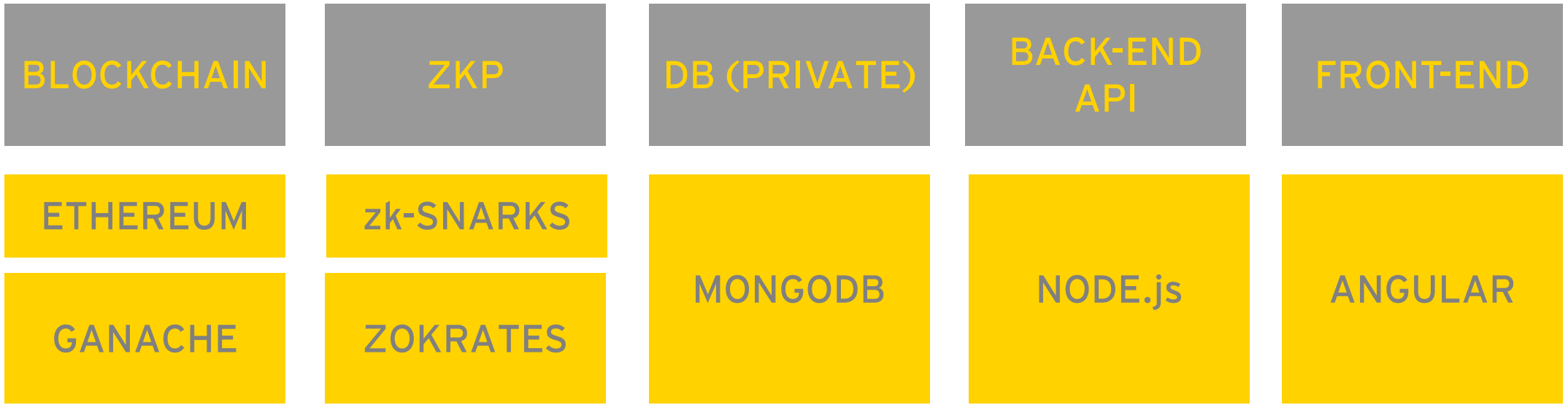
NIGHTFALL

WELCOME

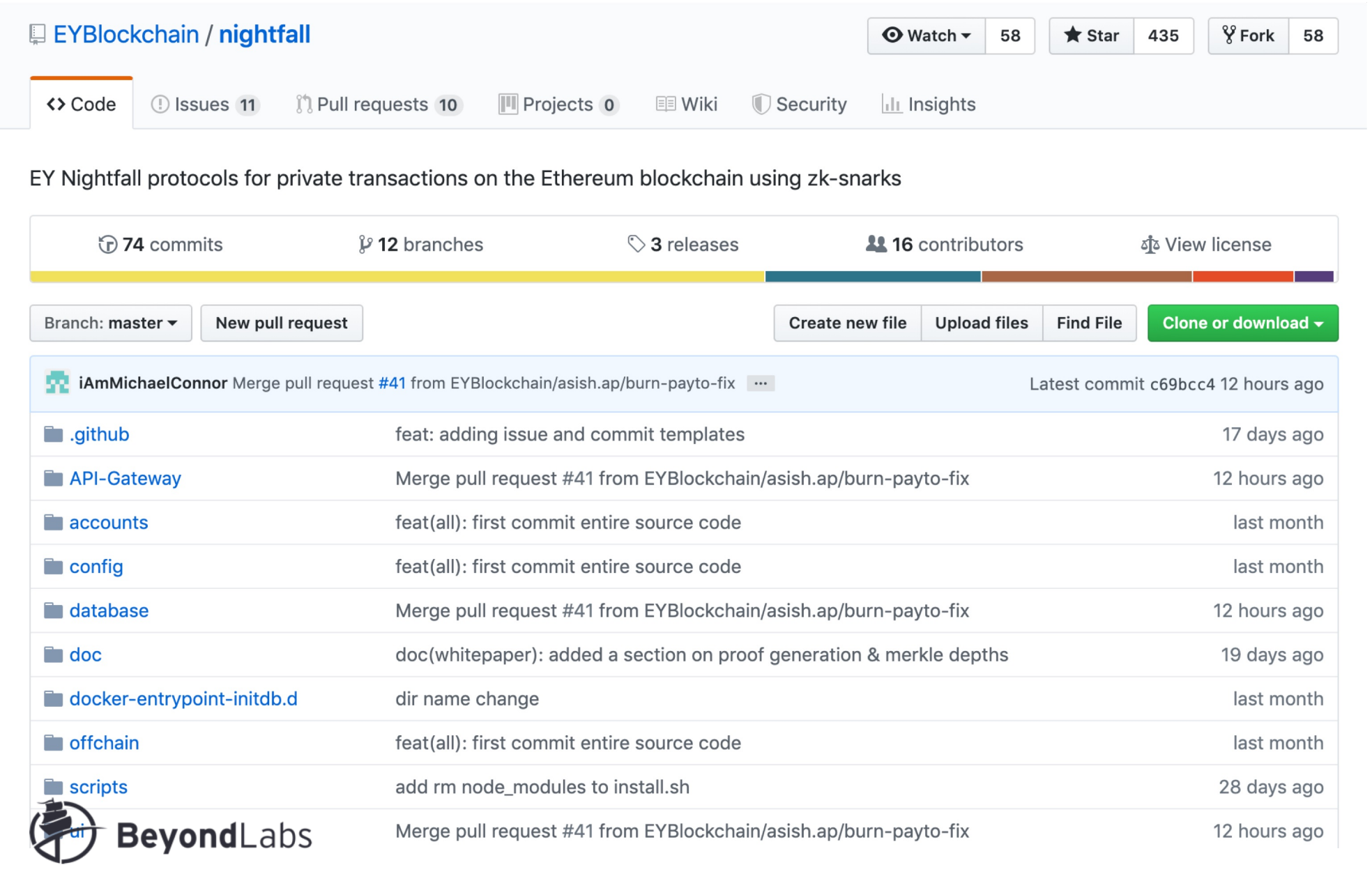
BeyondLabs

EY

NIGHTFALL'S STACK



https://github.com/EYBlockchain/nightfall



PUBLIC DOMAIN

OPEN SOURCE

ACCEPTING PULL REQUESTS ☺

ALPHA

BeyondLabs

EY

ZKP Demo

michel | Sign Out

Account Balance

0	1	50	50
ERC-721: EYToken (EYT)	EYToken Commitments	ERC-20: EY OpsCoin (OPS)	EY OpsCoin Commitments

Actions

MINT EYTOKEN	MINT EYTOKEN COMMITMENT	MINT EY OPSCOIN	MINT EY OPSCOIN COMMITMENT
TRANSFER EYTOKEN	TRANSFER EYTOKEN COMMITMENT	TRANSFER EY OPSCOIN	TRANSFER EY OPSCOIN COMMITMENT
BURN EYTOKEN	BURN EYTOKEN COMMITMENT	BURN EY OPSCOIN	BURN EY OPSCOIN COMMITMENT

Transactions History

EYToken | EYToken Commitment | EY OpsCoin | **EY OpsCoin Commitment**

Type	Coin Value	Coin Commitment	Coin 1 Value	Coin 1 Commitment	Coin 2 Value	Coin 2 Commitment	Date	Send To
MINTED	OPS 50	0xba588fb7ad70b7775f...					13/07/2019 02:08:37 PM	

BeyondLabs

EY

ZKP Demo

zabeu Sign Out

Account Balance

0	1	0	1
ERC-721: EYToken (EYT)	EYToken Commitments	ERC-20: EY OpsCoin (OPS)	EY OpsCoin Commitments

Actions

MINT EYTOKEN	MINT EYTOKEN COMMITMENT	MINT EY OPSCOIN	MINT EY OPSCOIN COMMITMENT
TRANSFER EYTOKEN	TRANSFER EYTOKEN COMMITMENT	TRANSFER EY OPSCOIN	TRANSFER EY OPSCOIN COMMITMENT
BURN EYTOKEN	BURN EYTOKEN COMMITMENT	BURN EY OPSCOIN	BURN EY OPSCOIN COMMITMENT

Transactions History

EYToken | EYToken Commitment | EY OpsCoin | **EY OpsCoin Commitment**

Type	Coin Value	Coin Commitment	Coin 1 Value	Coin 1 Commitment	Coin 2 Value	Coin 2 Commitment	Date	Send To
RECEIVED	OPS 1	0x6dbd0d3681c8ee4409...					13/07/2019 02:32:44 PM	

BeyondLabs

EY

REFERÊNCIAS

- Zero Knowledge Proofs - Computerphile – YouTube, https://www.youtube.com/watch?v=HUs1bH85X9I
- Introduction to zk-SNARKs (Part 1), https://blog.decentriq.ch/zk-snarks-primer-part-one/
- Introduction to zkSNARKs with Examples – ConsenSys Media, https://media.consensys.net/introduction-to-zksnarks-with-examples-3283b554fc3b
- Explain Like I'm 5: Zero Knowledge Proof (Halloween Edition), https://hackernoon.com/eli5-zero-knowledge-proof-78a276db9eff
- Zerocash: improving Bitcoin using SNARKs – YouTube, https://www.youtube.com/watch?v=S6qOj9ap6RM
- JavaScript API · ethereum/wiki Wiki, https://github.com/ethereum/wiki/wiki/JavaScript-API#web3ethgettransaction
- ZoKrates – A Toolbox for zkSNARKs on Ethereum – YouTube, https://www.youtube.com/watch?v=sSIrywb5J_0
- Managing your accounts · ethereum/go-ethereum Wiki, https://github.com/ethereum/go-ethereum/wiki/Managing-your-accounts
- JPM Develops New Privacy-Enhancing Tool for Payment Mechanisms on ETH Blockchain, https://cointelegraph.com/news/jpm-develops-new-privacy-enhancing-tool-for-payment-mechanisms-on-eth-blockchain

REFERÊNCIAS

- Irish banking industry first in Europe in building new education platform based on blockchain | Institute of Banking, https://www.iob.ie/?q=node/2282
- The rush for zero-knowledge proofs, and where it leaves privacy coins, https://hackernoon.com/the-rush-for-zero-knowledge-proofs-and-where-it-leaves-privacy-coins-32efdf27f18b
- Ethereum transactions, 500 TPS thanks to ZkSnarks - The Cryptonomist, https://cryptonomist.ch/en/2018/09/24/ethereum-transactions/
- Awesome-Layer-2/awesome-layer-2: All the layer 2 projects, https://github.com/Awesome-Layer-2/awesome-layer-2
- Matter Explorer, https://rinkeby.matter-labs.io/explorer/
- (8) Rise of the SNARKs with Howard Wu (SCIPR Lab, Blockchain at Berkeley, UC Berkeley) - YouTube, https://www.youtube.com/watch?v=Hig_1ZFbWRM
- (1) Howard Wu (@1HowardWu) | Twitter, https://twitter.com/1howardwu
- The Design of the Ceremony - Electric Coin Company, https://electriccoin.co/blog/the-design-of-the-ceremony/
- Zero Knowledge Proofs & zkSNARKs – Orom Exchange – Medium, https://medium.com/@OromExchange/zero-knowledge-proofs-zksnarks-ac558a8f91e2
- Tutorial: Proof of preimage – ZoKrates, https://zokrates.github.io/sha256example.html

REFERÊNCIAS

- What is the Zcash Sapling MPC ceremony? – Billy Garrison – Medium, https://medium.com/@blockchainbilly/what-is-the-zcash-sapling-mpc-ceremony-8b9c29e4c7c6
- Getting Started with zkSnarks/ZoKrates – Gnosis, https://blog.gnosis.pm/getting-started-with-zksnarks-zokrates-61e4f8e66bcc
- Introduction to Zero Knowledge Proof: The protocol of next generation Blockchain, https://medium.com/coinmonks/introduction-to-zero-knowledge-proof-the-protocol-of-next-generation-blockchain-305b2fc7f8e5
- Introducing Matter Testnet - Matter Labs – Medium, https://medium.com/matter-labs/introducing-matter-testnet-502fab5a6f17
- What are zk-SNARKs? | Zcash, https://z.cash/technology/zksnarks/
- Zk-SNARKs: Under the Hood, https://medium.com/@VitalikButerin/zk-snarks-under-the-hood-b33151a013f6
- EY Nightfall, https://github.com/EYBlockchain/nightfall/
- EatTheBlocks Newsletter #14 – zkSnarks / ZoKrates Tutorial, Learn Vyper, https://eattheblocks.com/eattheblocks-newsletter-14-zksnarks-zokrates-tutorial-learn-vyper/

REFERÊNCIAS

- What is ZKP? A Complete Guide to Zero Knowledge Proof | 101 Blockchains, https://101blockchains.com/zero-knowledge-proof/
- A Zero-Knowledge Proof: Improving Privacy on a Blockchain, https://www.altoros.com/blog/zero-knowledge-proof-improving-privacy-for-a-blockchain/
- Matter Labs GitHub, https://github.com/matter-labs/awesome-zero-knowledge-proofs
- Zokrates, https://github.com/Zokrates/ZoKrates