Decentralized Finance

PwC Switzerland
Smart Contract Assurance

Nov 2020

pwc

Centralization vs Decentralization

Trust the bank

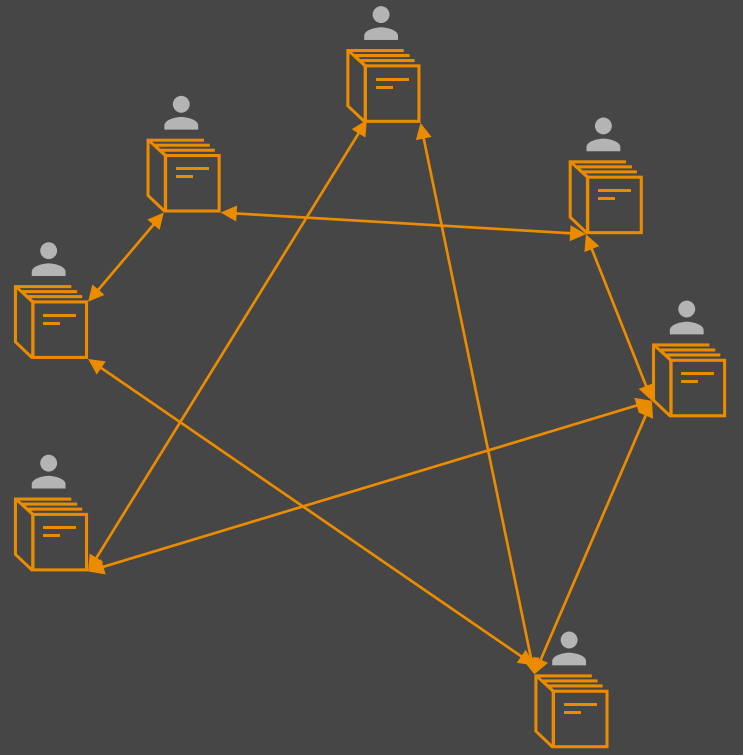
Generally, trust an institution

Bank / Network tracks:

- Account balance
- Transfers
- etc.

Trust the network

Generally, trust protocol and implementation



Smart Contracts

The execution / result can be verified by the network

DeFi* Smart Contracts

Software developers became ***super*** creative and wrote smart contracts for various purposes.

Today, we focus on financial smart contracts. They enable network participants for example to:

- Issue financial products / securities
- Exchange different securities
- Automatically enforce certain restrictions or terms
- Hold funds as a ”custodian”
- And much much more …

*Decentralized Finance

Smart Contract Assurance

Our team helps to **secure** smart contracts and the networks on which they run

…

We are an **ETH Zurich spin-off** founded by researchers.

We are **top contributors** to the **security** of the **Ethereum network** that runs most DeFi smart contracts.

We have an **extensive** track record in **code assessments** and experience with various networks like: **Ethereum, Corda, Zilliqa, Ren, Polkadot.**

We **developed** security tools **like**:

Securify https://github.com/eth-sri/securify2

VerX verx.ch

Enabling Trust

Networks

ethereum

r3.corda

Polkadot.

zilliqa

Ren

Projects

Polkadot.

kyber network

zilliqa

BIGIX

DAOstack

augur

Ren

PAXOS

HelloGold

pal NETWORK

POA

iExec

STK

Smart Contract Assurance
Services

Code Reviews

Architecture Reviews

Assurance or audit services
(including ISAE 3000 reports)

Research & Development

Consultation

Nico Schäfer

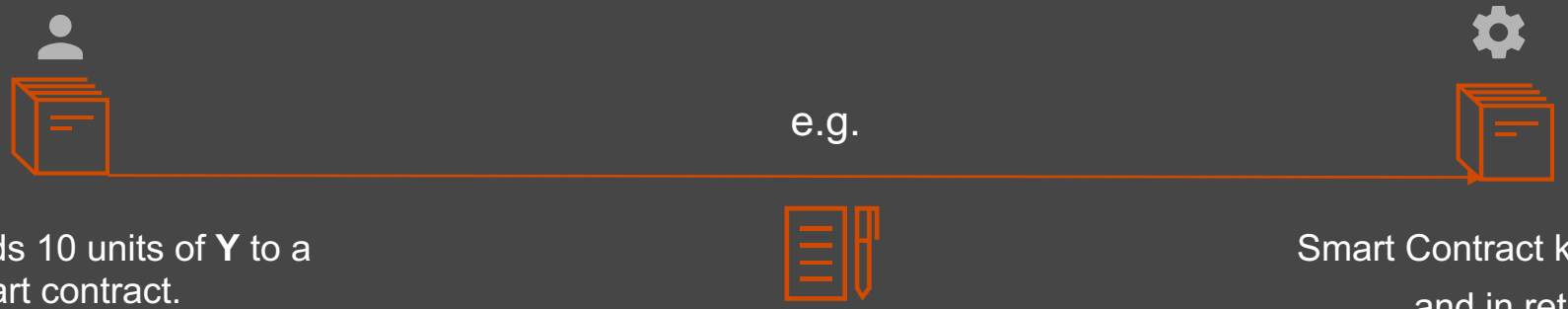
Lead Blockchain Security Engineer
PwC Switzerland

In case of questions or feedback write an email to:

nico.schaefer@pwc.ch

Have fun with the Webcast

Backup - Smart Contracts



User A sends 10 units of **Y** to a smart contract.

Smart Contract keeps 10 Y
and in return
user A gets an account balance of
100 units **S**

If the 10 **Y** represent a crypto currency worth 1000$ and **S** a stock, then this was an example for a stock purchase.

The smart contract could have encoded enforcements for a cerain vesting time or more which would be transparent and very hard or impossible to circumvent.