

Zero Knowledge Proofs for Financial Services

Markus Willms

Disclaimer

views and opinions are purely my own
and do not necessarily reflect the views & opinions
of the institution I work for,
or any of my fellow colleagues

Agenda

ZK Use case: KYC | enrolment | digital on-boarding

ZK Use case: loans | mortgages | pers. finance | **credit cards** | **scoring**

ZK Use case: investment strategy | financial risk | regulator window

ZK Proofs - What are the alternatives?

ZK Proofs: production examples

Conclusions

Contact

ZK Use case: KYC | enrolment | digital on-boarding

Do you **live in EU**? (without revealing country)

Do you have an **EU passport** (without revealing the document)

Are you **above 18**? (without revealing age)



ZK Use case: loans | mortgages | personal finance | credit cards | scoring

Do you have **Pension rights**? (without revealing amount, authority etc.)

Is your **salary within X EUR and Y EUR**? (without revealing amount)

Do you have **other incomes**? (without revealing it)



ZK Use case: investment strategy |
financial risk | regulator window

Does your **portfolio allocation** respect/match our
investors', regulator's, potential stakeholders'

risk profile?

investment strategy?

regulator's requirements?

Does your portfolio allocation respect/match our

concentration requirements/limits?

(without revealing the *assets, issuers, country*)

per geo location:

Do you *only* invest *within* the EU?

per sector:

Do you *only* invest *within* our target sectors:
ICT, renewable energy, blue-tech, green-tech?
(without revealing portfolio companies, countries)

Does your portfolio allocation respect/match our

liquidity, asset quality and **asset class** requirements?
(without revealing the **assets**)

per asset quality:

Low risk assets *only*? HQLA *only*? US treasury *only*?

per maturity:

Short term *only*? Long term *only*?

per asset class:

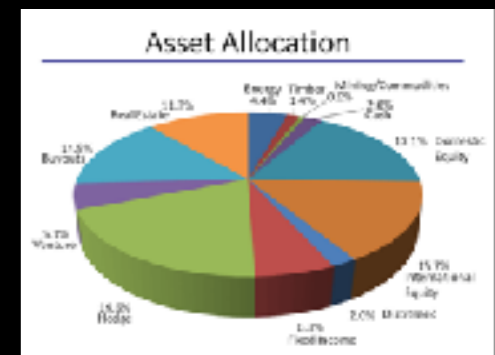
Debt based *only*? Equity based *only*? Private equity based *only*? Public equity based *only*?

per asset type:

Only corporate debt, *or* corporate equity? Only public sector debt, *or* public equity?

Low risk assets *only*?

...



Does your portfolio allocation respect/match our

diversification requirements ...

(without revealing portfolio allocation/***structure/ranges!***)

per basket of currencies:

20% EUR, 30%USD,...?



per issuer location:

10% US based issuers, 10% Japanese based issuers, 20% EU based issuers?

per fund size:

Within range of: 50-100 MIO EUR AUM? 101-200 MIO EUR AUM?

per asset rating:

Within range of: 20% AAA rated AND 10%... AND...?

Does your portfolio allocation respect/match our

sanctions requirements?

(without revealing the *assets, countries, trade details*)

per risk profile:

Do you have high risk assets, that are on the sanction list?

per low risk transactions:

Are your counterparties in **non-sanctioned** countries *only*?

per high risk transactions:

Proof that you have not traded with sanctioned counterparties.

ZK Proofs - What are the alternatives?

not many

not scalable

expensive (legal fees, manpower,
loss of control over private data,...)

not always or only **partially digital**

in essence: **legal contracts** and **NDA**s

ZK Proofs: production examples

ZEC (ZCASH), ETH, ADA, Z...
(**privacy coins; and utility coins with privacy features**)

JPM Quorum, Hyperledger, Apla, ...
(**permissioned chains**)

Corda (www.corda.net)
public chain aims at solving **scalability issue of blockchains**
tailoring blockchain **history** (vs. blockchain state machine)

ZK Proof frameworks

Project Franclin (<https://matter-labs.io>),
Project ISEKAI (<https://www.sikoba.com>)

ING's bullet range, bulletproofs...

EY's Knightfall (making private transactions on Ethereum public chain **less gas expensive**)

and **many other projects...**

Privacy on open (permissionless) vs permissioned blockchains

Privacy is less hard to solve on permissioned blockchains because of **trust model** (all actors are **identified**)

ZK Proofs tend to be **more expensive** on public chains (e.g. gas consumption, on-going improvements).

Public blockchains are the **way to go** though (at least mid/long term), because of:

1/ **higher security**

2/ large **network effects**,

3/ being **real commons**

(without tragedy of commons problem, when token economics are well designed/aligned)

4/ wider **cost mutualization**

Privacy rendering Cryptography | out of space view

Symmetric Cryptography (sender and receiver have same keys)

Asymmetric cryptography (different keys for sign/verify; encrypt/decrypt, computationally expensive encryption)

Proxy Re-Encryption (asymmetric cryptog. 'upside down' | uses 'trusted 3rd party' proxy for relaying encrypted messages | user keeps keys (not proxy) | allows access right revocation and right to forget (GDPR!))

Zero Knowledge Proofs (*snarks, starks, sharks, bulletproofs ... | proving a secret without revealing it*)

Homomorphic Encryption (hybrid of asym./sym. cryptog. | encryption with additional eval capability | not revealing key | computation on ciphertexts generating an encrypted result | when decrypted, matches result of operations | as if performed on plaintext)

Conclusions

for the **(traditional) financial services** industry already now **some**
Zero Knowledge proof **use case & examples exist**

more use cases to be **considered and analysed** by the traditional
financial industry

blockchain ecosystem and **decentralised (open) finance ahead of**
traditional financial services industry in terms of ZK proof adoption

privacy (transaction, portfolio, smart contract) on public
blockchains is one of the major hindering factors **preventing wide**
adoption of blockchain technology and decentralised finance

contact



Markus Willms

thisisfunnysir@gmail.com