byont

ZERO-KNOWLEDGE PROOF

PRESENTATION 2

BY VITALI BESTOLKAU AND IGNAS APSEGA

byont

TABLE OF CONTENTS

byont

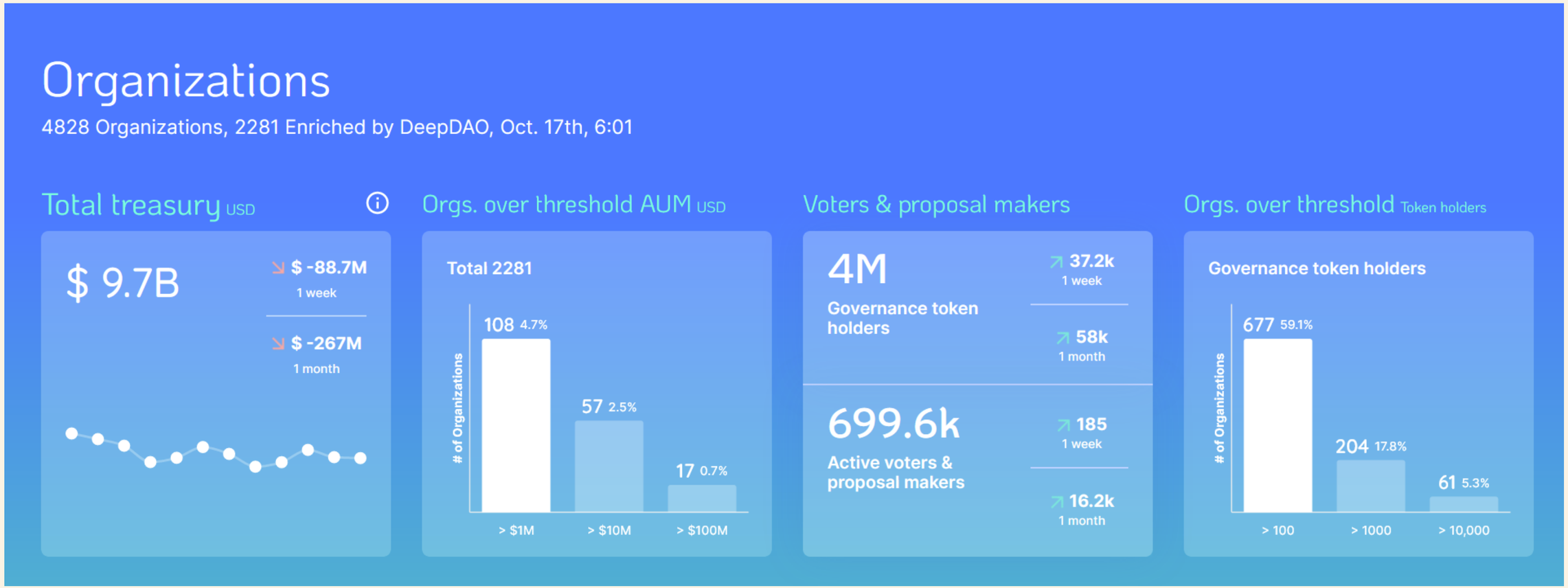
WHAT IS A DAO?

A decentralized autonomous organization (DAO) - is an emerging form of legal structure with no central governing body and whose members share a common goal to act in the entity's best interest.

Source: https://ecryptobulls.com/en/what-is-dao/

byont

OVERVIEW OF DAOS



Source: https://ecryptobulls.com/en/what-is-dao/

byont

COMMON CHALLENGES OF DAOS

DAO users are pseudonymous - using a fictitious name

Policy-based challenges:

- Smart contracts
- Legality
- Privacy

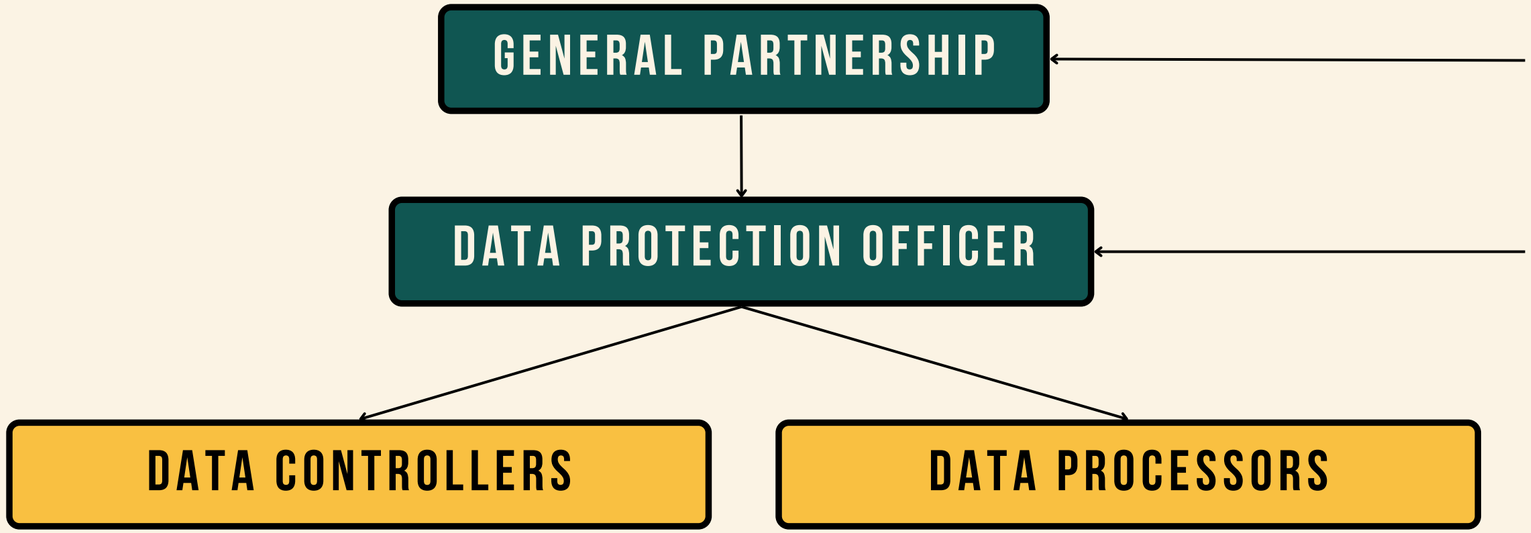
Technical challenges:

- Security
- Networking
- Scalability

LEGAL PROBLEMS

byont

DAO APPLICABILITY WITH GDPR



- Users must consent for data collection
- DAOs must ensure that the minimum security standards of the GDPR are met

byont

COMMON PRIVACY PROBLEMS IN DAOS

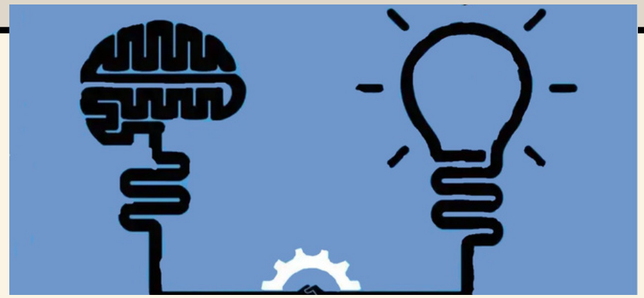
DAO stakeholders are vulnerable to off-chain coercion.

Source:
https://study.com/learn/lesson/coercion-overview-

The limited talent pool for hiring

Source:
https://medium.com/hr-blog-resources/talenthow-

DAOs risk disincentivizing innovation and experimentation by their developers



Source:
https://www.cio.com/article/236607/how-it-leaders-

POSSIBLE SOLUTIONS

BLOCKCHAIN-BASED REPORTING PROTOCOLS (BBRP)

- Used only for hiding reporting users who are detecting misbehaving nodes

DECENTRALIZED IDENTITIES

- Could be used to identify the malicious person

ZERO-KNOWLEDGE PROOFS (ZKP)

Hides all the transactions on the blockchain:

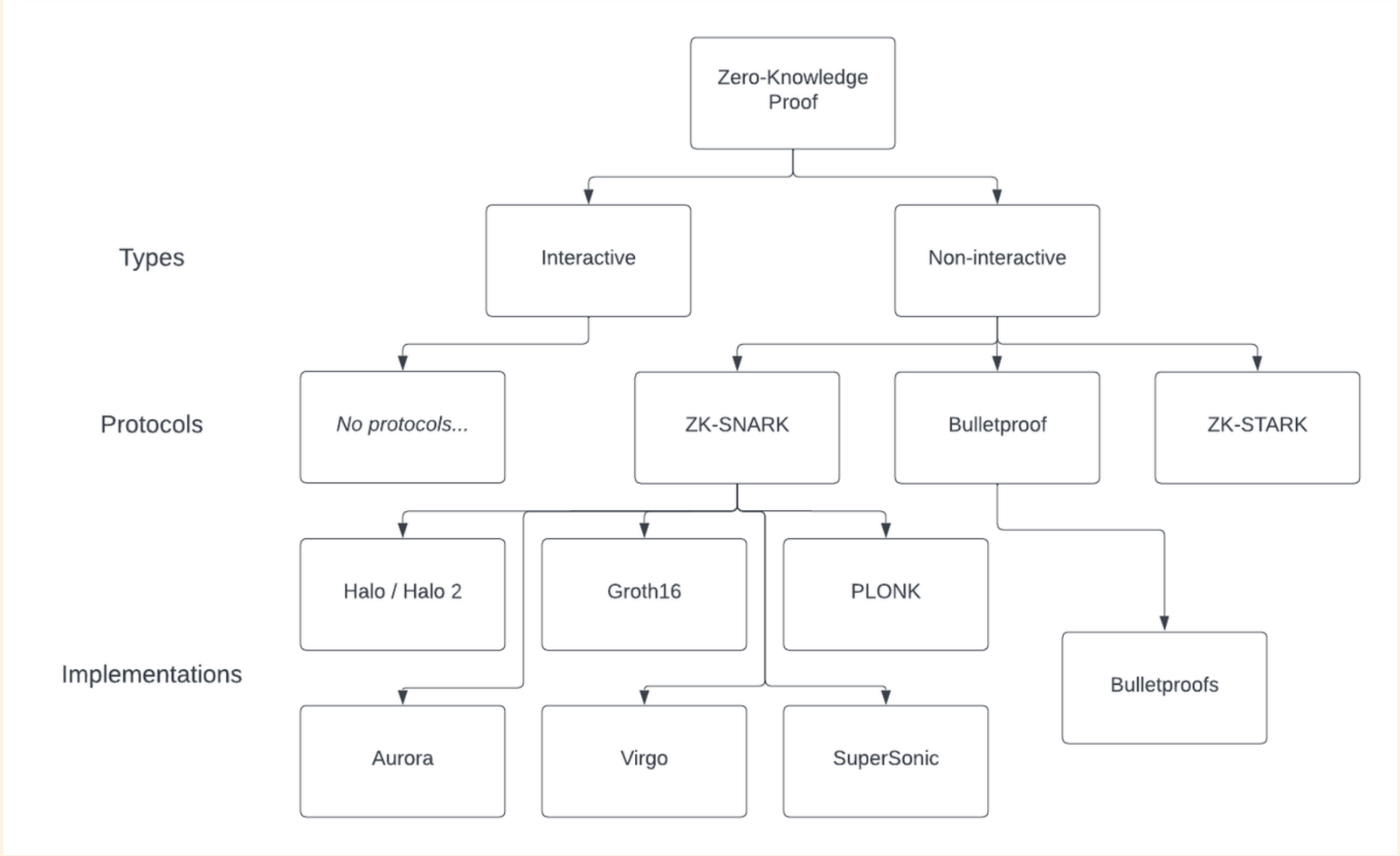
- Private fundraising in DAOs
- Private issue of DAO assets (tokens or equivalent)
- Private management of DAO treasury

DAOS SUMMARY

- Around 4800 of DAOs and 700k active participants and still growing
- DAOs have to be aware of compliance with GDPR
- Privacy is expanding problem of DAOs
- Zero Knowledge Proofs looks like the most promising and sophisticated solution to the privacy problems

byont

ZERO KNOWLEDGE PROOFS



ZKP TYPES (RECAP)

	INTERACTIVE ZKP	NON-INTERACTIVE ZKP
Advantages	• Easy to execute	• Scalable • Transferable
Disadvantages	• Limited Transferability • Not scalable	• Requires a lot of computational power

PROTOCOLS

Succinct
Non-interactive
ARgument of
Knowledge

ZK-SNARKS

ZCASH

"Short like a bullet,
with bulletproof
security
assumptions"

BULLETPROOFS

MONERO

Scalable
Transparent
ARgument of
Knowledge

ZK-STARKS

STARKWARE

byont

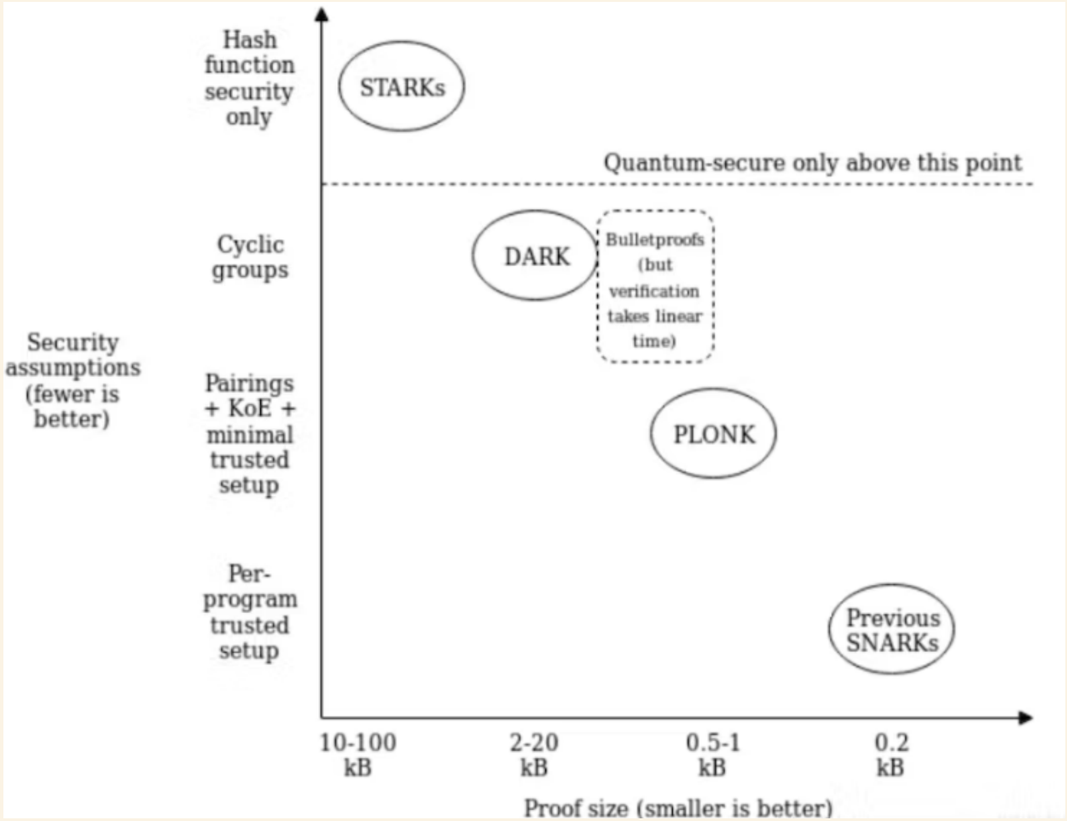
PROTOCOL COMPARISON

Comparison of the most popular zkp systems

	SNARKs	STARKs	Bulletproofs
Algorithmic complexity: prover	O(N * log(N))	O(N * poly-log(N))	O(N * log(N))
Algorithmic complexity: verifier	~O(1)	O(poly-log(N))	O(N)
Communication complexity (proof size)	~O(1)	O(poly-log(N))	O(log(N))
- size estimate for 1 TX	Tx: 200 bytes, Key: 50 MB	45 kB	1.5 kb
- size estimate for 10.000 TX	Tx: 200 bytes, Key: 500 GB	135 kb	2.5 kb
Ethereum/EVM verification gas cost	~600k (Groth16)	~2.5M (estimate, no impl.)	N/A
Trusted setup required?	YES 😒	NO 😄	NO 😄
Post-quantum secure	NO 😒	YES 😄	NO 😒
Crypto assumptions	DLP + secure bilinear pairing 😒	Collision resistant hashes 😄	Discrete log 😶

Source:
https://github.com/matter-labs/awesome-zero-knowledge-proofs#comparison-of-the-most-popular-zkp-systems

Source:
https://hackernoon.com/zero-knowledge-proofs-the-simplest-explanation-on-the-internet-yf6g37nq



byont

IMPLEMENTATION

ZK-SNARKS

BULLETPROOFS

ZK-STARKS

GROTH16

PLONK

HALO (2)

BULLETPROOFS

(SUPER)SONIC

AURORA

VIRGO

ZK-STARKS

ZILCH

byont

IMPLEMENTATION JUSTIFICATION

Zero-knowledge proof (ZKP) systems

ZKP System	Publication year	Protocol	Transparent	Universal	Plausibly Post-Quantum Secure	Programming Paradigm
Pinocchio[32]	2013	zk-SNARK	No	No	No	Procedural
Geppetto[33]	2015	zk-SNARK	No	No	No	Procedural
TinyRAM[34]	2013	zk-SNARK	No	No	No	Procedural
Buffet[35]	2015	zk-SNARK	No	No	No	Procedural
ZoKrates[36]	2018	zk-SNARK	No	No	No	Procedural
xJsnark[37]	2018	zk-SNARK	No	No	No	Procedural
vRAM[38]	2018	zk-SNARG	No	Yes	No	Assembly
vnTinyRAM[39]	2014	zk-SNARK	No	Yes	No	Procedural
MIRAGE[40]	2020	zk-SNARK	No	Yes	No	Arithmetic Circuits
Sonic[41]	2019	zk-SNARK	No	Yes	No	Arithmetic Circuits
Marlin[42]	2020	zk-SNARK	No	Yes	No	Arithmetic Circuits
PLONK[43]	2019	zk-SNARK	No	Yes	No	Arithmetic Circuits
SuperSonic[44]	2020	zk-SNARK	Yes	Yes	No	Arithmetic Circuits
Bulletproofs[45]	2018	Bulletproofs	Yes	Yes	No	Arithmetic Circuits
Hyrax[46]	2018	zk-SNARK	Yes	Yes	No	Arithmetic Circuits
Halo[47]	2019	zk-SNARK	Yes	Yes	No	Arithmetic Circuits
Virgo[48]	2020	zk-SNARK	Yes	Yes	Yes	Arithmetic Circuits
Ligero[49]	2017	zk-SNARK	Yes	Yes	Yes	Arithmetic Circuits
Aurora[50]	2019	zk-SNARK	Yes	Yes	Yes	Arithmetic Circuits
zk-STARK[51]	2019	zk-STARK	Yes	Yes	Yes	Assembly
Zilch[31][52]	2021	zk-STARK	Yes	Yes	Yes	Object-Oriented

Source:

https://en.wikipedia.org/wiki/Zero-knowledge_proof#Zero-Knowledge_Proof_protocols

Implementations Comparison Table

	Proof size	Trustless	Scalable	Universal	Verification time	Languages for implementation
Groth16	0.2 kB	No	No	No	10 ms	Rust
PLONK	0.5 - 1 kB	No	Yes	Yes	~10 ms	Rust
Halo 2	3.5 kB	Yes	Yes	Yes		Rust
SuperSonic	10 kB	Yes	Yes	Yes	100 ms	
Bulletproofs	1 - 1.5 kB	Yes (?)	Yes	Yes		Rust

Source:

me

ZKP SUMMARY

- SNARKs: fast, cheap, usually rely on a trusted setup.
- Bulletproofs: have moderate proof-size, verification time, are believed not to rely on a trusted setup, but use MPC.
- STARKs: relatively fast, post-quantum secure, too big proof size for blockchain.
- A lot of ZKP implementations, but most suitable for our case: Halo 2, SuperSonic and Bulletproofs.

Q & A