Variants of **Proof-of-Stake** and their Privacy Limitations

By @awasunyin

Proof-of-X ≠ Consensus Algorithm

Mechanisms that determine what **peers** are **eligible** for producing the next block

Variants of **Proof-of-Stake**

Delegated PoS
(DPoS)
e.g. EOS

Liquid PoS
(LPoS)
e.g. Tezos

Cosmos PoS
(BDSMPoS ¿?)
e.g. Cosmos Hub

Nominated PoS
(NPoS)
e.g. Polkadot

	Delegated PoS (DPoS)
Who is allowed to participate?	By holders' votes (21/100)
How is leader elected?	21 *Producers* / round voted
What is at stake?	None
What are the slashing conditions?	None
What are the rewards?	Fixed rate + % on blocks
Consensus Mechanism?	Nakamoto Consensus

	Delegated PoS (DPoS)	**Liquid** PoS (LPoS)
Who is allowed to participate?	By holders’ votes (21/100)	10,000 XTZ self-bonded
How is leader elected?	21 *Producers* / round voted	Pseudorandom slots
What is at stake?	None	*Bakers*’ self-bond, rewards
What are the slashing conditions?	None	Double-signing Double-baking
What are the rewards?	Fixed rate + % on blocks	Baking + fees Endorsement
Consensus Mechanism?	Nakamoto Consensus	Nakamoto Consensus

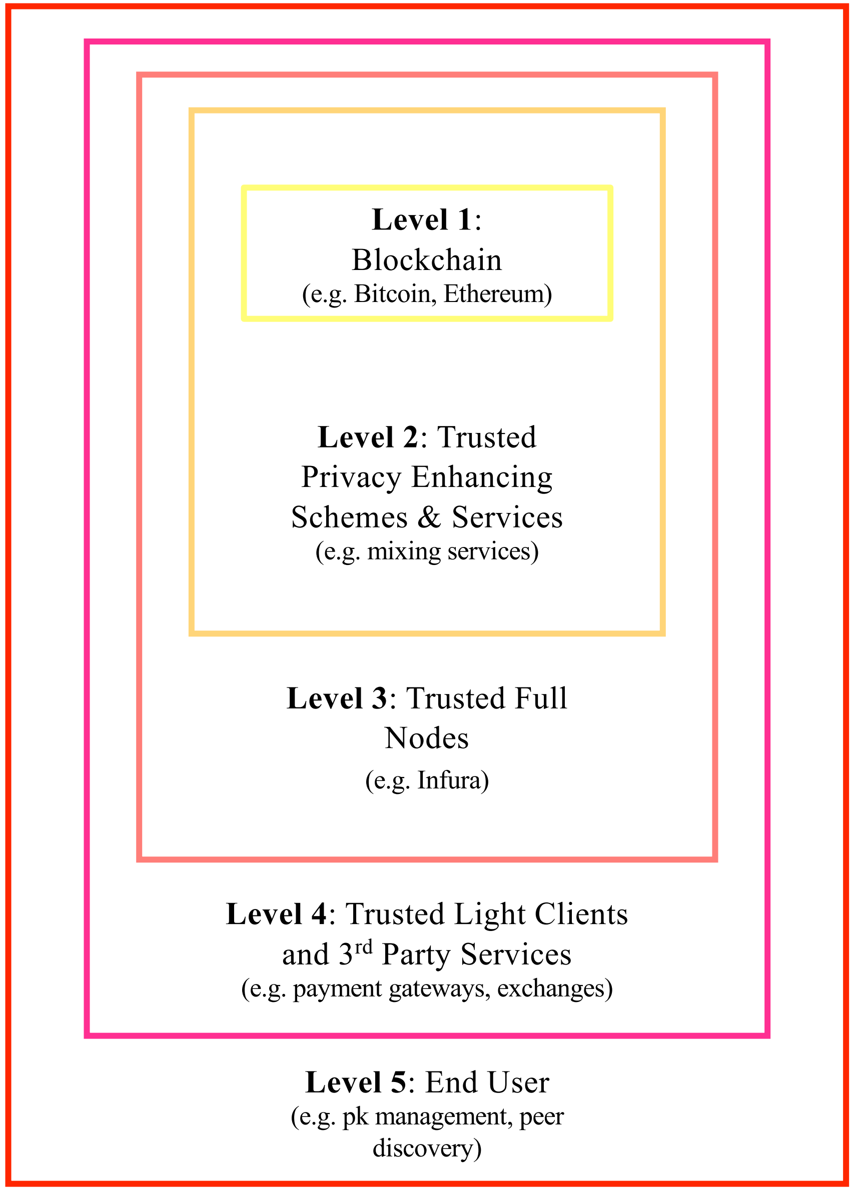
	Delegated PoS (DPoS)	**Liquid** PoS (LPoS)	**Cosmos** PoS (BDSMPoS ¿?)
Who is allowed to participate?	By holders' votes (21/100)	10,000 XTZ self-bonded	Top 100 by economic stake
How is leader elected?	21 *Producers* / round voted	Pseudorandom slots	Weighted Round-Robin
What is at stake?	None	*Bakers*' self-bond, rewards	Self-bond, delegation, rewards
What are the slashing conditions?	None	Double-signing Double-baking	Double-signing Liveness
What are the rewards?	Fixed rate + % on blocks	Baking + fees Endorsement	Validation rewards + fees
Consensus Mechanism?	Nakamoto Consensus	Nakamoto Consensus	Tendermint Consensus

	Delegated PoS (DPoS)	**Liquid** PoS (LPoS)	**Cosmos** PoS (BDSMPoS ¿?)	**Nominated** PoS (NPoS)
Who is allowed to participate?	By holders' votes (21/100)	10,000 XTZ self-bonded	Top 100 by economic stake	*Sufficiently high bond deposited*
How is leader elected?	21 *Producers* / round voted	Pseudorandom slots	Weighted Round-Robin	-
What is at stake?	None	*Bakers'* self-bond, rewards	Self-bond, delegation, rewards	Self-bond, rewards
What are the slashing conditions?	None	Double-signing Double-baking	Double-signing Liveness	Double-signing Liveness
What are the rewards?	Fixed rate + % on blocks	Baking + fees Endorsement	Validation rewards + fees	Validation rewards + fees
Consensus Mechanism?	Nakamoto Consensus	Nakamoto Consensus	Tendermint Consensus	Tendermint, HoneyBadger

Privacy Limitations in PoS Networks

How do you discover validators?
How do participants you interact
with validators?

Privacy Layers for Blockchain Developers to Consider by @awasunyin



Level 1:
Blockchain
(e.g. Bitcoin, Ethereum)

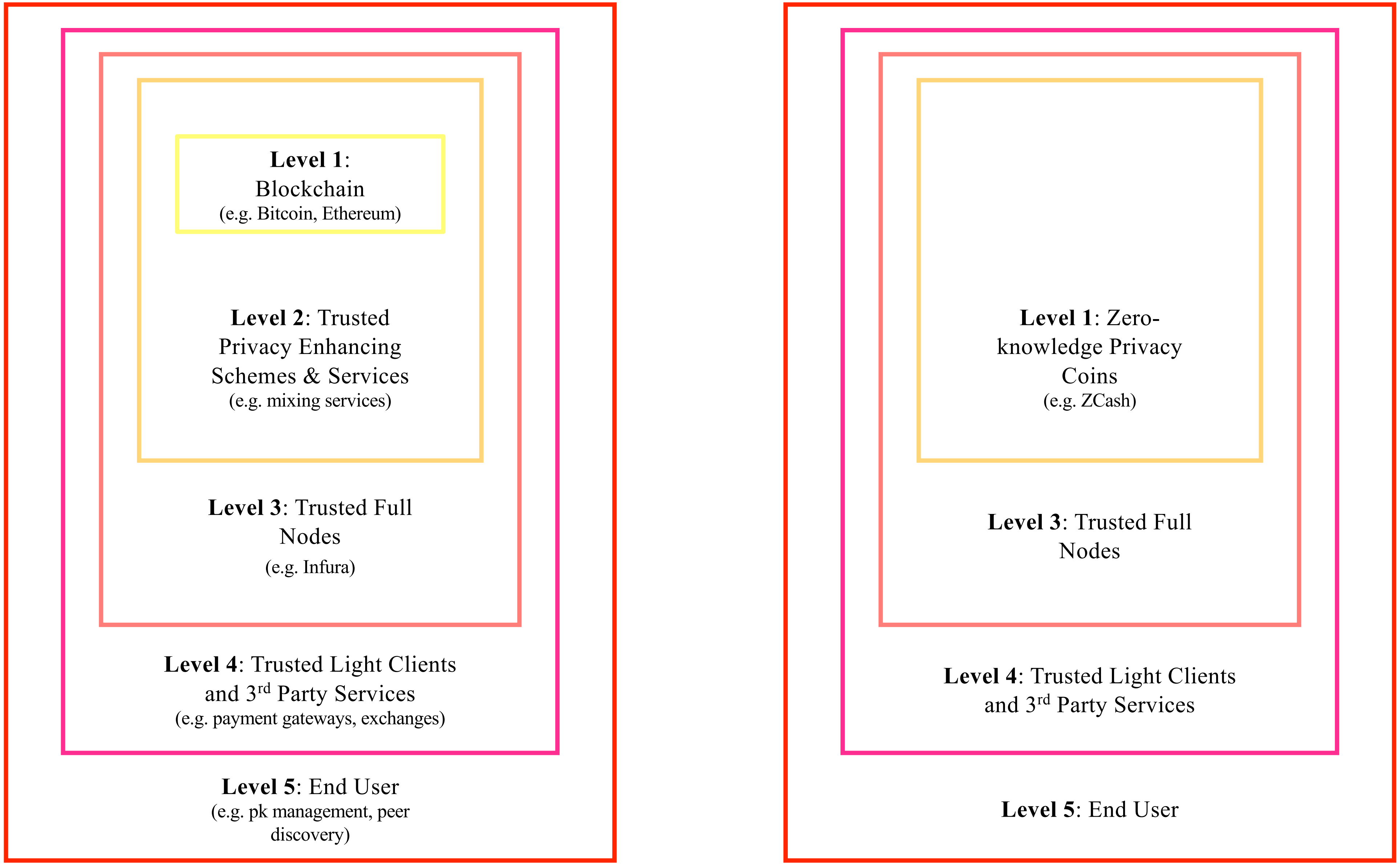
Level 2: Trusted
Privacy Enhancing
Schemes & Services
(e.g. mixing services)

Level 3: Trusted Full
Nodes
(e.g. Infura)

Level 4: Trusted Light Clients
and 3rd Party Services
(e.g. payment gateways, exchanges)

Level 5: End User
(e.g. pk management, peer
discovery)

Privacy Layers for Blockchain Developers to Consider by @awasunyin



Level 1:
Blockchain
(e.g. Bitcoin, Ethereum)

Level 2: Trusted Privacy Enhancing Schemes & Services
(e.g. mixing services)

Level 3: Trusted Full Nodes
(e.g. Infura)

Level 4: Trusted Light Clients and 3rd Party Services
(e.g. payment gateways, exchanges)

Level 5: End User
(e.g. pk management, peer discovery)

Level 1: Zero-knowledge Privacy Coins
(e.g. ZCash)

Level 3: Trusted Full Nodes

Level 4: Trusted Light Clients and 3rd Party Services

Level 5: End User

How can we increase Privacy on PoS Networks?

Join our discussion session at 12:00 (Breakout 2)!

Resources

- Larimer, D. (2014). Delegated proof-of-stake (dpos). Bitshare whitepaper.
- Goodman, L. M. (2014). Tezos—a self-amending crypto-ledger White paper. URL: https://www.tezos. com/static/papers/white_paper. pdf.
- Kwon, J. (2014). Tendermint: Consensus without mining. Draft v. 0.6, fall.
- Wood, G. (2016). Polkadot: Vision for a heterogeneous multi-chain framework. White Paper.
- Buchman, E., Kwon, J., & Milosevic, Z. (2018). The latest gossip on BFT consensus. arXiv preprint arXiv:1807.04938.
- Arluck, Jacob (2018). Liquid Proof-of-Stake. URL: https://medium.com/tezos/liquid-proof-of-stake-aec2f7ef1da7