Public and Private Blockchains

same idea, inverted context

Decentralized 2017

Gregor Borosa
borosa.g@unic.ac.cy

UNIVERSITY *of*
NICOSIA

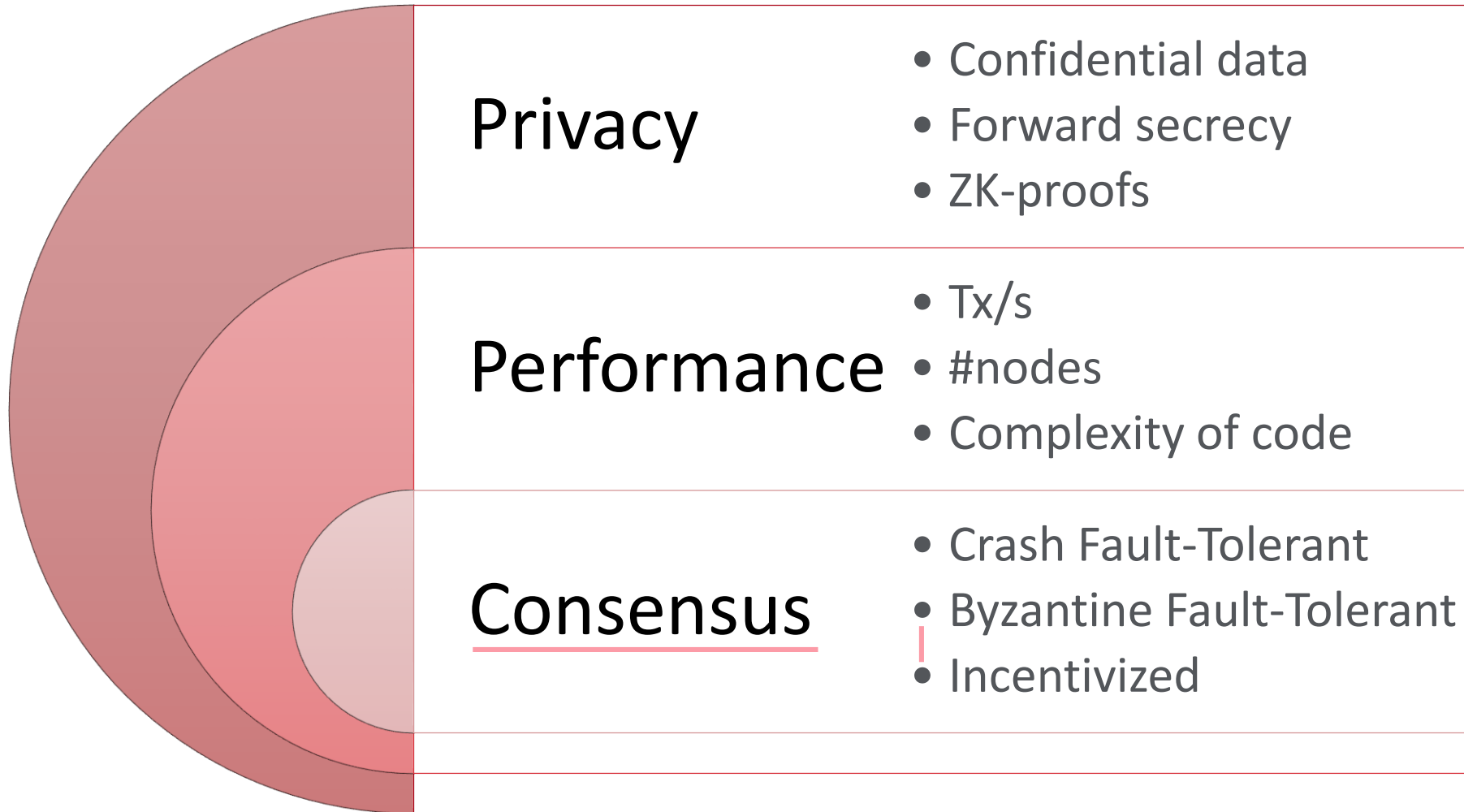# Public & Private Blockchains

▰ Competitors or complementors?

▰ Original premise of blockchain: *P2P* currency – data – logic; *open, uniform access.*

▰ Not everything can be public, even more so when transactions are generalized into smart contracts.

▰ Now & Future.

UNIVERSITY *of* NICOSIA

A Matter of Control

Technological Divergence

Privacy
- Confidential data
- Forward secrecy
- ZK-proofs

Performance
- Tx/s
- #nodes
- Complexity of code

Consensus
- Crash Fault-Tolerant
- Byzantine Fault-Tolerant
- Incentivized

Consensus Boom

1988	1989	1990	...	1999	...	2005	2006	2007	2008	2009	2010	2011	2012	2013	2014	2015	2016	2017
VSR		Paxos		PBFT		Q/U	HQ	BFT-Smart	POW	Abstract		POS	POB	Dagger	Dagger-Hashimoto	ADAPT	2-hop blockchain	Algorand
										Aardvark			Ripple RTP	GHOST	Delegated POS	Bitcoin-NG	Honey Badger BFT	Forking-free Hybrid C.
										Zyzzyva				Raft	Deposit-based POS	Ethash	Hybrid c.	Ouroboros-Praos
														RBFT	Hashimoto	SCP	POET	Practical Synch. BFT
															POA	Stellar SCP	POL	POUW
															POC	XFT	Scalable BFT	REM
															Tangaroa		Sieve	SPECTRE
															Tendermint		Tangle	Subchain POS
																		Tortoise and Hares C.

Same idea, inverted context

Image by geralt

The Great Divide — public 🔓 consortium 🔒 private

Business models

- Digital currency
- True dApps
- 2nd layer services

Governance

- Decentralization
- Coordination
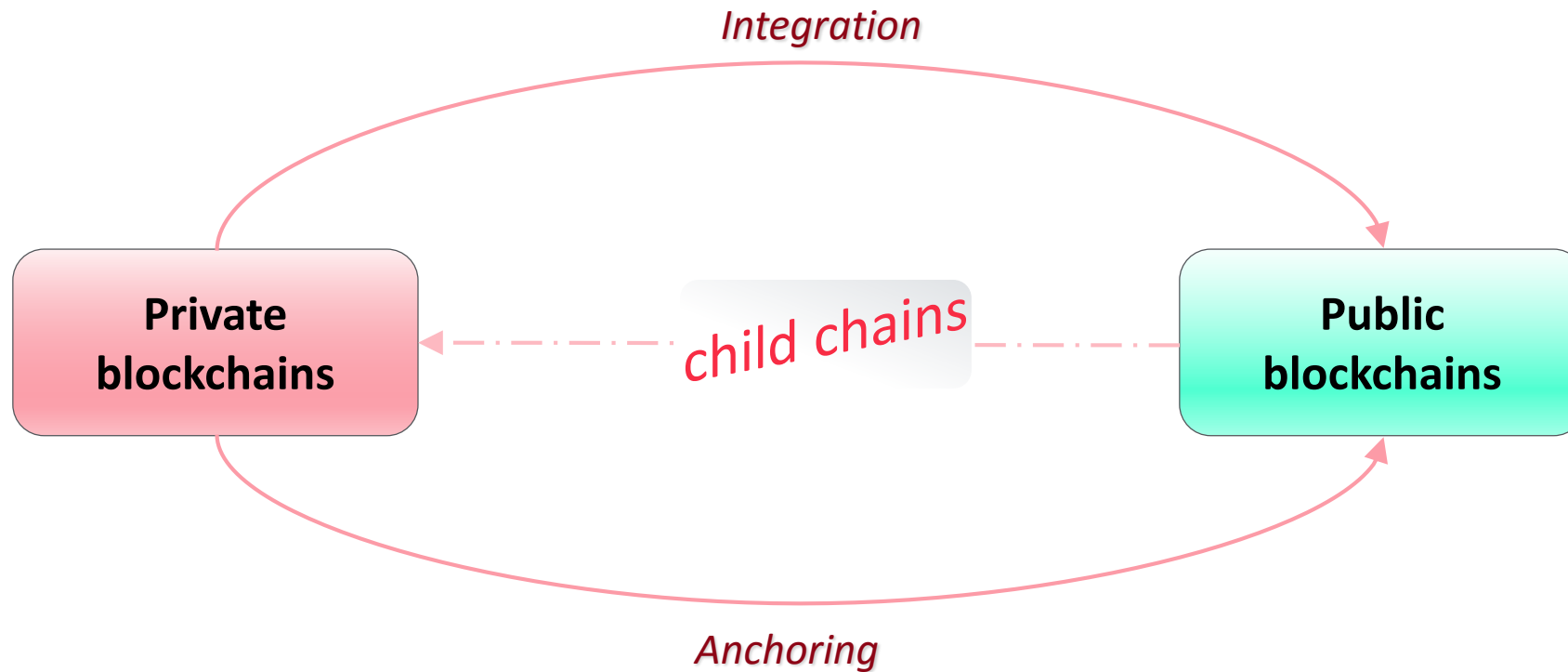- Stewardship

Structural profiles

- Organizations with delicate, scattered data sources
- Multiple organizations/peers

How much decentralization is enough?

FOMO the hype or a genuine need for blockchain?

UNIVERSITY of NICOSIA

Prediction for the Future?

Public … or private … or consortium?
– Yes.

Gregor Borosa

borosa.g@unic.ac.cy