Generic Privacy Preserving Private Permissioned Blockchains

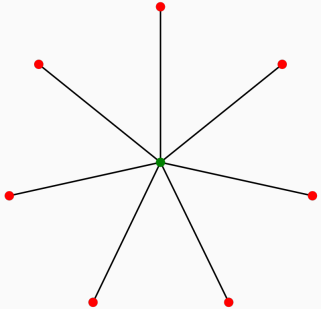
Frédéric A. Hayek [1] Mirko Koscina [2] Pascal Lafourcade[1] Charles Olivier-Anclin[1,2]

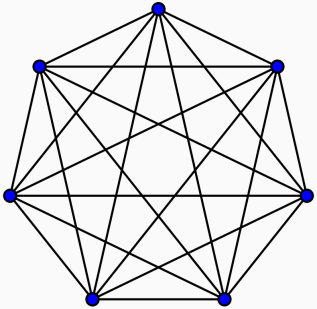
LIMOS – Journées Axe SIC 2024

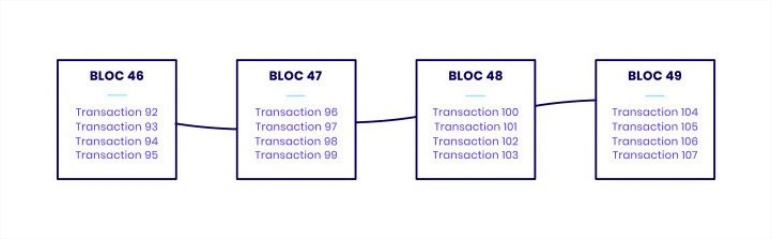
[1]Université Clermont-Auvergne, CNRS, Mines de Saint-Étienne, LIMOS, Clermont-Ferrand, France

[2]be ys Pay, Clermont-Ferrand, France

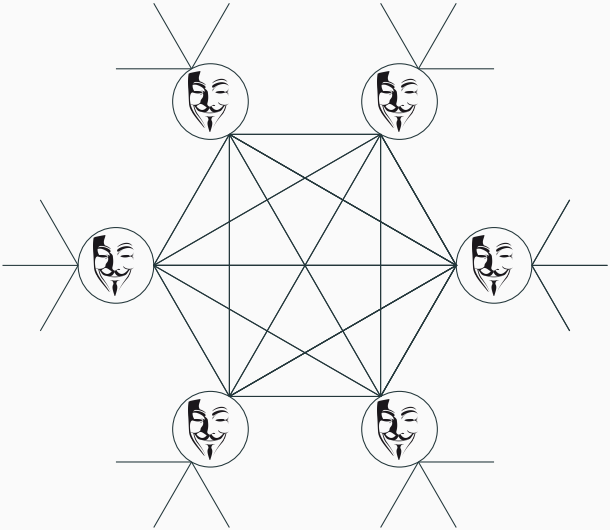
Blockchain





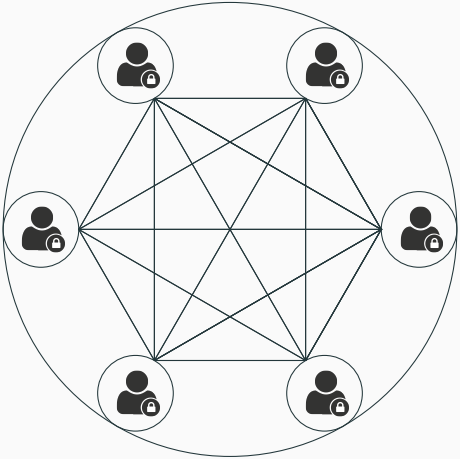

BLOC 46
Transaction 92
Transaction 93
Transaction 94
Transaction 95
BLOC 47
Transaction 96
Transaction 97
Transaction 98
Transaction 99
BLOC 48
Transaction 100
Transaction 101
Transaction 102
Transaction 103
BLOC 49
Transaction 104
Transaction 105
Transaction 106
Transaction 107

Privacy for Blockchain: Public/Permissionless



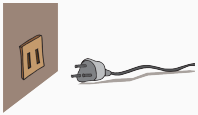
Privacy for Blockchain: Public/Permissionless

Privacy for Blockchain: Private/Permissioned

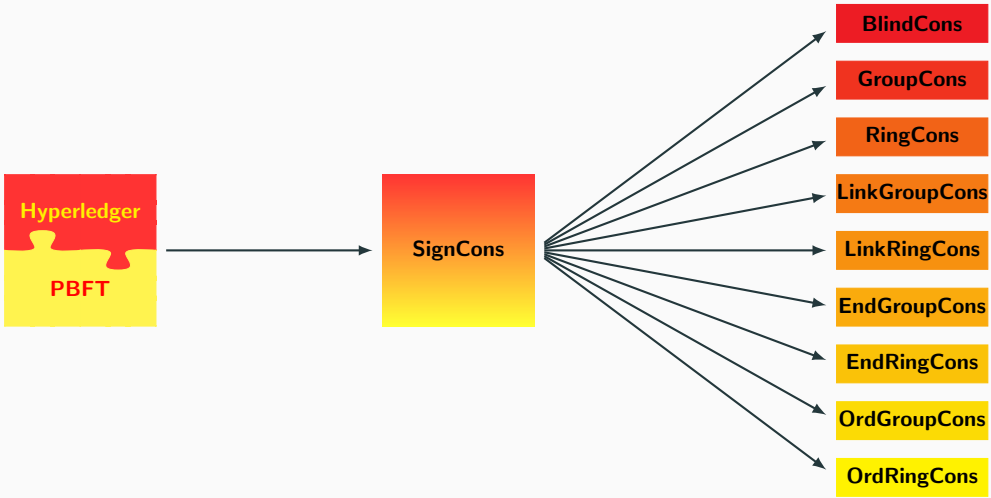


Dilemma

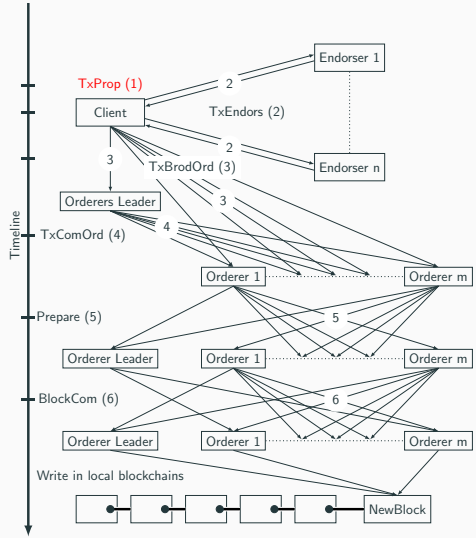
Are private/permissioned blockchains and privacy incompatible?



Our Solution: SignCons



SignCons


Endorser 1
TxProp (1)
2
Client
TxEndors (2)
2
Endorser n
3
TxBrodOrd (3)
Orderers Leader
3
4
TxComOrd (4)
Timeline
Orderer 1
Orderer m
Prepare (5)
5
Orderer Leader
Orderer 1
Orderer m
BlockCom (6)
6
Orderer Leader
Orderer 1
Orderer m
Write in local blockchains
NewBlock

Cryptographic Tools - Signature Schemes

Signature:

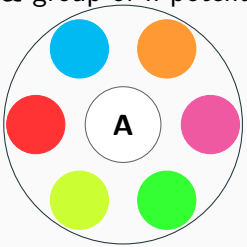
Signer pk

Blind Signature:

Issuer & Signer pk

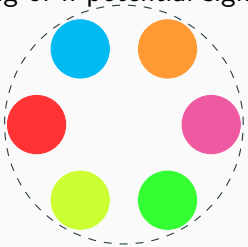
Group Signature:

Authority & group of n potential signers



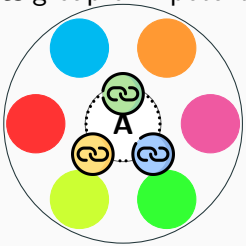
Ring Signature:

Ring of n potential signers



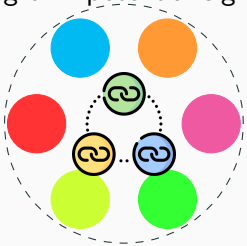
(Linkable) Group Signature:

Authority & group of n potential signers

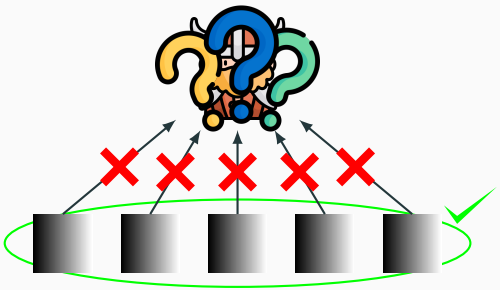


(Linkable) Ring Signature:

Ring of n potential signers

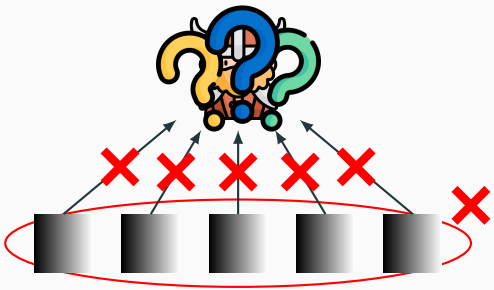


Pseudonymity



Theorem
Based on secure signatures, our protocols are pseudonymous.

Anonymity

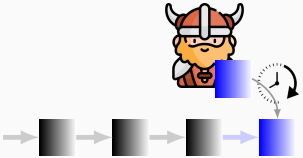


Theorem
Based on secure signatures, our protocols are anonymous.

Security Arguments

Safety

Liveness



Theorem
Our protocols are safe if at most $\lfloor \frac{n-1}{3} \rfloor$ *out of total n orderers are malicious.*

Theorem
Our protocols satisfy liveness when at most $\lfloor \frac{\text{TotEnd}-1}{2} \rfloor$ *endorsers and* $\lfloor \frac{\text{TotOrd}-1}{3} \rfloor$ *orderers are malicious.*

Constructions Properties

Users' Privacy Preserving Protocols:

	Revoke User	Authority		Privacy Level
		No	Inactive	
BlindCons				Anonymity
GroupCons	✓		✓	Anonymity
RingCons		✓	✓	Anonymity
LinkGroupCons	✓		✓	Pseudonymity
LinkRingCons		✓	✓	Pseudonymity

Orderers' and Endorsers' Protocols:

	Revoke Endorser	Authority Not Needed	Privacy Level
(Ord) EndGroupCons	✓		Pseudonymity
(Ord) EndRingCons		✓	Pseudonymity

See you at the poster session!