A Broad Treatment of Privacy in Blockchains

Challenge:

Address privacy issues on public blockchains

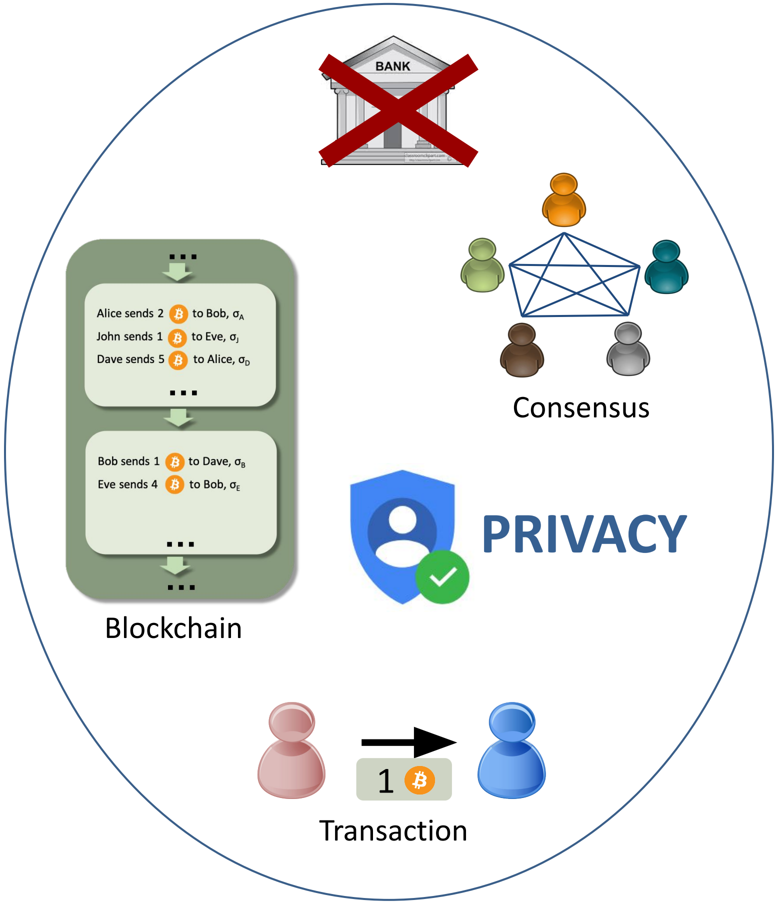
- Consensus level
- Transaction level

Solution:

Advances in both foundations and applications

- Upper and lower bounds for anonymous Proof-of-Stake consensus
- ZK proofs for blockchains
- Privacy with accountability
- Anonymous Signaling and Signatures

#1717067 Foteini Baldimtsi, GMU
#1764025 Alessandra Scafuro, NCSU


BANK
Consensus
Alice sends 2 ₿ to Bob, σ_A
John sends 1 ₿ to Eve, σ_J
Dave sends 5 ₿ to Alice, σ_D
...
Bob sends 1 ₿ to Dave, σ_B
Eve sends 4 ₿ to Bob, σ_E
...
Blockchain
PRIVACY
1 ₿
Transaction

Scientific Impact:

New models & constructions

- Anonymous PoS [S&P22,CSF'20]
- Differentially Private Mixing [PoPETS'22]
- Private + Accountable Permissioned Ledgers [Esorics'21]

Primitives, Foundations

- ZK proofs [Asiacrypt '19,'20]
- Traceable Signatures from RO [Esorics'21]
- Private Signaling [USENIX'22]

Broader Impact and Broader Participation:

- Adoption of blockchain requires privacy
- New ZK proofs for RSA setup deployed [Asiacrypt'19]
- 4 PhD students (3 minorities funded)
- 2 new classes on blockchain and ZK proofs
- Multiple seminars/talks to academic and general public audiences