



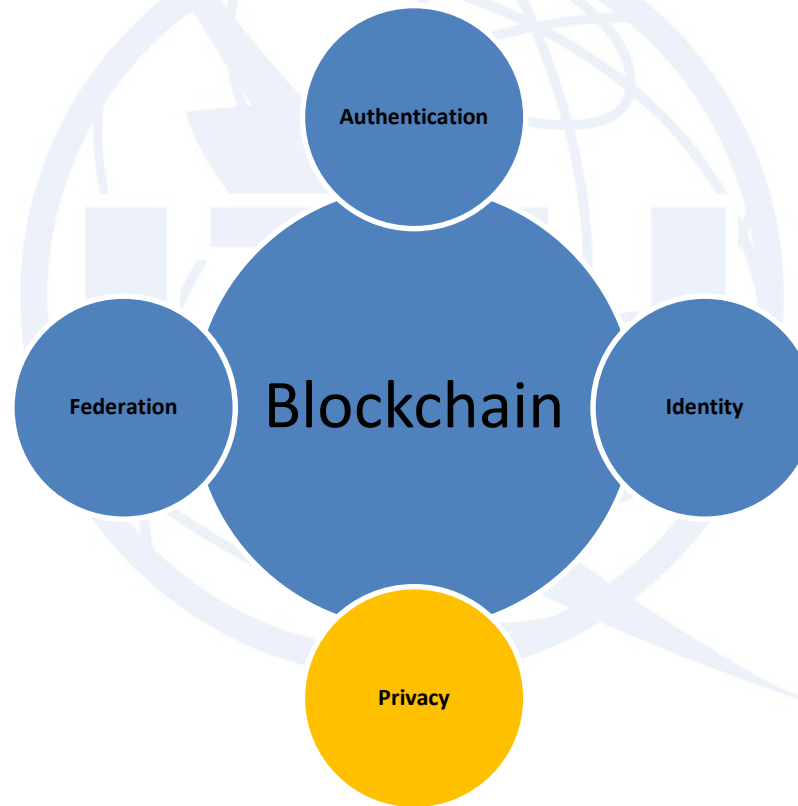
ITU Workshop on “Security Aspects of Blockchain” (Geneva, Switzerland, 21 March 2017)

Privacy on the Blockchain

Sylvan Tran
Security Advisor, Aetna
trans@aetna.com

Geneva, Switzerland, 21 March 2017

My Perspective



Geneva, Switzerland, 21 March 2017



Foot On The Gas

- New racecar drivers always ask “How do I drive faster?”
- Veteran racecar drivers always ask “How do I stop faster?”

Stopping faster allows you to ultimately drive faster.

Immutable Data

Blessing

- Cannot be forged
- Ledgers become permanent
- Records can never be altered

Curse

- Cannot be altered
- Erroneous entries can never be removed
- All federated organizations will perpetuate erroneous data

Previous Tech Fails

Fingerprints

- Organization stored actual prints
- Unable to revoke / reassign after compromised

Retinal Scans

- Organization stored actual scans
- Unable to revoke / reassign after compromised

Knowledge Based Authentication

- Organizations used the same questions
- Once compromised, cannot be “unshared”

Recommendations

Never write actual or encrypted data to the Blockchain

- Abstract the data using tokens or links

No blanket permissions

- Fine grain controls per attribute must be in place

Know who can attest for your data

- What data is there about me, who has the actual data and the purpose for its use

Unconsent support

- Technical controls must exist to comply with user's data wishes

More discussion

- Others smarter than I will have more to contribute

Thank You

Questions?

Sylvan Tran

trans@aetna.com



(Sylvan's vCard)