FIGI Security Clinic

DLT Security

Dr. Leon Perlman
Columbia University, New York

4-5 December 2019
#financialinclusion

Sponsored by

BILL & MELINDA GATES foundation

Organized by

Committee on Payments and Market Infrastructures
BANK FOR INTERNATIONAL SETTLEMENTS

WORLD BANK GROUP

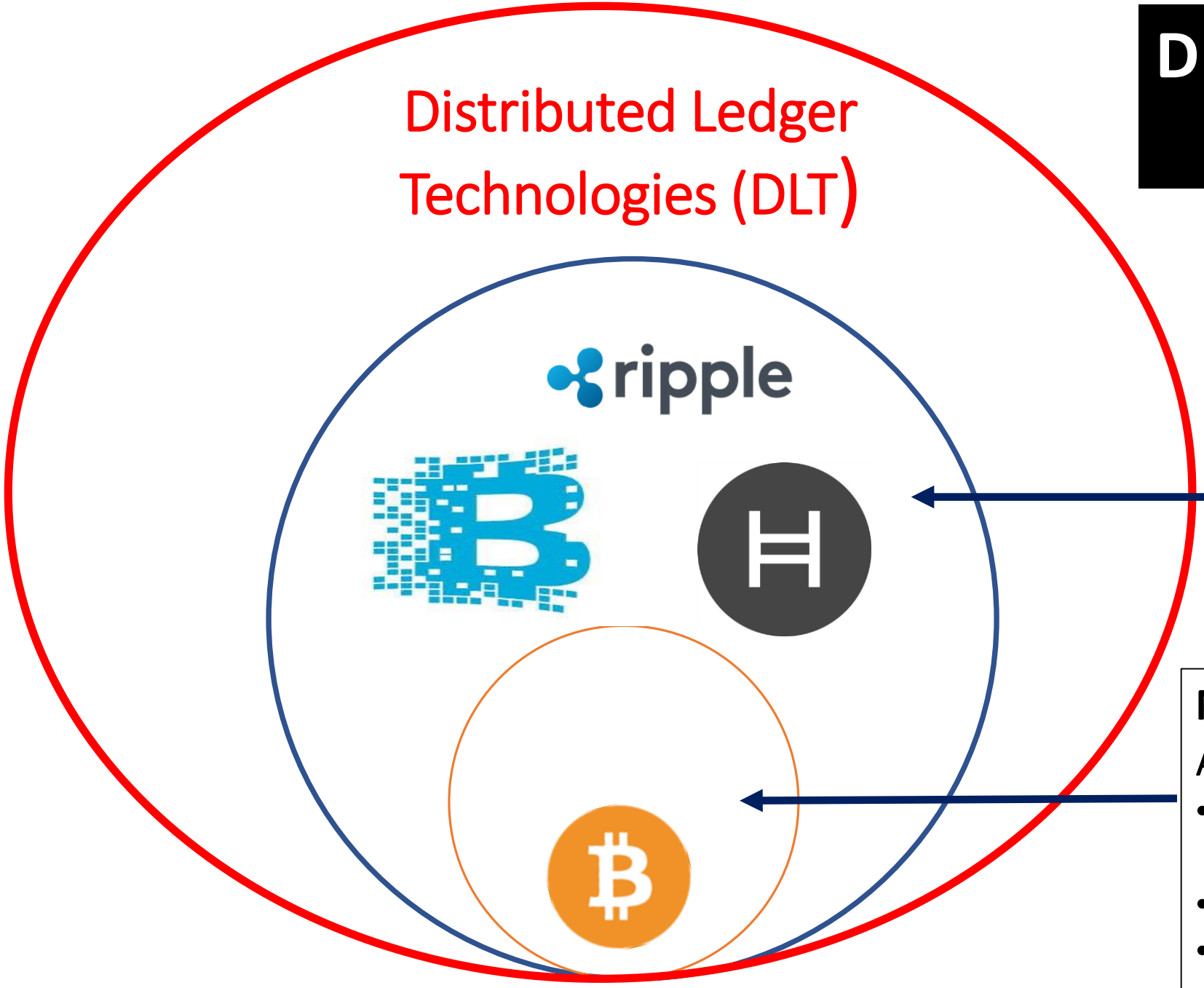
ITU

DLT Security Report (80+ pages)

- Overview Of Distributed Ledger Technologies
- Use Of DLTs For Financial Inclusion
- The Crypto-Economy & Smart Contracts

- Typical Actors And Components And Their Security Profiles
- General Security Risks And Concerns In Use Of DLTS
- Ecosystem-Wide Security Vulnerabilities
- Risks In Implementation Of DLTs
- Smart Contracts
- Software Development Flaws
- Transaction And Data Accuracy
- Conclusions & Recommendations

DLT TECHNOLOGY HIERARCHY



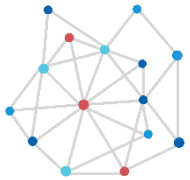
New Technologies:
Used To *Create* Applications

New Applications:
As a **crypto asset:**

- 'Crypto-currency' as a 'means of payment' (few applications)
- Utility token
- Initial Coin Offering
- Security Token

Blockchain Core Concepts

Type of Distributed Ledger



Data Stored In Sequential Blocks*

Cryptographic Keys

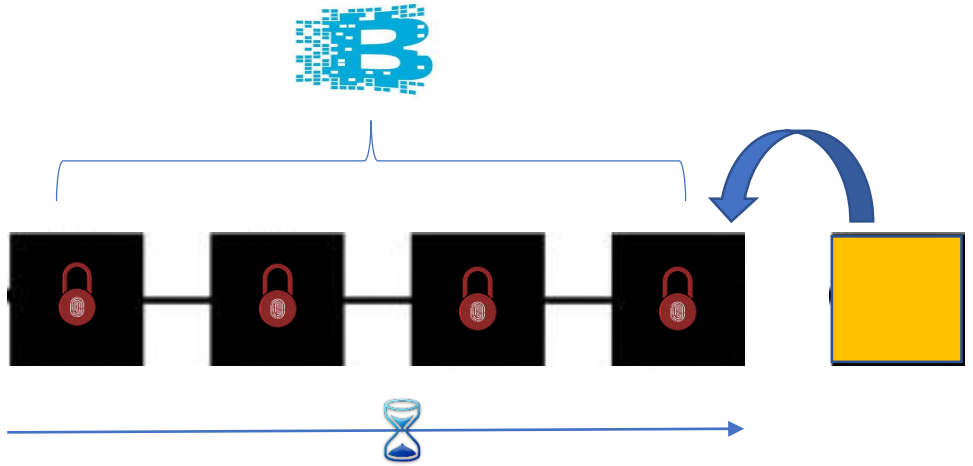
Tamper Evident*

Consensus

*NOT 'immutable'

Blocks On The Blockchain

- Transaction/info stored on **blocks**
- New data inputs from participants (nodes) are usually the result of **'mining'**
- As more data in new blocks added, (block) **chain** grows
- **Tamper Evident:** Tampering with the data is evident to everyone



The Crypto-Economy

Laws & Regulations

Crypto-Assets

UT | ST | CC
ICO | IEO

Users

Banks | Individuals
Institutions

Technology

DLT | Internet | dApps
Tokens | Wallets
Smart Contracts

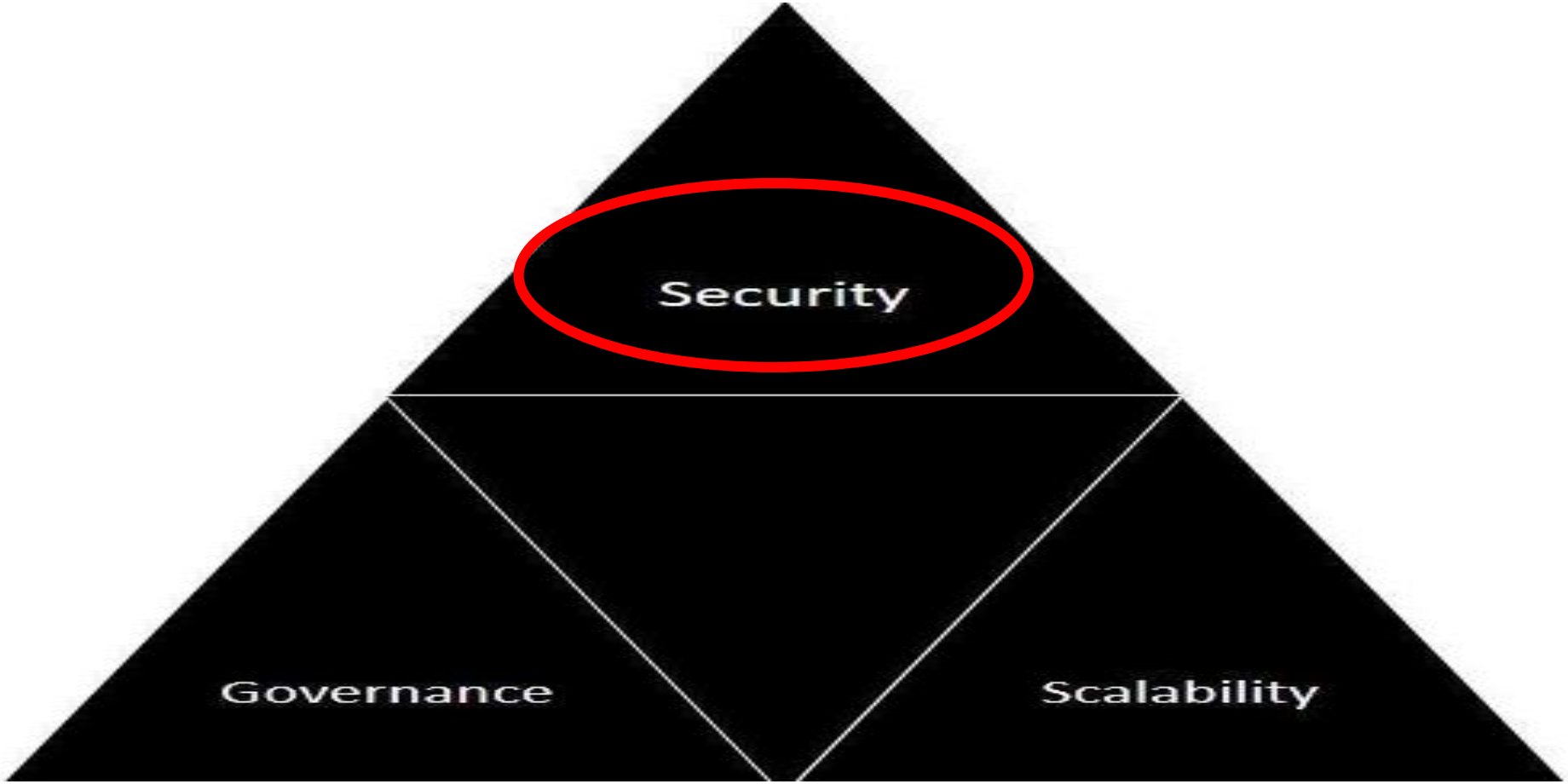
Actors

Miners | Custodians
Exchanges | Escrow
Developers | Banks
Institutions | Traders

Overall Summary

- DLTs are NOT 100% secure
  - Not even 80% secure, but improving….glacially
  - Vulnerabilities being addressed, but will take a while for technologies to mature
- Vulnerabilities applies to **ALL** DLTs eg DAG, blockchain types
- Security = technology **AND** governance of DLTs

The Blockchain ‘Trilemma’



Current DLT designs mean you cant have ALL three simultaneously !

Due to a widespread start-up mentality in the crypto-economy, security often takes a **backseat** to growth.

Number of evolving security risks are emerging with DLTs

- New risks **EVERY** week, sometimes every day
- Reflective of the new actors, technologies and products
- Users and enterprises all have significant risk profiles
- Not just the technology as a security risk….but also governance and implementation
- Exacerbated by the distributed nature of DLTs and the associated wide attack surface
- Some risks and vulnerabilities emanate from the non-DLT world eg DDoS

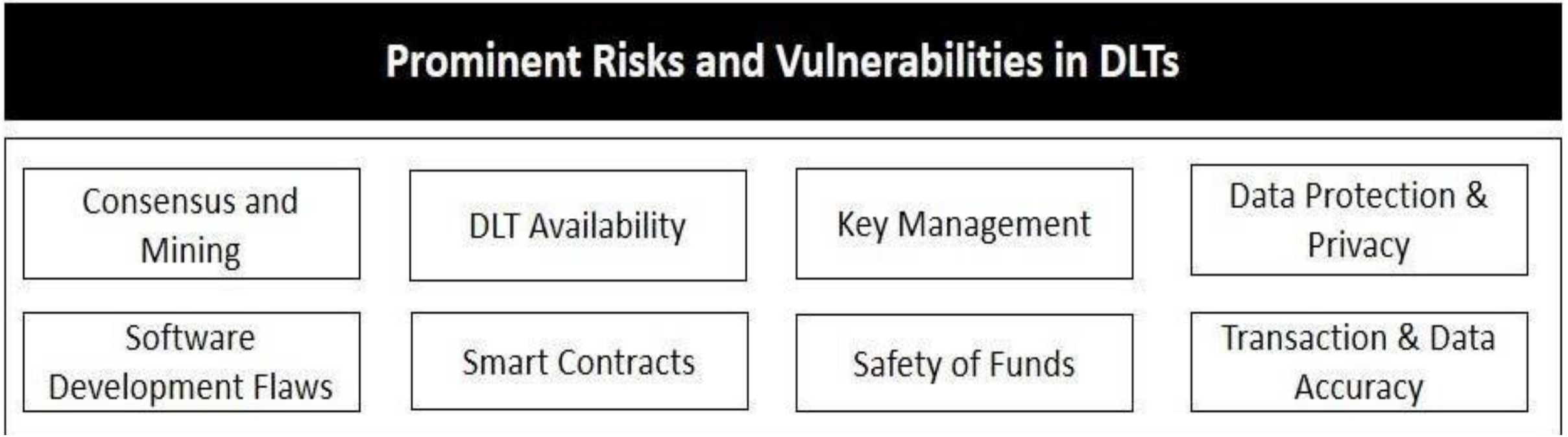
Main Attacks (2017-2019) on:

- Crypto-currency exchanges
- User crypto-currency wallets
- DLT technologies & implementation

Key DLT Security Risks and Vulnerabilities

- Software development flaws
- Bad architecting
- DLT availability
- Transaction and data accuracy
- Private key management
- Data privacy and protection
- Safety of funds via wallets & crypto-exchanges
- Consensus in adding data to a DLT
- ‘Smart contract’ implementation flaws
- Use of ‘offline’ Oracles

Stylized Prominent Risks and Vulnerabilities in DLTs



This taxonomy developed based on a survey of the most frequent risks permeating the DLT ecosystem worldwide

Typical participants in DLTs & Security Aspects of their Roles

Type	Typical Role in DLTs	Security Aspects
Inventors	First publisher of new DL technology	May not provide a method of collegially updating a DL, leading to multiple forks.
Developers	Independent parties who may improve on the initial DL technology	May not agree amongst themselves, leading to lapses in improvements
Miners	Paid to add new data to blocks	Those with 51% mining power may act to unilaterally change the form and data structure on a DL
Users	Use data or value stored on a DL or exchange	May not sufficiently secure their PINs for wallets and exchanges.
Oracles	Provide input/output data for use in Smart Contracts	Usually insecure and may feed incorrect data into a DLT
Centralized Exchanges	Exchange tokens, custodians of token credentials/keys, facilitate ICOs, STOs and IEOs	'Honey pot' for hackers due to lack security implementations. May not implement security controls; DDOS attacks.
Nodes	Hold copies of a Distributed Ledger	May go offline and thus increase possibility that a DLT is compromised/hacked
Auditors	May test smart contracts for coding errors and/or legal validity	Could catch and fix vulnerabilities before exploitation
DLT Network Operators	Define, create, manage and monitor a DLT network.	May not implement security controls; DDOS attacks.

Implementation Attacks

- The closer gets to the core of blockchain technology, the **more difficult it is to succeed with an attack.**

- **Instead:** Attacks against blockchain **implementation** & support tools:

  - Often similar to exploits of traditional centralized software and web applications.
  - Has resulted in DDOS denial of service attacks, coin theft, data exposure
  - Costs ‘Gas’ to fix in case of Ethereum
  - Commonly discovered and fixed **after** release.
  - Difficult to build and maintain secure code while explosive growth

….Areas of Risks & Concerns in DLT use

Areas of Concern	Examples
'Download & Decrypt Later'	Longevity of the security data on Distributed Ledgers
Authorized Access	Nodes on DL usually cannot distinguish between a transaction by un/authorized, users with key access.
Vulnerabilities in Nodes	Node non-availability may disrupt DL use
Transfer of Data Between Distributed Ledgers	Interoperability Attempts Between DLs Raises Concerns *eg Layer 2 lightning networks are insecure*
Open Source Software Development in DLT	The underlying code in any DL may have security flaws
Trust of Nodes	Trade-off between replacing costly – and often risky – intermediaries with nodes.
User Interface/User Experience Failures	Wallets etc

Potential Effect of Quantum Computing

Encryption Name	Type	Use	Staus
AES-256	Symmetric Key	Encryption	Ok, but larger key sizes needed
SHA-256, SHA-3		Hash function	Ok, but larger output needed
Lattice-based (NTRU)	Public Key	Encryption; signature	Believed
Code-based	Public Key	Encryption	Believed
Multivariate polynomials	Public Key	Encryption; signature	Believed
Supersingular ellptic curve isogenies (SIDH)		Encryption; possibly signature	Believed
ECDSA, ECDH	Public Key	Signatures; Key exchange	No longer secure
RSA	Public Key	Signatures; Key establishment	No longer secure
DSA	Public Key	Signature	No longer secure

Issue: 'No longer secure' indicates that researchers have found that these encryption types subject to quantum computing attacks.

Risks: 'Download and Decrypt Later' breaking of private keys; transaction accuracy; and leakage of private data.

[**Data from ID Quantique**]

Causes of Risks and Vulnerabilities in DLTs

- Rush to implement solutions not properly tested
- Inexperienced developers
- 'Wisdom of the crowd' development
  - Means no central security assessments
- Dependencies on often insecure 3rd party external data inputs
  - 'Oracles' input/output are vulnerable (offchain)
- Crypto-exchanges & user wallets poor security, billions stolen
- New DLT protocols varying initial designs with complex & untested log
- Start-ups without resources to assess and address security issues.

Recommendations (Policy Makers)

- Could develop (or even mandate) principles rather than specific technologies or standards for those involved in developing and implementing DLTs

- Security audits could be mandatory

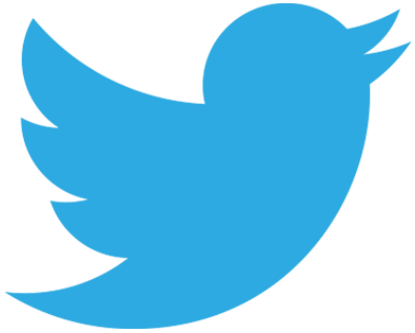
- Use of 2FA methodologies if available in a particular environment.

Recommendations (DLT in Dev World)

	Who	How: System Level	How: Individual Level
DESIGN	Who would set up, maintain, test, and update security? Who would be responsible for preventing and recovering from potential breaches?	How would you ensure that vulnerable data was protected as cryptographic and hacking technologies evolve? How could peripheral connections to a blockchain such as oracles be vulnerable to security threats? Would different information be protected in different ways?	How would you ensure that individuals were aware of and could protect themselves against potential security threat? How would you ensure that users maintain effective and safe access to private keys? How would you ensure a (safe) and reliable mechanism for users to recover lost keys?
ASSESSMENT	Who understands the technology and the evolution of it well enough to create adequate security?	What are security risks faced by the community as a whole? Where are the peripheral connections to the blockchain that may cause risks to the system and veracity of data? What information is the most vulnerable and how can it be protected?	Do users have experience protecting themselves against security threats? What mechanisms can users use to protect themselves and recover from security threats? How would users be alerted to compromise of their data?
EVALUATE	How do you ensure that the stakeholders are incentivized to adequately protect the system?	Does the system remain secure as technologies, politics, and other social factors change? What mechanisms will be undertaken to periodically test the system for vulnerabilities?	Does the system make users more susceptible to security risks? Can they adequately protect themselves? Is the key system accessible to users without compromising security? Can users recover from lost keys, and prevent interim use of those keys?

FIGI FINANCIAL INCLUSION GLOBAL INITIATIVE

Thank you!



@leonperlman