A Reality Check on Blockchain

Khaled Salah

ksalah@ieee.org

IEEE UAE Cyber Intelligence Summit, Dubai, October 25, 2018

Outline

(1) Background and Current State

(2) Non-security Challenges

(3) Security Challenges

Global Blockchain Council backs du Pilot for First Blockchain Service for Healthcare in Middle East

Monday, 30 May 2016

Together with the support of Dubai Future Foundation through the Global Blockchain Council, du today announced plans to revolutionise healthcare in the UAE using pioneering blockchain technology. For the first time in the UAE, du's pilot will introduce a safer common system for instantly sharing and verifying electronic health records (EHR) between hospitals and clinics.

arabian Business.com

EDITION: INT 'L | YOU ARE NOT LOGGED IN: SERVICES | LANGUAGE: بالعربية

All Articles Videos Photos Companies People

GCC Industries Markets Opinion Interviews Photos Videos Lists Lifestyle StartUp CEO Company News Property

Banking & Finance Construction Education Energy Healthcare Media Real Estate Retail Technology Transport Travel & Hospitality

Dubai's Emirates NBD joins India's ICICI on blockchain project

Blockchain works as an electronic transaction-processing and record-keeping system through a secure network

GULF NEWS

GOVERNMENT

December 3, 2016 | Last updated 1 minute ago

UAE NEWS BUSINESS SPORT OPINION LEISURE LIFE&STYLE

COURTS 2 CRIME 1 WEATHER 2 SOCIETY 22 HEALTH 1 TRANSPORT 1

Dubai launches Blockchain strategy to become paperless by 2020

Hamdan unveils ambitious plan to save 25 million work hours annually through paperless transactions

Published: 20:22 October 5, 2016

GULF NEWS

UAE Pushes Blockchain Tech Development to Become a Leading Center for Innovation

Dec 26, 2016 04:05 PM by Diana Ngo

The Telegraph

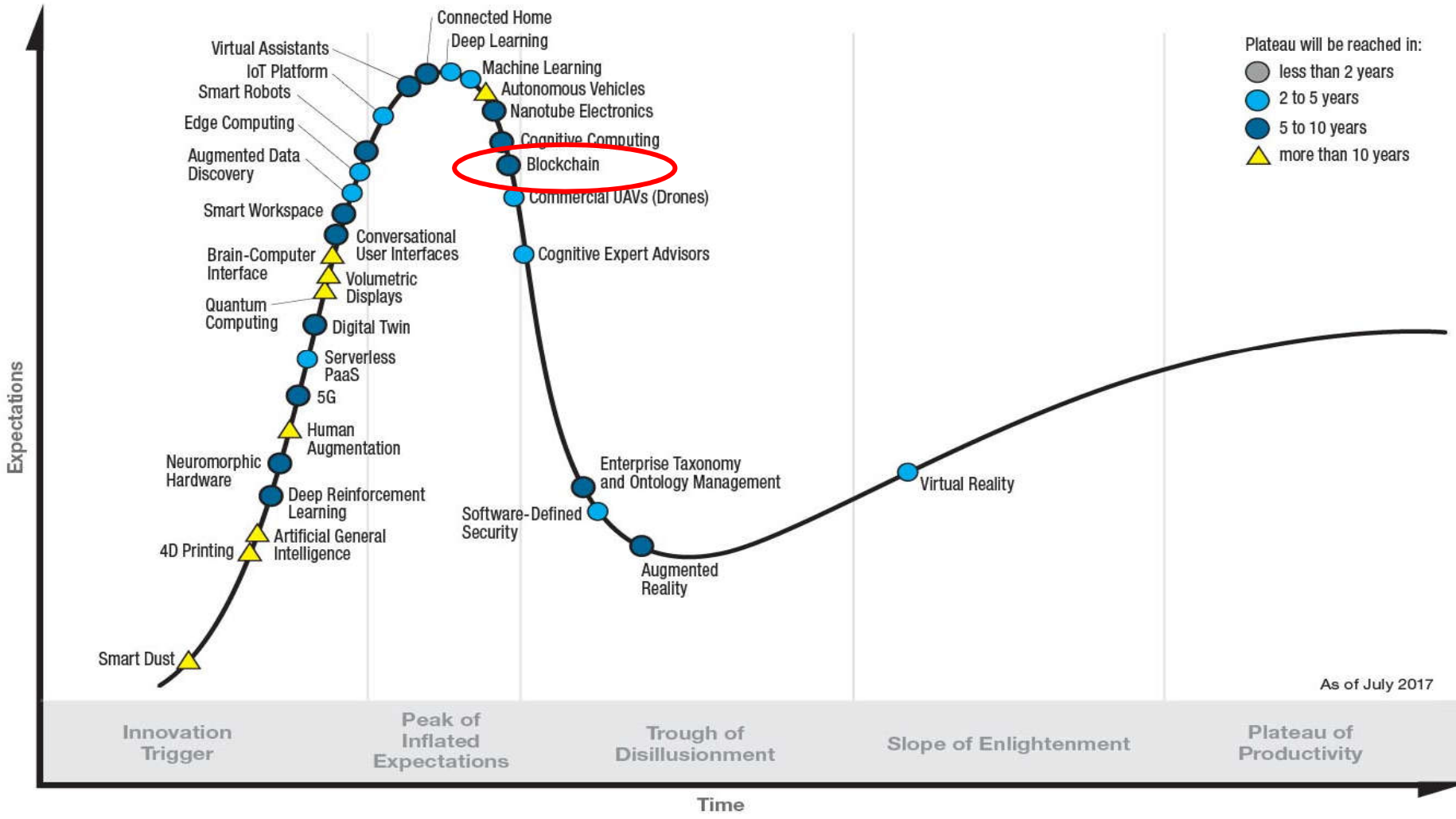
Home Video News World Sport Business Money Comment Culture Travel Life W

HOME » FINANCE » MARKETS

Nasdaq makes first share trade using blockchain technology

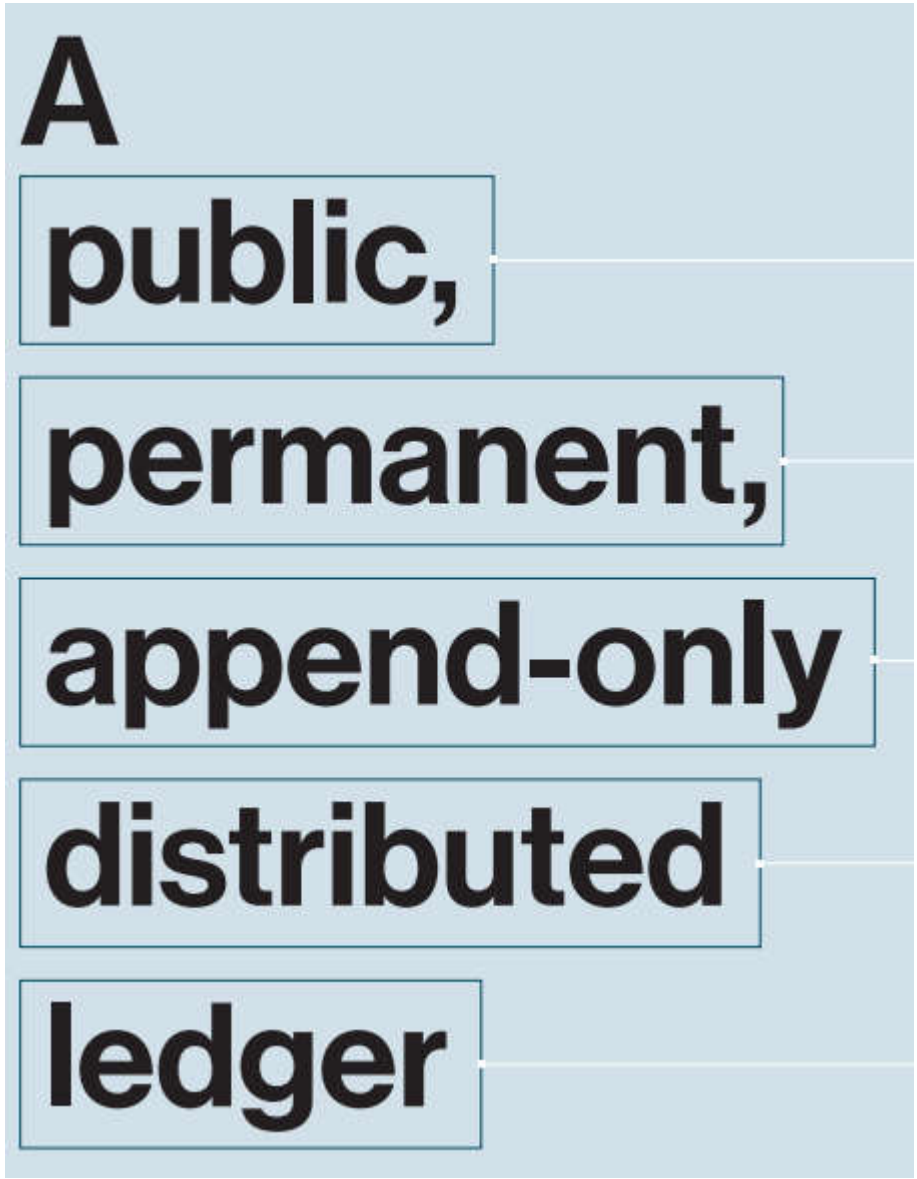
Market operator has spent millions experimenting with the technology behind Bitcoin

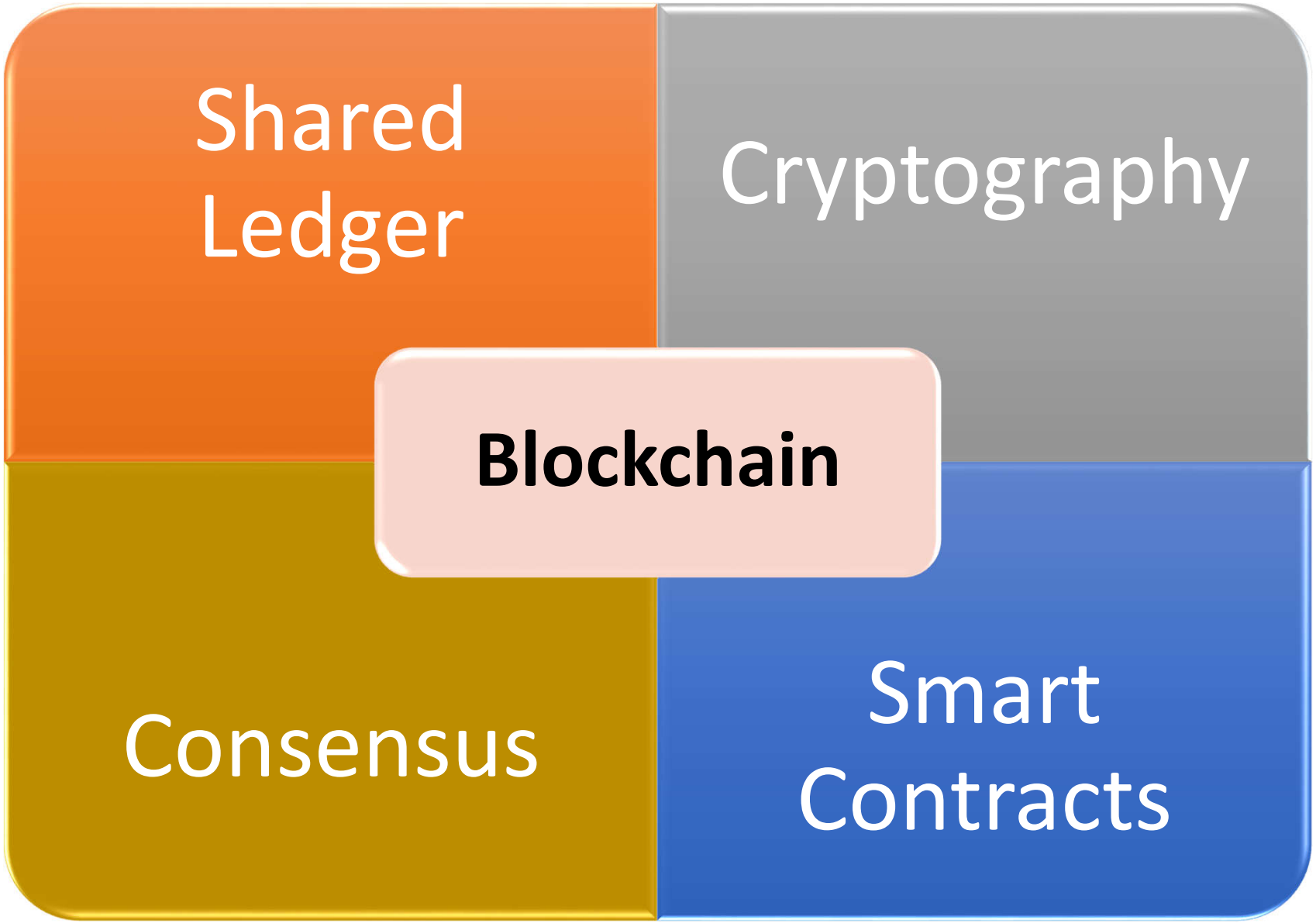
Gartner Hype Cycle for Emerging Technologies, 2017

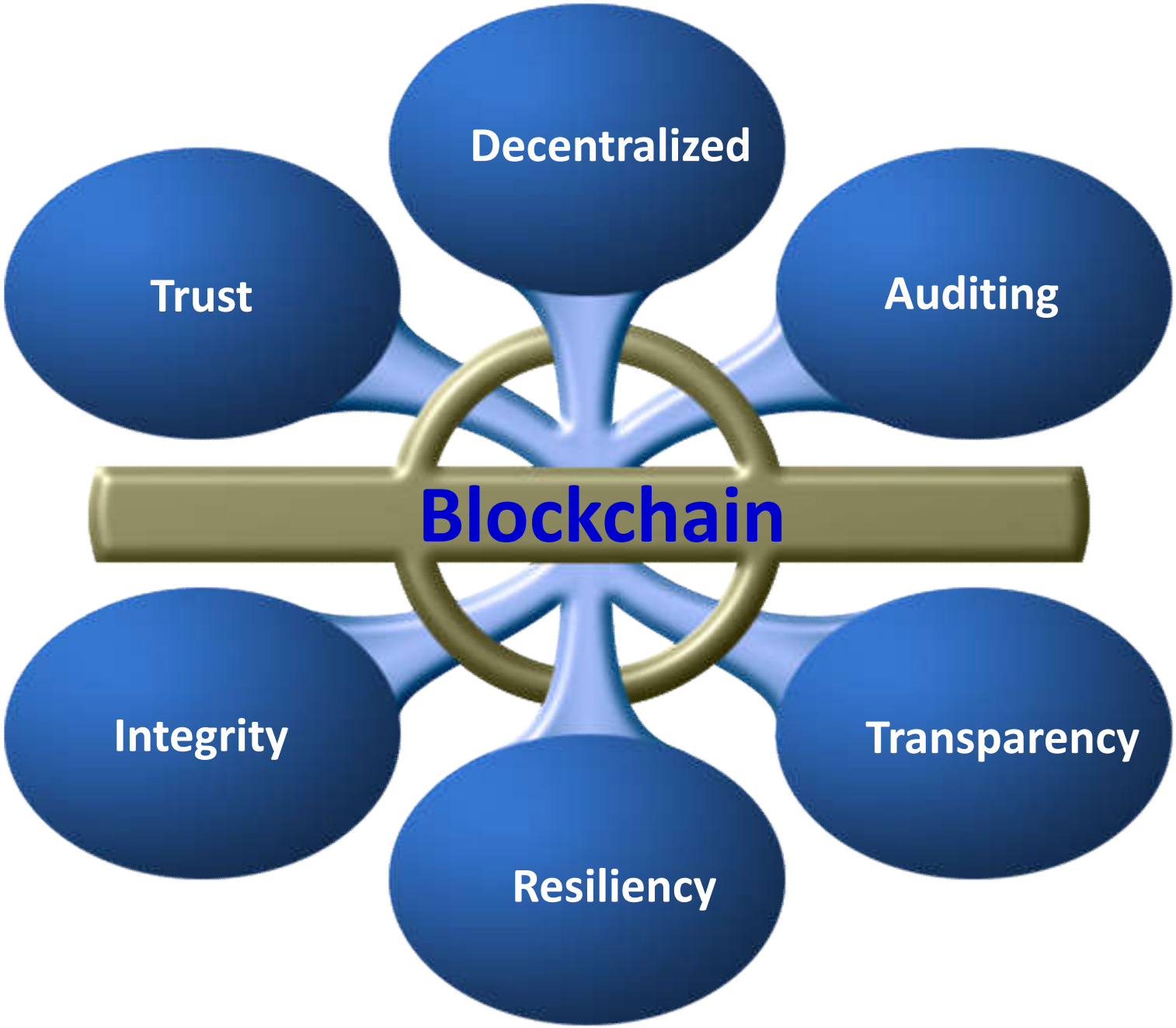


What is Blockchain?

#blockchain


A
public,
permanent,
append-only
distributed
ledger


Shared Ledger
Cryptography
Blockchain
Consensus
Smart Contracts


Decentralized
Trust
Auditing
Blockchain
Integrity
Transparency
Resiliency

Reality Check …

Challenges to Growth and Mainstream Adoption

Blockchain challenges – non security

- Scalability
- Blocktime
- Power consumption
- Governance
- Arbitration
- Standards
- Regulation
- Interoperability
- SideChains
- More centralized
- GDPR
- **Smart contracts**
  - Un-upgradable
  - Deterministic
  - Limited
  - Oracles

Blockchain challenges - Security

- Trusted oracles
- Smart contracts vulns & bugs
- Privacy
- Key storage & management
- TEE
  - Trust Intel?
- Key collision ~10^{-48}
- 51% attacks
- and ...

Impact of Quantum Computing

Cryptographic Algorithm	Type	Purpose	Impact from large-scale quantum computer
AES	Symmetric key	Encryption	Larger key sizes needed
SHA-2, SHA-3	----------	Hash functions	Larger output needed
RSA	Public key	Signatures, key establishment	No longer secure
ECDSA, ECDH (Elliptic Curve Cryptography)	Public key	Signatures, key exchange	No longer secure
DSA (Finite Field Cryptography)	Public key	Signatures, key exchange	No longer secure

Takeaways

- Blockchain will continue to gain traction
- Has serious challenges
- *Immature* solutions are emerging
- Be wary …

thankyou

ksalah@ieee.org