ITU Workshop on "FG DFC Workshop on Standards for Digital Fiat Currency (DFC)"
(Beijing, China, 12 October 2017)

# Key Security Issues for implementation of Digital Currency, including ITU-T SG17 activities

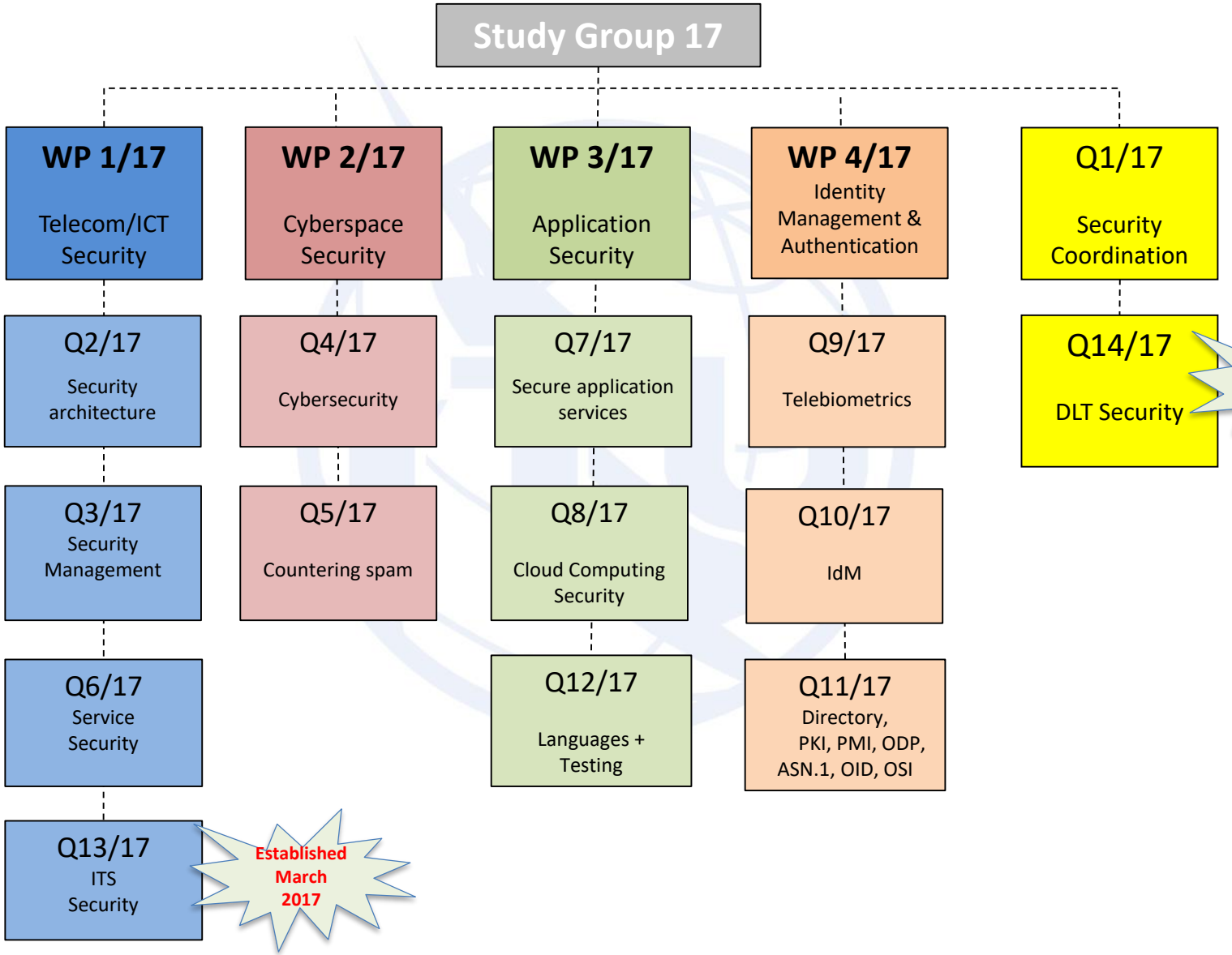
Heung Youl Youm, PhD.

Chairman of ITU-T SG17
Professor, SCH Univ. Korea

# ITU-T Study Group 17

- Title: Security
  - Responsible for building confidence and security in the use of information and communication technologies (ICTs).
- A lead study group for :
  - Security
  - Identity management (IdM)
  - Languages and description techniques
- This lead study group is responsible for the study of the appropriate core Questions.
- As of October 2017, there are 14 Questions in SG17.

# Structure of ITU-T SG17, Security




Beijing, China, 12 October 2017

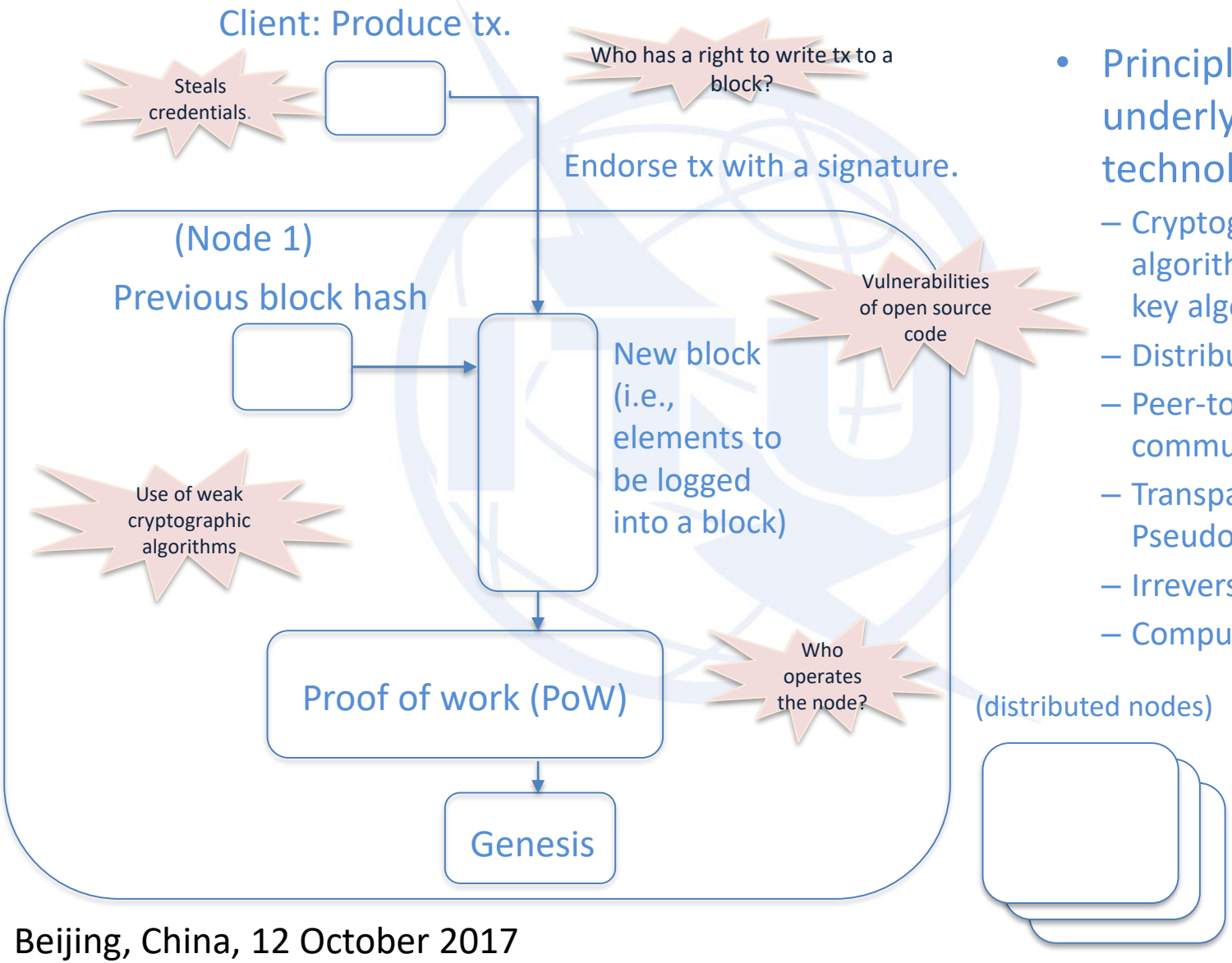
# Recent SG17 activities in DLT security (1/2)

- ITU-T SG17 held ITU workshop on security aspects of blockchain on March 21, 2017.
- SG17 at its March 2017 meeting discussed ways forward:
  - establishment of new Question on security aspects of blockcahin;
  - creation of new Focus Group on security aspects of blockchain; or
  - establishment of several new work items.
- ITU-T March 2017 SG17 meeting proposed TSAG to consider the establishment of a Focus Group on Blockchain under the auspices of TSAG as the liaison to TSAG in TD 277.
- At the request of SG17, the May 2017 TSAG meeting then agreed to the creation of the new ITU-T Focus Groups on Application of Distributed Ledger Technology (FG DLT) under the auspicious of TSAG.
- SG17 at its September 2017 meeting established a new Question 14/17, titled “Security aspects for Distributed Ledger Technologies”.
- SG17 approved 7 new work items under a new Q14/17.

# Bitcoin, Decentralized Digital Currency

- Virtual currency > Cryptocurrency > Bitcoin
- A cryptocurrency that uses blockchain technology.
- A digital currency (DC) allows two users to exchange value without the need for an intermediary, wholly digitally.
- Both a currency and a payment system.
- Using a process known as mining, which involves users needing to solve a cryptographic puzzle.
  - Once the puzzle has been solved, a new Bitcoin is issued, and its presence is announced to Bitcoin users – nodes - on the Bitcoin blockchain.
- Spending of a Bitcoin cryptocurrency unit, or issuance of a new Bitcoin by 'miners', is sent across the nodes for verification.
- The purpose of the blockchain is to track Bitcoin spending, specifically to prevent 'double spending' of the same Bitcoin.
- Known as permissionless and public Blockchain.

# A example model and typical threats to DC




- Principles underlying the technology
  - Cryptographic algorithm, e.g., public key algorithm
  - Distributed ledgers
  - Peer-to-Peer communication
  - Transparency with Pseudonymity
  - Irreversibility of Blocks
  - Computational Logic

# Potential threats, risks for an implementation of DC

# Vulnerabilities in Wallet

- There have been very high frequent intrusions into the ‘Wallet’ that stores DC, resulting in huge loses for Bitcoin owners.
- A hardware security modules (HSM) based wallet or secure zone based wallet is preferred for a high profile DC, which stores cryptographic keys and performs critical functions such as encryption, decryption and authentication.
- Hardware based wallet can provide more robust security than software based one.

# Long-term weakness of cryptographic algorithms used in DC

- If a quantum computer that outperforms classical supercomputers is built, due to Shore's algorithm, it could break RSA algorithm with a key length of 2048 and 3072. In a similar manner, it could also break the digital signatures (e.g., ECC 256, ECC 521) used in Bitcoin and other cryptocurrencies.
- Cryptographic algorithms get weaker over time, but the data remains in the DC.
- Deprecated crypto algorithms could be replaced with new secure ones, which are used for DC.
  - The possibility of 'old' transactions on a particular DC may be vulnerable to advance in cryptography analysis over a period of years or decades such 'old' transactions can be undetectably modified.



○ Why Quantum Computing's Threat To Bitcoin And Blockchain Is A Long Way Off

# Use of weak credentials for entity authentication

- Nodes on the DC are unable to distinguish between a transaction by an authorized user and a fake transaction by someone who somehow has gained access to the DC trusted party's private keys.
- Risk for loss of funds where credentials are controlled by a single entity was demonstrated in the recent compromise of the credentials used in the transfer of funds through the (non-DLT) SWIFT network from the Federal Reserve Bank of New York to the central bank of Bangladesh, Bangladesh Bank.
- Novel key management functions or biometric linked private keys (in FIDO) need be used.

# Vulnerabilities of the underlying open codes in Digital Currency

- The open source codes are normally used to implement applications and services for DC.
- The underlying open codes in any implementation of DC may cause a security issue.
- The exploitation of a flaw in the DC may potentially lead to compromise of the immutability paradigm of DC, which may result in lost funds of the DC owner.
- Secure coding, the practice of writing programs that are resistant to attacks by malicious people or programs should be used.
  - for example, avoiding buffer overflows and underflows, validating input and interposes communication, race conditions and secure file operations, etc.

# Conclusions and Recommendations

- Take care seriously of security risks in the surrounding of DC system itself.
- Consider evaluating long-term security risks and prepare for their countermeasures to these risks.
- Enable large scale trust and federation without the need of one to one trust relationship.
- Some key works, e.g., cryptographic algorithms profile, proof of work, authentication, credential management, and security level of assurance for implementation of DC, need to be studied.