Blockchain Security in ITU-T

May 21, 2018

Heung Youl Youm
Chairman, ITU-T SG17 (Security)
Prof., SCH University, Korea

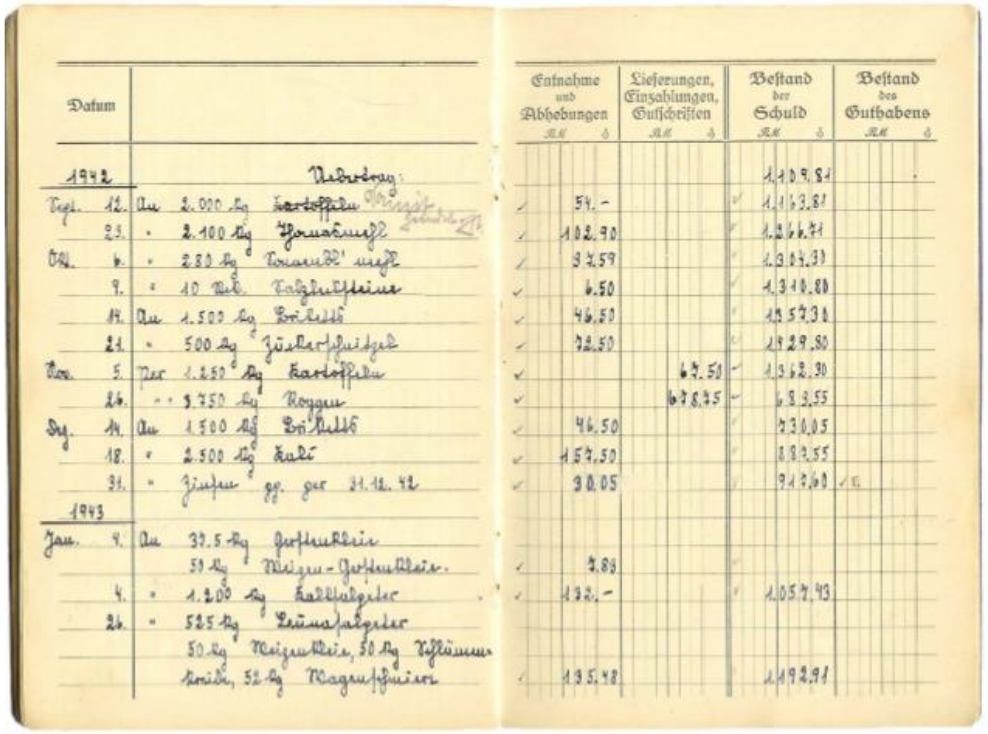
SOON CHUN HYANG UNIVERSITY

Contents

- Overview of Blockchain
- ITU-T SG17
- FG DLT
- FG DFC
- Conclusion

Ledger

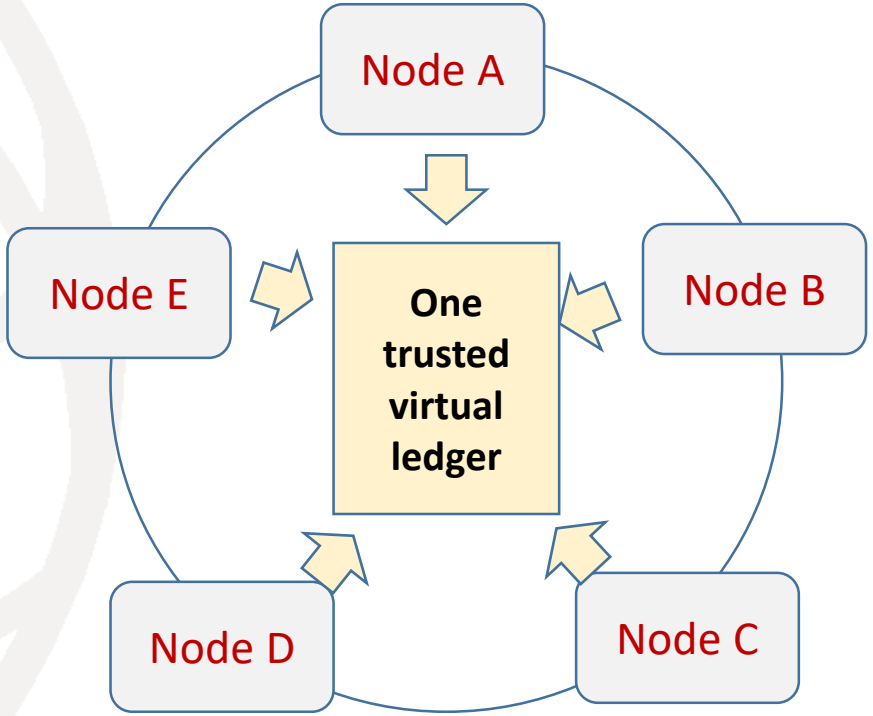
- Ledger records all business activities as transactions.
  - Databases
- Every market and network defines a ledger.
- Ledger records asset transfers between stakeholders.
- Problem
  - (Too) many ledgers
  - Every market has its ledger.
  - Every organization has its own ledger.



Datum		Entnahme und Abhebungen RM ₰	Lieferungen, Einzahlungen, Gutschriften RM ₰	Bestand der Schuld RM ₰	Bestand des Guthabens RM ₰
1942	Uebertrag:			1.109.81	
Sept. 12.	Zu 2.000 kg Kartoffeln	54.–		1.163.81	
23.	" 2.100 kg Futtermehl	102.90		1.266.71	
Okt. 6.	" 280 kg Futtermehl mehl	32.59		1.299.31	
9.	" 10 Ztr. Futterkleie	6.50		1.310.80	
14.	Zu 1.500 kg Futterkalk	46.50		1.357.30	
21.	" 500 kg Zuckerschnitzel	22.50		1.379.80	
Nov. 5.	Per 1.250 kg Kartoffeln		62.50	1.362.30	
26.	" 9.750 kg Roggen		678.75	683.55	
Dez. 14.	Zu 1.500 kg Futterkalk	46.50		730.05	
18.	" 2.500 kg Kali	157.50		887.55	
31.	" Zinsen gg. per 31.12.42	30.05		917.60	
1943					
Jan. 4.	Zu 37.5 kg Futterkleie				
	50 kg Weizen-Futterkleie.	2.80			
4.	" 1.200 kg Kalkhalbleder	132.–		1.057.40	
26.	" 525 kg Leimsalpeter				
	50 kg Weizenkleie, 50 kg Futterkleie				
	Kreide, 52 kg Magnesiumsulfat	135.48		1.192.91	

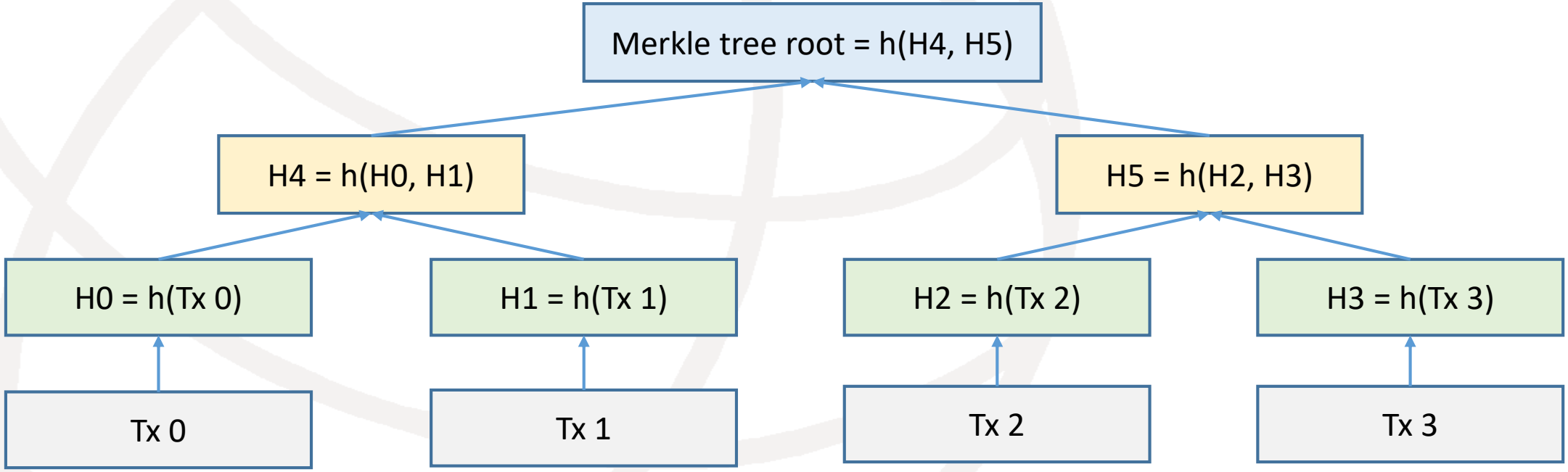
Blockchain = one trusted virtual ledger.

- Blockchain creates one single trusted ledger for all node.
- A append-only distributed ledger, where records are stored in blocks, and blocks form a chain.
- Distributed ledgers implemented by multiple parties, not by a centralized intermediary.
- Replicated and produced collaboratively.
- Trust in ledger from
  - Cryptographic mechanisms, such as Merkle-Hellmann Hash tree
  - Distributed validation such as PoW

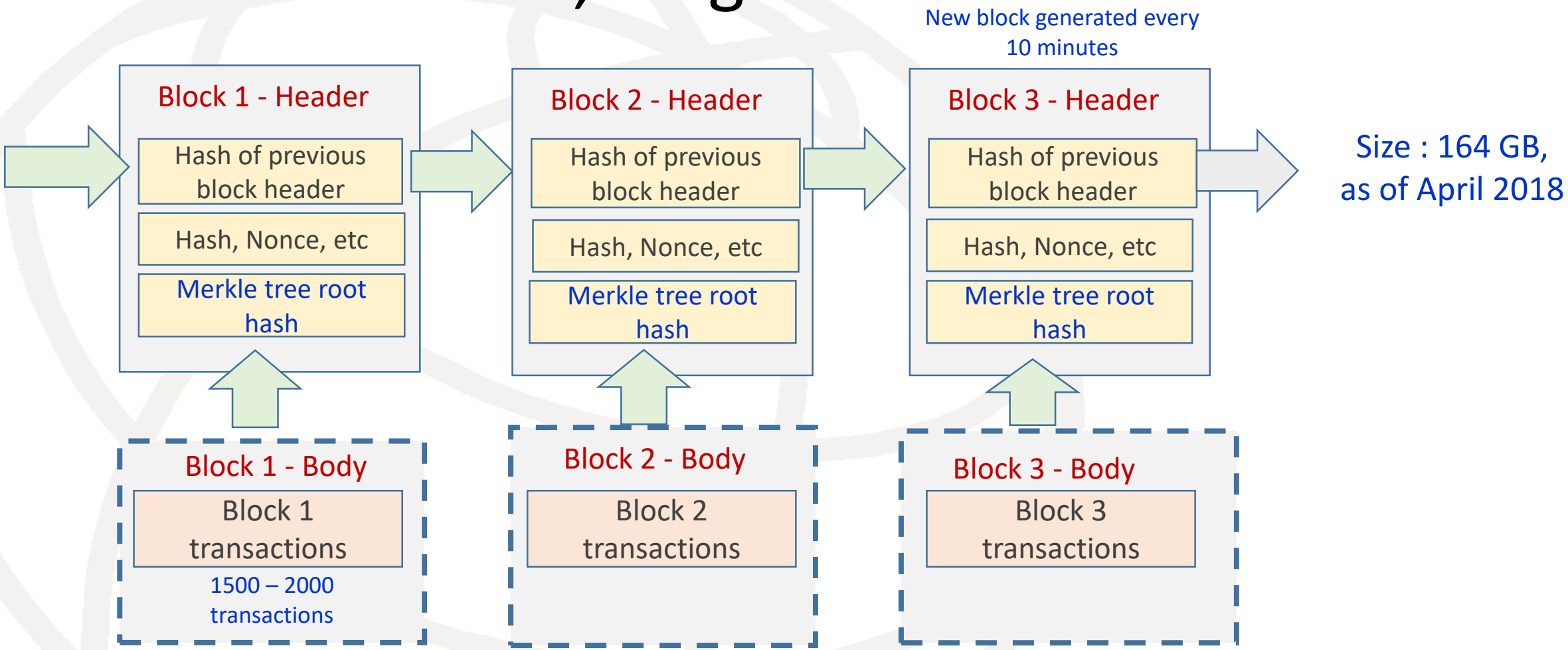


Merkle tree and transactions

- A data structure where the data is hashed and combined until there is a singular root hash that represents the entire structure.



Bitcoin blockchain, ledger

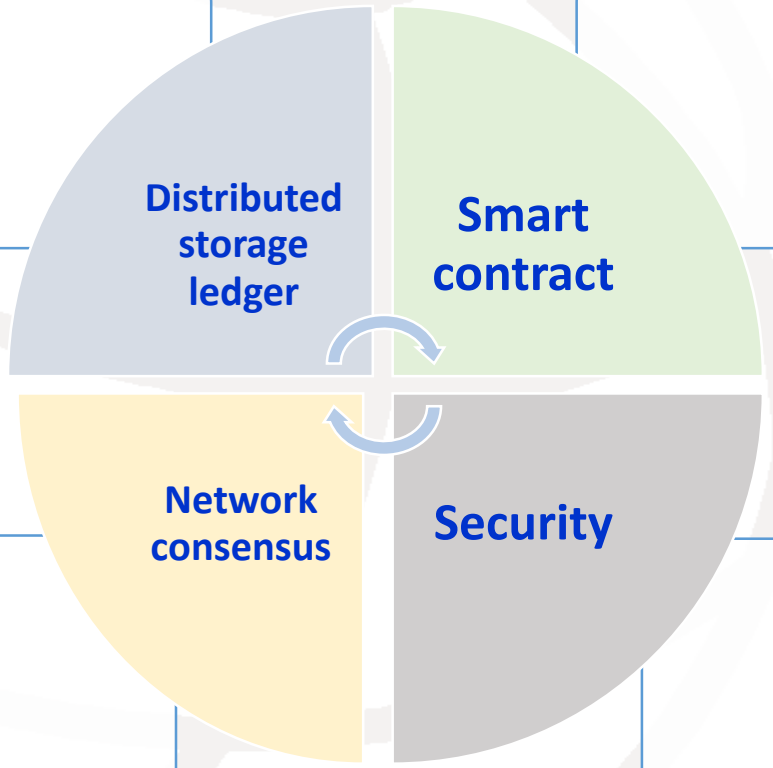


- A hash chain is a sequence of records in which each record contains the hash of the previous record in the chain, and the hash of all the current record's content (Merkle root).

Blockchain technology – key properties

- A chronological **record of transactions** in a distributed ledger

- Business logic embedded in ledger that can be triggered when certain conditions are met.



- All participants agree to a network verified transaction by consensus.

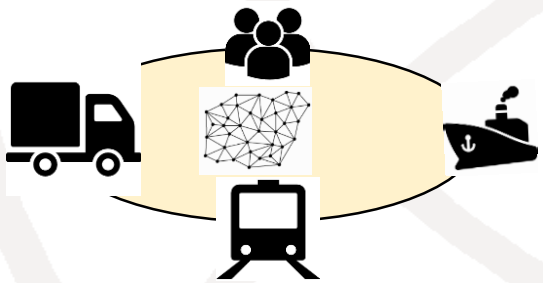
- Cryptography is a central feature, transactions are secure, authenticated & verifiable .

Types of Blockchain and their example

Permission-less, Public	Permissioned, Public
• Bitcoin • Etherium	• Land properties • University certificate
Permission-less, Private	**Permissioned, Private**
• Public poll	• Medical record

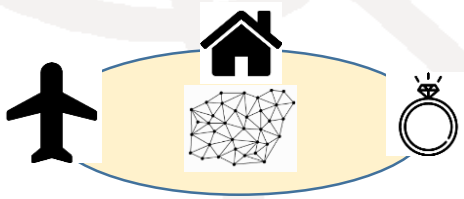
Permissioned vs. Permissionless: Who can write data to a Blockchain (i.e., accessibility)
Public vs. Private: Who can read from a Blockchain (i.e., visibility)

Exemplary Blockchain use cases



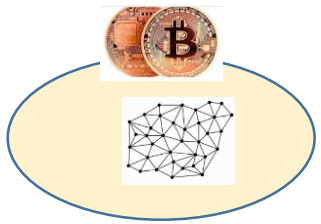
Supply Chain Management

- Visibility and data consolidation
- Traceability, Transparency, verifiability
- Reduced fraud, minimize courier cost
- Increase partner trust



Property management

- Ownership of both physical and non-physical property to be verified, programmable and tradeable
- The ownership details of a property written on the Blockchain.



Financial Application

- Fast, secure and global transaction
- Reduced settlement times
- Increased credit availability Transparency & verifiability
- No reconciliation cost

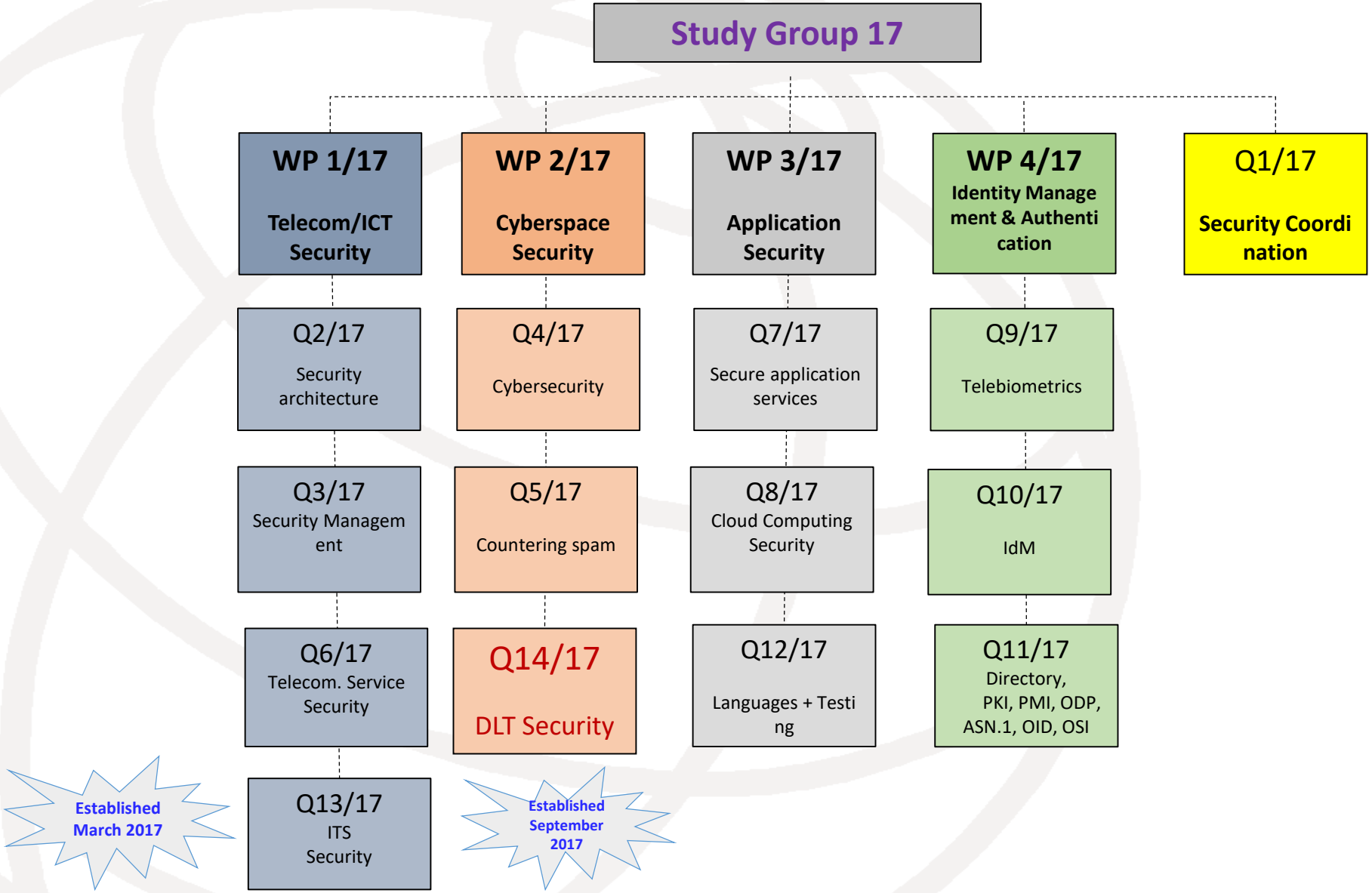
Contents

- Overview of Blockchain
- ITU-T SG17
- FG-DLT
- FG-DFC
- Conclusion

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.
  - 12 approved by WTSA-16
  - 2 established in 2017 after WTSA-16

Structure of ITU-T SG17, Security



ITU-T Question 14/17

- Question on security aspects for distributed ledger technologies
  - SG17 agreed to establish this new Question at its September 2018 SG17 meeting.
  - TSAG endorsed its establishment at its March 2018 TSAG meeting.
  - SG17 approved this Question at the March 2018 SG17 meeting.

- New work items established
  - SG17 has agreed to establish 9 new work items.

Q14/17 Tasks in ToR

- Tasks include, but are not limited to: Perform a gap analysis on ongoing security relevant work in other organizations for distributed ledger technologies.
- Produce a set of Recommendations providing comprehensive security solutions for DLT based applications and services.
- Study further to define security aspects of applications and services based on DLT, which are based on telecommunication/ICT networks.
- Study and identify security issues and threats in applications and services based on DLT.
- Study and develop security mechanisms, protocols and technologies for applications and services based on DLT.
- Study and develop secure interconnectivity mechanisms for applications and services based on DLT.
- Study and identify PII protection issues and threats in applications and services based on DLT.
- Study and develop information management system for entities providing applications and services based on DLT.

9 new work items (as of May 2018)

- Security for DLT
  - ITU-T X.sct-dlt, Security capabilities and threats of Distributed Ledger Technology
  - ITU-T X.sra-dlt, Security Framework for Distributed Ledger Technology
  - ITU-T X.sa-dlt, Security assurance for Distributed Ledger Technology
  - ITU-T X.dlt-sec, Privacy and security considerations for using DLT data in Identity Management
- Security by DLT
  - ITU-T X.ss-dlt, Security Services based on Distributed Ledger Technology
  - ITU-T X.stov, Security threats to online voting using distributed ledger technology
  - ITU-T X.str-dlt, Security threats and requirements for digital payment services based on distributed ledger technology
  - ITU-T X.tf-spd-dlt, Technical Framework for Secure Software Programme Distribution Mechanism Based on Distributed Ledger Technology
  - ITU-T X.das-mgt, Security framework for the data access and sharing management system based on the distributed ledger technology

Activities in ITU-T SG13, SG16, SG20

- Study Group 13 (Future networks)
  - Y.NGNe-BC-reqts, Scenarios and capability requirements of blockchain in next generation network evolution
  - Y.BaaS-reqts, Cloud computing - Functional requirements for blockchain as a service
- ITU-T SG16 (Multimedia)
  - Requirements for distributed ledger services
- Study Group 20 (IoT, smart cities and communities (SC&C))
  - ITU-T Y.IoT-BoT-fw, Framework of blockchain of things as decentralized service platform

Contents

- Overview of Blockchain
- ITU-T SG17
- FG DLT
- FG DFC
- Conclusion

What is a Focus Group?

- Created to study a well-focused topic, under clear Terms of Reference (ToR), and report findings to its parent group.
- Normally less than 2 years' life time.
- Can be created by TSAG if the topic is across multiple SGs or by a SG if the topic is within the mandate of that one SG.
- Any individuals including non-members from an ITU Member State can participate (except on ITU-T strategic, structural or operational matters).
- For topics not clearly within the mandate of a single SG, TSAG and cross-SG management consultation is required to establish a FG.

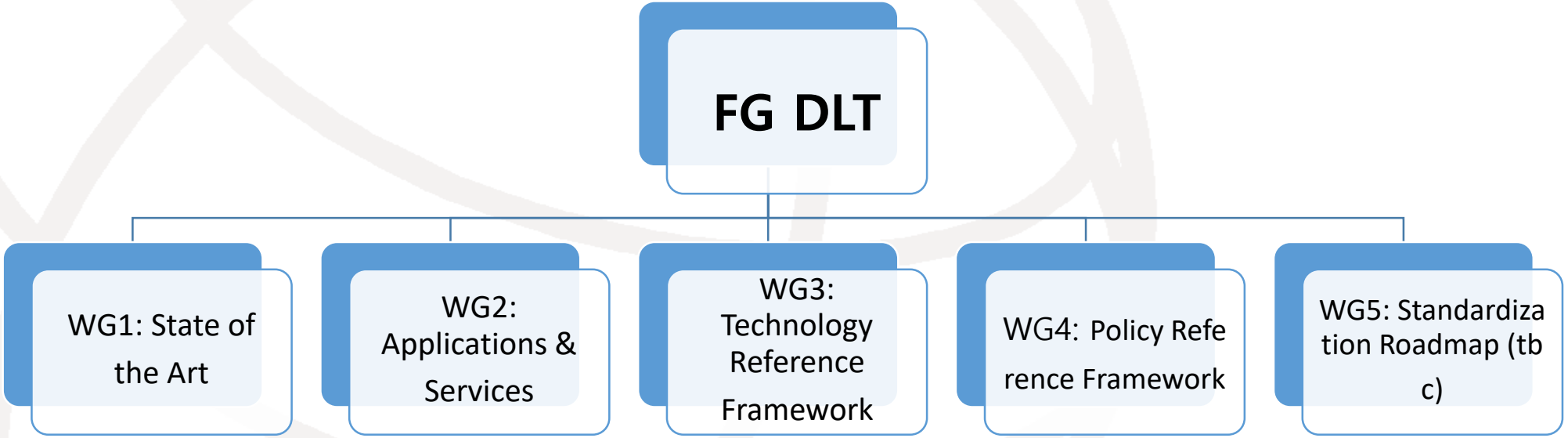
FG on Application of DLT

- Established in May 2017 for 18 months.
- Proposed by ITU-T SG17 and supported by Korea (Republic of) with providing terms of reference
- Objectives :
  - to identify and analyse DLT-based applications and services;
  - to draw up best practices and guidance which support the implementation of those applications and services on a global scale; and
  - to propose a way forward for related standardization work in ITU-T Study Groups.
- Target :
  - FG DLT will develop a standardization roadmap for interoperable DLT-based services, taking into consideration the activities underway in ITU, other standards developing organizations, forums and groups.

FG on Application of DLT - meetings

- ITU workshop on Security Aspects of Blockchain by ITU-T SG17
  - 21 March 2017, Geneva, Switzerland
- Kickoff meeting
  - Geneva, 17-19 October 2017
  - The appointment of vice-chairman
    - based upon demonstrated competence both in technical content of the group and in the management skills required.
- The second meeting
  - 5-7 February 2018, Bern, Switzerland
- The next meeting
  - Geneva, 28-30 May 2018

FG DLT: Structure



WG1: State of the Art

- Mission:
  - Identify and introduce key elements of the DLT ecosystem (e.g., terminologies, definition, taxonomy, standardization), general concepts for DLT and related technologies, and
  - identify and analyze standardization gaps in the DLT ecosystem.
- Two deliverables
  - Terms & Definitions
  - Overview, Concepts, Ecosystem

WG2: Applications & Services

- Mission:
  - Identify and describe DLT-based use cases, specify which DLT features are required.
  - Highlight the competitive advantage brought by DLT to the use cases. Highlight how the use cases could benefit from a standardization effort.
- Deliverables
  - Horizontal Applications & Services (e.g., data usage control, identity management, security)
  - Vertical Applications & Services (e.g., telco, fintech, supply chain, energy)

WG3: Technology Reference Framework

- Mission:
  - Study architectural aspects of DLT including interoperability and abstract a high level technology reference framework.
  - Provide a mapping of existing DLT platforms on the framework, and explore criteria and methods for assessment.
- Deliverables
  - Architectural aspects and reference framework
  - Overview of existing platforms and mapping to reference framework
  - Platform assessment criteria and methods

WG4: Policy Reference Framework

- Mission:
  - Identify and describe relevant policy and regulatory dimensions (e.g., auditability, traceability, privacy, legal compliance) and
  - highlight associated constraints (e.g., GDPR, lawful intercept) to the adoption of DLT-based applications and services.
  - Provide a mapping of existing DLT platforms on the dimensions, and explore methods for assessment.
- Deliverables
  - Policy and regulatory dimensions and constraints for adoption of DLT-based applications
  - Mapping of existing DLT platforms to policy and regulatory dimensions and constraints, and assessment criteria

Contents

- Overview of Blockchain
- ITU-T SG17
- FG DLT
- FG DFC
- Conclusion

Overview of FG on DFC

- FG on DFC
  - established at May 2017 TSAG meeting.
- First kickoff FG DFC meeting
  - 12-13 October 2017
  - Beijing, China
- Second FG DFC meeting
  - 18-20 July 2018
  - New York, United States
- Digital Fiat Currency (DFC)
  - known as Central Bank issued digital currency.
  - a catalyst to accelerating interoperability in digital financial services.
  - Digital fiat currency could enable more efficient, secure and seamless interoperable services to be built within the ICT infrastructure.

Security aspects for a digital fiat currency

Gold → *Bifurcate* → **Private Bank Notes** → *Unify* → **Central Bank Currency** → *Bifurcate* → **Private e-money** → *Unify* → **Digital Fiat Currency**

Upaisa, JazzCash, easypaisa, PayPal, bitcoin, UBL Omni

Security Objects

Machine Identity Security Criteria

Identity Entity Security Criteria

Protection of Currency Security Criteria

Retail Key Management Security Criteria

Digital Security Platform Criteria

Hardware Security Module Criteria

Good Security Practices Criteria

Digital Security Interfaces Criteria

Source: ISO TC 68 SC 2

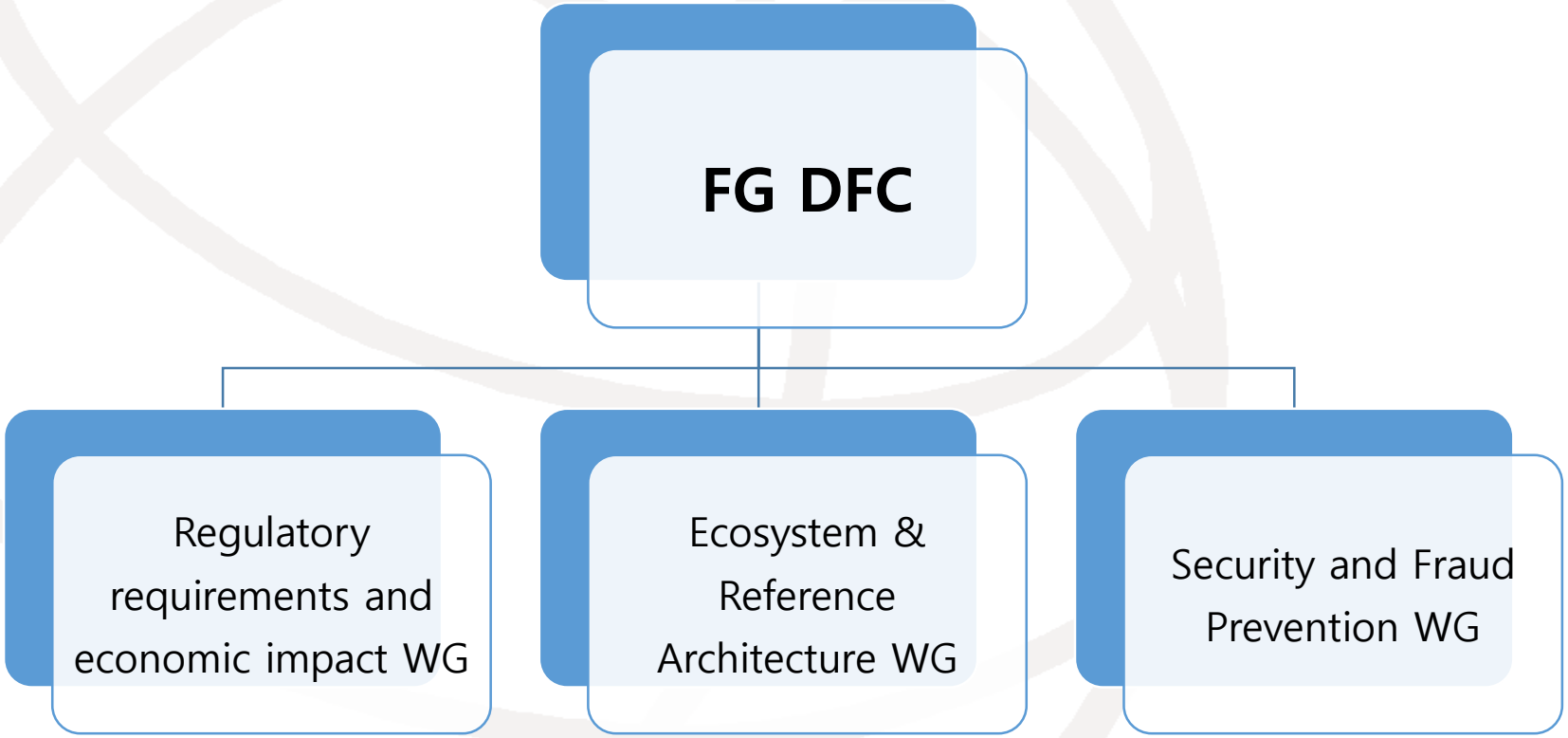
FG on DFC – Objectives (1/2)

- Study the economic benefit and impact of introducing DFC over mobile money;
- Investigate the ecosystem of digital fiat currency implementation for financial inclusion;
- Map the functional network reference architecture and process components required to implement digital fiat currency and integration with existing payment systems for interoperability;
- Identify use cases, requirements and applications of digital fiat currency;

FG on DFC – Objectives (2/2)

- Develop better understanding of the security, regulatory implications, consumer protection, fraud prevention and counterfeiting issues of DFS and how can digital fiat currency can address these concerns;
- Identify critical sovereign security, transparency and verifiability of DFC technology and provide guidelines towards the escrow of critical software and hardware components to ensure trust and verifiability; and
- Identify new areas for standardization in ITU-T study groups.

Proposed Focus Group Structure



FG DFC Deliverables

- Report on interoperability scenarios for digital fiat currency implementation.
- Develop a security architecture and reference model for implementation of digital fiat currency.
- Report on use cases for digital fiat currency and integration framework with existing payment systems for interoperability and consumer protection.
- Report on use cases for big data analytics in digital fiat currency implementation.
- Report on ICT security and governance reference model for digital fiat currency and assurance framework for compliance. Report on new areas for standardization in ITU-T study groups.
- Organize thematic workshops and events in order to collect inputs from various stakeholders.

Contents

- Overview of Blockchain
- ITU-T SG17
- FG DLT
- FG DFC
- Conclusion

Conclusion

- Blockchain enables new trust models.
- Many interesting technologies
  - Distributed computing for consensus
  - Cryptography for integrity, privacy, anonymity
- We are only at the beginning.
- Blockchain = Distributing trust over the Internet
- The APT region is invited to participate ITU-T blockchain standardization activities in ITU-T SG17, FG on DLT and FG on DFC to influence regional requirements to the deliverables & Recommendations.

References

- [1] ITU-T SG17, https://www.itu.int/en/ITU-T/studygroups/2017-2020/17/Pages/default.aspx
- [2] ITU-T SG20, https://www.itu.int/en/ITU-T/studygroups/2017-2020/20/Pages/default.aspx
- [3] FG-DLT, https://www.itu.int/en/ITU-T/focusgroups/dlt/Pages/default.aspx
- [4] FG-DFC, https://www.itu.int/en/ITU-T/focusgroups/dfc/Pages/default.aspx
- [5] ISO TC307, https://www.iso.org/committee/6266604.html

Thank you for your attention!!