SNS COLLEGE OF ENGINEERING

Kurumbapalayam (Po), Coimbatore – 641 107

An Autonomous Institution

Accredited by NBA – AICTE and Accredited by NAAC – UGC with 'A' Grade
Approved by AICTE, New Delhi & Affiliated to Anna University, Chennai

DEPARTMENT OF COMPUTER SCIENCE AND ENGINEERING

COURSE NAME: 19CS622-Blockchain Technology

III YEAR /VI SEMESTER

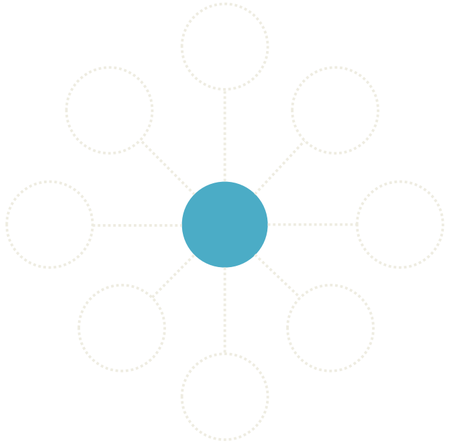
Unit 1- INTRODUCTION TO BLOCKCHAIN

Topic 3: Distributed ledger

Brain Storming

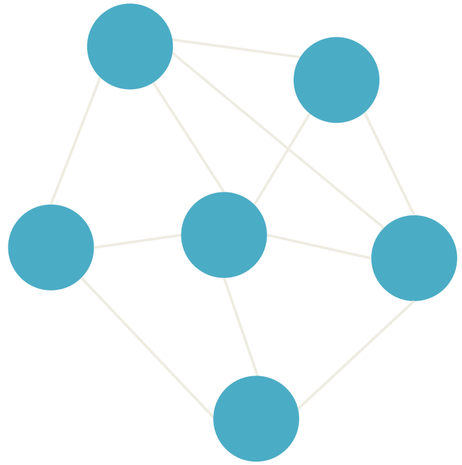
1. What Is a General Ledger ?
2. Define Distributed ledger.

General Ledger



The ledger is safe stored centrally by the service provider. Participants do not have access to the ledger.

Distributed ledger



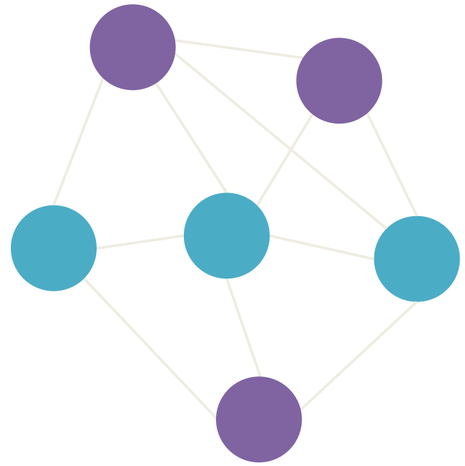
Every participant in a service has a copy or can have access to a copy of the ledger supporting this service, which gets updated throughout the day. It has no central server.

Distributed Ledgers - Architecture

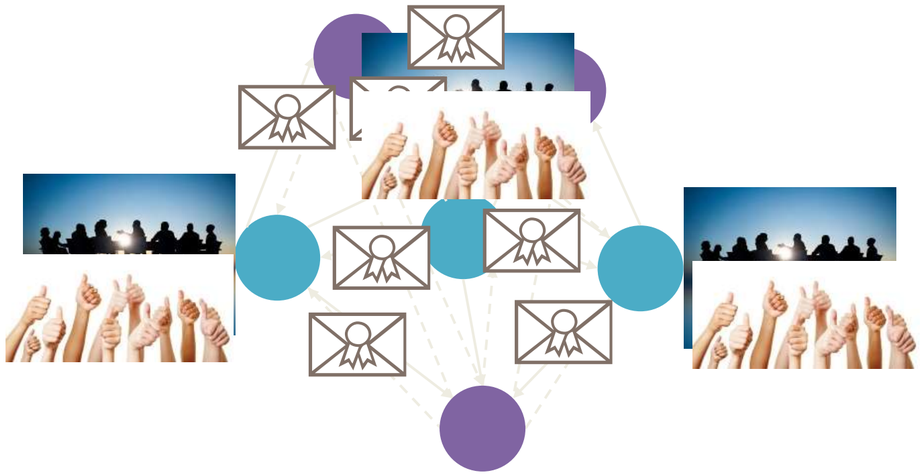
- Distributed Ledgers are designed as a peer-to-peer distributed system composed by a number of nodes. Each node propagates transactions and ledger updates to all other nodes and fulfils one or more of the below roles:

Participant: responsible for transactions input. Depending on the implementation, have the option to either store the full copy of the ledger or not. Wallet in Bitcoin terminology.

Validator: Verify transactions and update the ledger. Miner in Bitcoin terminology.



Distributed Ledgers – How does it work?



1. Transactions are broadcasted to all nodes by participants
2. Validators verify all transactions and reach a consensus amongst themselves on what transactions to include in the ledger. Various consensus methods exist (e.g. Proof of Work for Bitcoin)
3. Once consensus is reached new set of transactions is included in the ledger by all participants

Participants

Validators

What can be exchanged

On-platform assets *(e.g. digital currency)*

Off-platform assets reference *(e.g. Fiat currency, securities, anything!)*

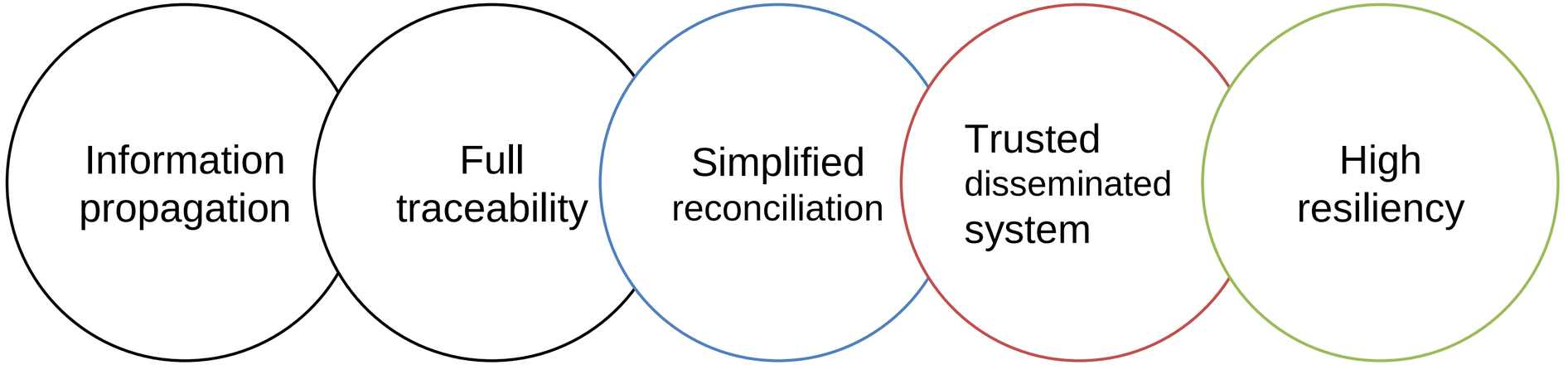
Obligations and rights contracts (maybe “smart”) and agreements *(e.g. real estate ownership, derivatives)*

Public versus permissioned ledgers

- Public Ledger : anyone, without permission, may submit and validate transactions (eg, bitcoin)
- Permissioned Ledger : only known and trusted actors may submit and/or validate transactions

- Permissioned how?
  - Validation by consensus, not proof-of-work
  - Validators chosen by contract, reputation, organization
  - Faster, more efficient than proof-of-work
  - Faster (but less secure) than POW algorithm
  - Requires high level of trust between participants

Why: Key strengths of DLTs



Information propagation – Efficient means of keeping a full network up to date with latest information

Full traceability – Participants are able to trace information flows back through the entire chain

Simplified reconciliation – Local access to complete and verified data easing reconciliation processes

Trusted disseminated system – Ability to trust authenticity of data on the ledger without recourse to a central body

High resiliency – Operates seamlessly and removes dependency on a central infrastructure for service availability

What business problems can permissioned DLT solve in the securities industry?

- Paper intensive process streamlining, eg syndicated loans, bonds, etc.
- Real-time DVP settlement
- Consistent ref data real-time distribution
- Remove the need for data reconciliation
- Perfect audit trail of transactions from first to last
- Beneficial ownership real-time registration
- Regulatory trade reporting mandate support
- Equity issuance, trading and settlement for small cap issuers
- Etc, Etc, Etc…

Applying DLTs in the financial services industry: requirements

Strong governance – Governance models with clearly defined roles and responsibilities of parties, business and operating rules.

Data Controls – Controlled data access and availability to preserve data confidentiality.

Compliance with regulatory requirements – Ability to comply with regulatory requirements (e.g. Sanctions, KYC, etc.).

Standardisation – Standardisation at all levels to guarantee straight-through processing (STP), interoperability and backward compatibility.

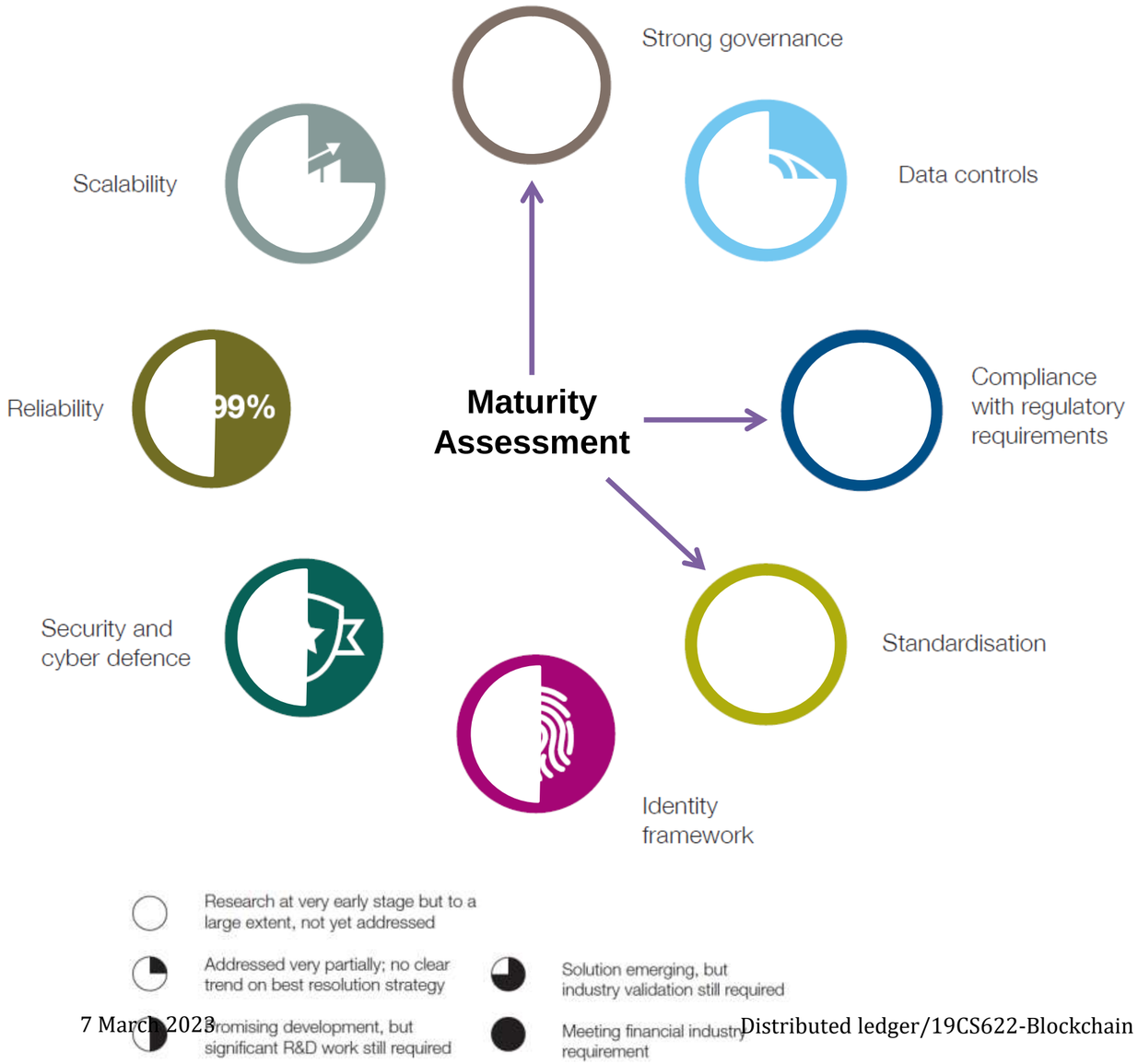
Identity framework – Ability to identify parties involved to ensure accountability and non-repudiation of financial transactions.

Security and cyber defense – Ability to detect, prevent and resist cyberattacks growing in number and sophistication.

Reliability – Readiness to support mission-critical financial services.

Scalability – Readiness to scale to support services which process hundreds or thousands of transactions per second.

Why not: DLT maturity, more R&D needed



Strong governance – Role of centralized governance versus open-source models needs to be investigated further.

Data Controls – Work required to better define what kind of data must reside in the ledger and be distributed.

Compliance with regulatory requirements – R&D related to regulatory compliance in a distributed ledger environment will need to come from both the industry and regulatory bodies.

Standardisation – Fundamental questions to be addressed (DLT standard or interoperability, ISO 20022 re-use, interoperability with legacy, smart contract standardisation).

Identity framework – Key management, both in terms of issuance/identity and recovery, requires close examination.

Security and cyber defense – More work required to allow for partial or complete data protection on the ledger through the use of encryption or selective distribution.

Reliability – Needed definition of the right software management and release policy principles in distributed environment, in line with best practice of the industry such as ITIL.

Scalability – R&D to be carried out to assess available consensus algorithms and validation methods against realistic and representative business throughput requirements.

DLT is not messaging...

…but we can benefit from shared business content

ISO 20022 as a messaging standard

The logical message layer references the business layer for semantic definitions

Business / Conceptual

- Defines financial concepts, e.g., ‘Credit Transfer’ and business processes

Logical

- Defines e.g. credit transfer messages, to serve the business process

Physical

- Defines physical syntax, e.g. XML

Shared business definitions

***Imagine*:**
Standards for DL

The logical DL implementation re-uses business concepts to ensure interoperability with messaging

Business / Conceptual

- Defines financial concepts, e.g., ‘Credit Transfer’ and business processes

Logical

- A ‘logical’ implementation’ – defines data and behaviour based on new paradigm assumptions

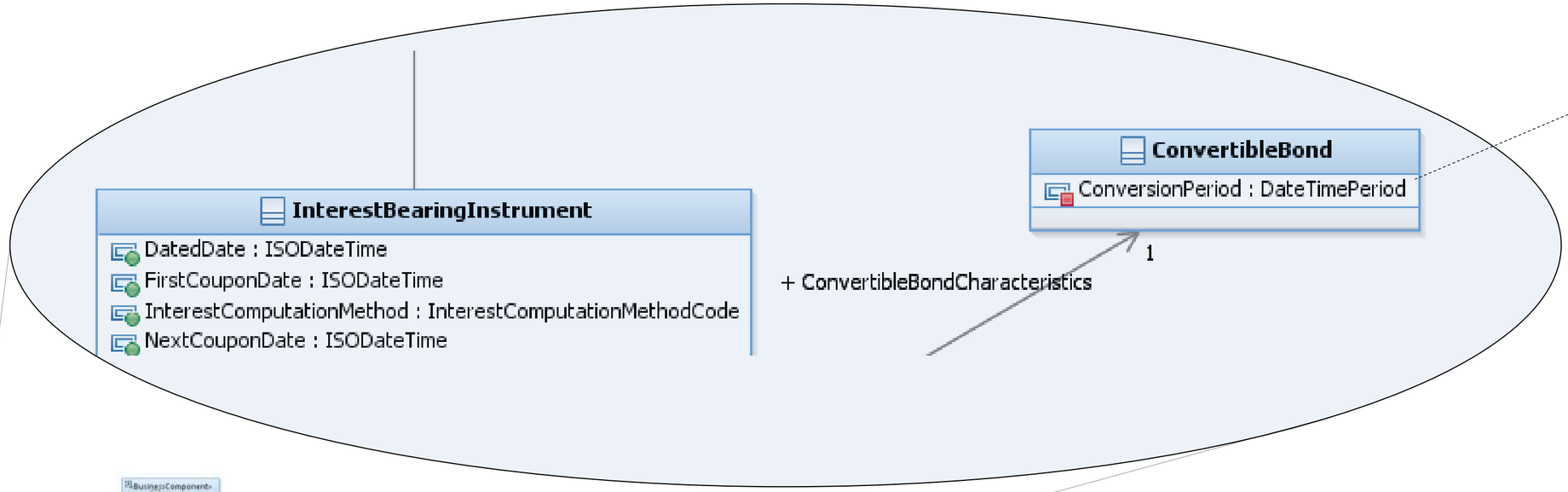
Physical

- A physical implementation using e.g. Hyperledger, Ethereum

Re-use of business model content

Bonds

Business / Conceptual

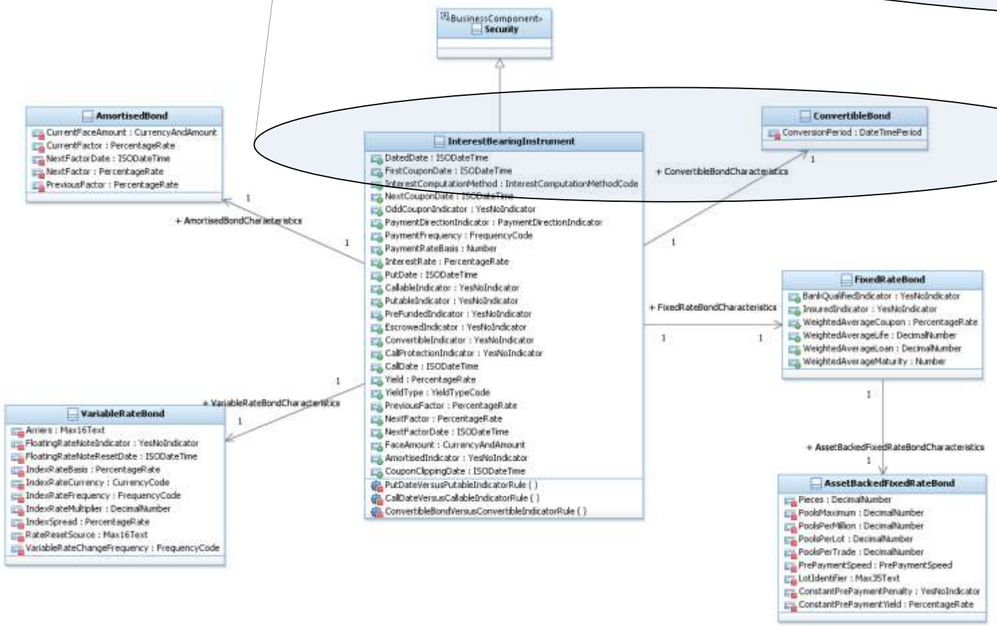


ISO 20022 Definition

ConversionPeriod

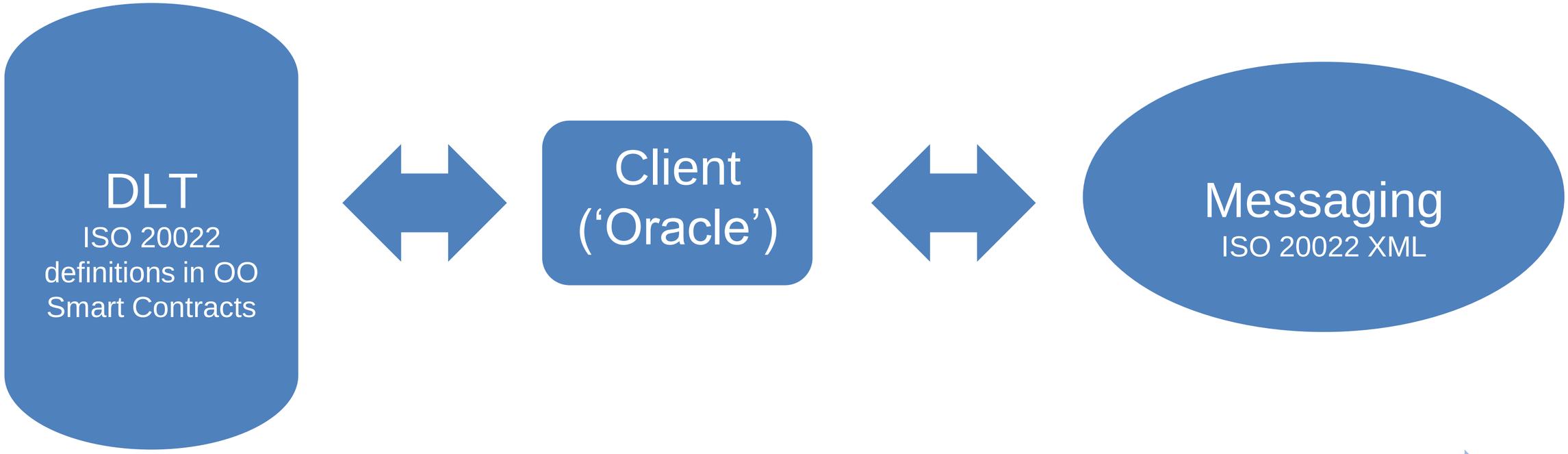
Period during which a convertible security may be converted according to the terms of the issue.

DateTimePeriod is ISO data-type



ISO 20022 also captures *behaviour* in message flow diagrams which can be used to inform design of smart contracts – e.g. for coupon payments

Interoperability



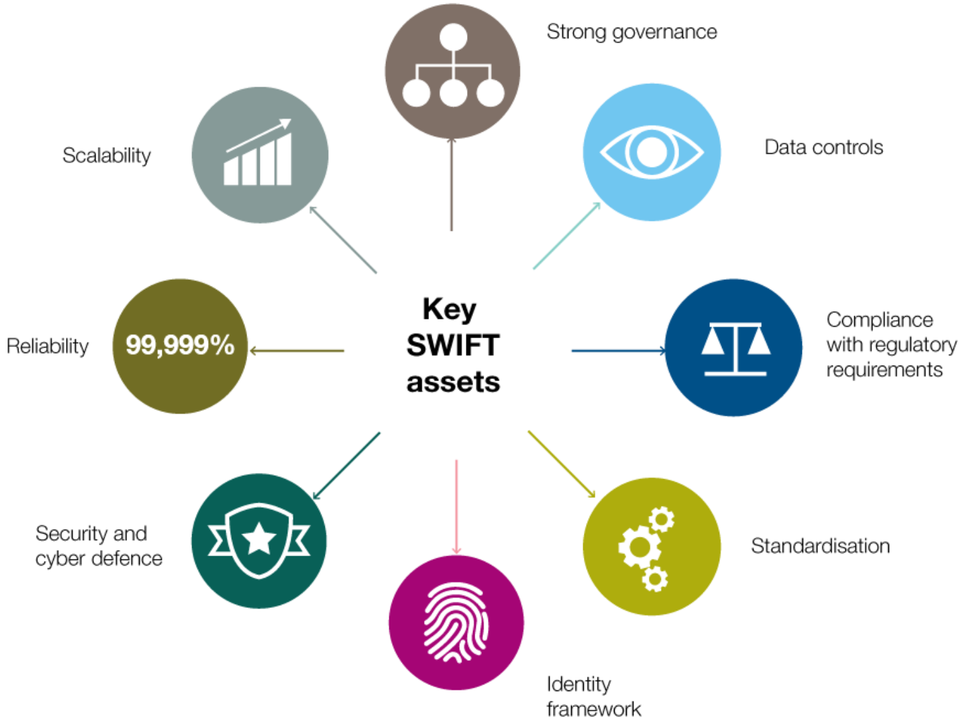
ISO 20022 *definitions* end-to-end

Distributed Ledger – SWIFT position

- SWIFT's focus is on building technical, operational and business capabilities with a view **to evolving our platform** such that DLT-based services could be offered to our 11,000+ members, **when the technology matures** and firm **business use cases emerge**.

- SWIFT have been **delivering solutions to the financial services industry for 40+ years**, building out industry trusted infrastructure and services

- We will leverage our **unique set of assets and capabilities** around strong governance, deep standards expertise, operational efficiency, security, reliability, and reach to deliver a distinctive DLT platform offer for the benefit of its community.



Assessment 1

1. A blockchain provides

Ans : _____

2. Basic application:

Current largest:

Ans : _____

References

TEXT BOOKS

1. Mastering Bitcoin: Unlocking Digital Cryptocurrencies, by Andreas M Antonopoulos 2018
2. Imran Bashir, “Mastering Blockchain: Distributed Ledger Technology, Decentralization and Smart Contracts Explained”, Second Edition, Packt Publishing, 2018.
3. https://101blockchains.com/blockchain-vs-database-the-difference/

REFERENCES

1. William Mougayar, “Business Blockchain Promise, Practice and Application of the Next Internet Technology, John Wiley & Sons 2016.
2. Josh Thompson, ‘Blockchain: The Blockchain for Beginnings, Guild to Blockchain Technology and Blockchain Programming’, Create Space Independent Publishing Platform, 2017.
3. Arvind Narayanan, “Bitcoin and Cryptocurrency Technologies: A Comprehensive Introduction”, Princeton University Press, July 19, 2016.
4. Henning Diedrich, Ethereum: Block chains, Digital Assets, Smart Contracts, Decentralized Autonomous Organizations-2016

Thank You