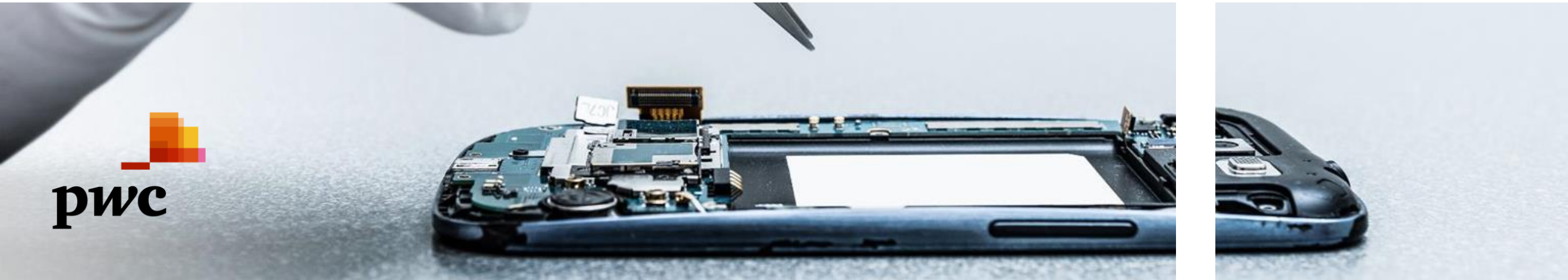
Blockchain & Smart Contracts

Presentation by **Paul Kayrouz**



Agenda

1

Evolution of Finance & Blockchain

Blockchain: A simple definition

A Distributed Ledger Technology (DLT) shared across private or public network. The Network is visible to all nodes (end users) who hold a LIVE copy of the Ledger.

The Blockchain is a continuously growing set of blocks which contain information cryptographically stored/encrypted that form a chain – Thus, the name Blockchain.

Blocks are added to the historical chain after consensus protocols validate the transaction. And since all information is timestamped on the ledger, double entries or fraud are thus made virtually impossible.

A Blockchain can be programmed by algorithms as referred to as 'Smart Contracts' that execute transactions on the ledger once a specific set of conditions are met.

Given its transparent nature, a blockchain network has no central authority – Hence the birth of 'Decentralised' and 'Democratised' systems.

Blockchain Key principles

Decentralisation
No centralised authority controls the network.

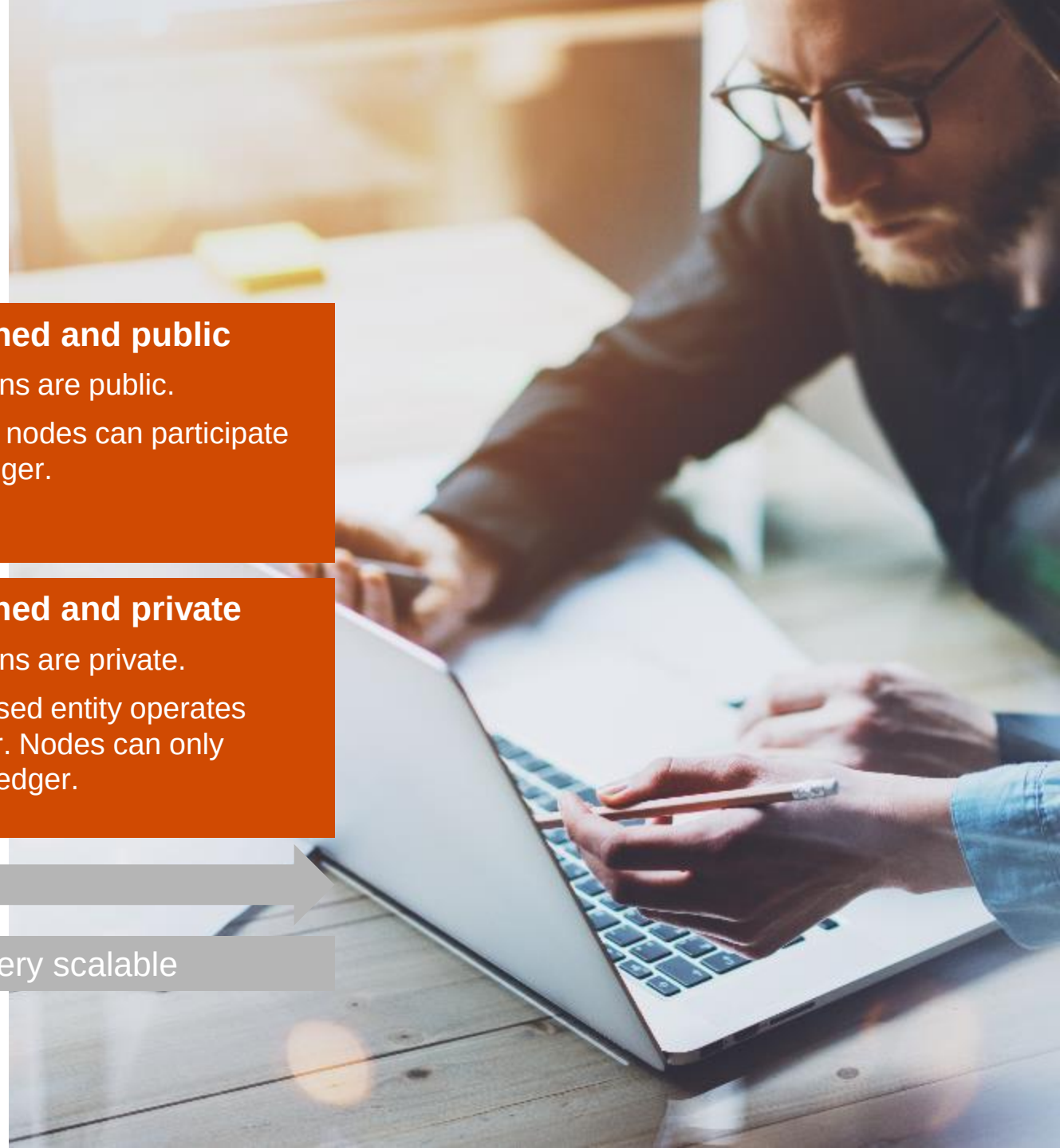
Transparency
The ledger is visible to all nodes and historically trackable.

Security
Data is cryptographically encrypted.

Immutability
Information is timestamped, thus cannot be tampered with.

No third party involvement

Blockchain Types/Forms



Public

Private

Permissionless and public

- Blockchains are public.
- Any node can participate to add blocks or verify a transaction.

Permissioned and public

- Blockchains are public.
- Permitted nodes can participate on the ledger.

Permissionless and private

- Blockchains are private.
- A centralised entity permits nodes to participate in the ledger.

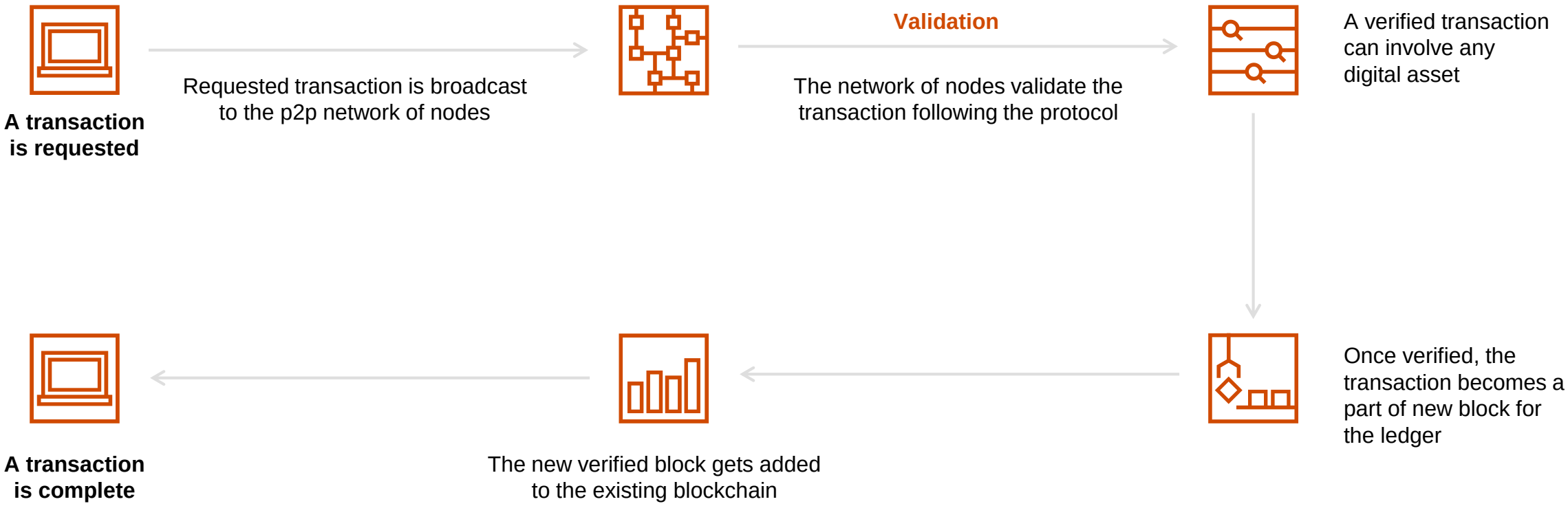
Permissioned and private

- Blockchains are private.
- A centralised entity operates the ledger. Nodes can only view the ledger.

Little scalable

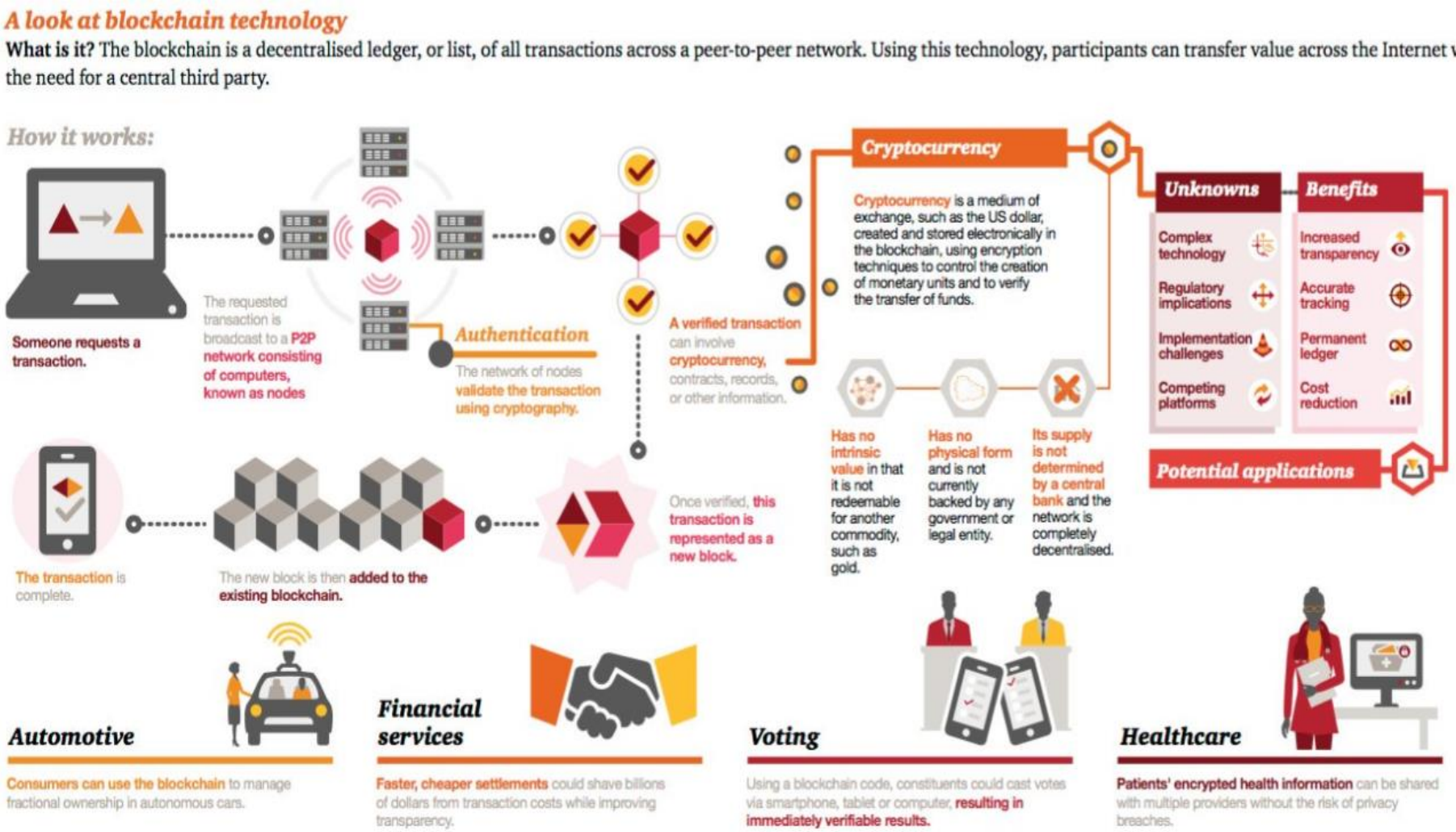
Very scalable

Blockchain: Illustrative example



Source: https://www.edureka.co/blog/blockchain-technologyar

A look at Blockchain Technology



Why Blockchain vs. Other Solutions?

Legacy Ecosystem	Blockchain Ecosystem
- Ability to automate, create, populate, and certify certain low risk reconciliations - Ability to automate daily data matching, exception management, and period-end balancing with internal controls and audit trail	- Data matching between systems will no longer be needed as transaction posted on shared ledger is immutable and consistent shared across all systems - GL to Sub-ledger reconciliations will still be needed. Account reconciliations are performed on balance sheet accounts, whereas blockchain will be driven by transactions
- Automated internal and external reporting tools	- Reporting tools will still be needed to create the reports, however data used in reporting will be enhanced as the transactional data is from one single source vs. multiple sources containing potential conflicting information
- Close workflow integration across systems & manual processes	- Workflow tools will still be needed to automate and manage the close process, however, fewer steps may be needed to close due to level of comfort over quality of data and fewer reconciliations needed
- Delivers global data collection, financial consolidation, reporting and analysis in a single solution	- Consolidation and reporting tools will still be needed to perform consolidation and elimination steps, however, fewer reconciliations and out of balance entities as due to shared ledger
- Automates and streamlines planning, budgeting, forecasting, and consolidation activities	- Planning tools will still be needed for budgeting and forecasting, however data from shared ledger can be used to enhance the quality of the forecasts for better planning and quicker management decisions

In-house blockchain-as-a-service (BaaS) offerings

Early Adopters – Highly Developed

Microsoft Azure

November 9 , 2015: Microsoft announces development of **Blockchain as a Service** on the Azure platform

IBM

December 17, 2015: **IBM** announces it will be leading member of Linux foundation, the origination of the **Hyperledger Project**

amazon web services

May 3, 2016: **Amazon** announces **Blockchain as a Service Sandbox** for Developers

pwc

Recent Adopters – Minimally Developed

SAP Leonardo

May 16, 2017 – SAP announces a **BaaS offering** within its new SAO Leonardo SAP digital innovation tool. The tool is classified as having "early-stage blockchain capabilities."

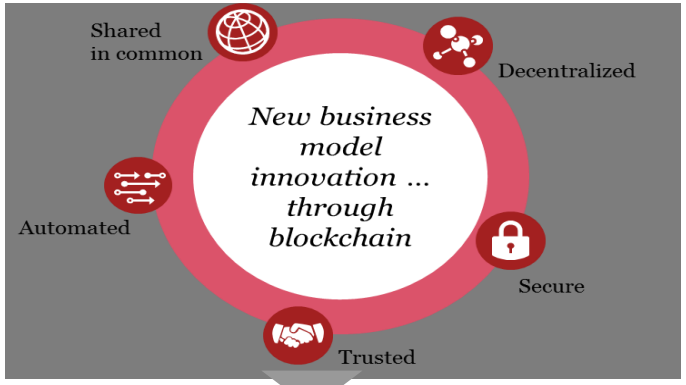
ORACLE

October 2, 2017 – Oracle announces the **"Oracle Blockchain Cloud Service,"** a BaaS offering integrated into the Oracle Cloud Platform

workday.

No announcements have been made by Workday in regards to blockchain technology as of October 2017

Effective Blockchain journey starts with identifying high impact areas for application



- **Define goals and success factors**
- **Confirm use case(s) for proof of concept (POC)**
- **Determine which product/customer segment offers the highest value to support POC validation**

- Engage selected channel partners for partnership and innovation piloting
- Evaluate platforms / blockchain technology vendors to the vision, capabilities and requirements
- Confirm blockchain vendor partnership arrangements

- Conduct technology experimentation in sandbox environment (iterative)
- Coordinate with selected channel partners on specific data sets required for simulation
- Confirm channel partner arrangements

- Configure/build logic and rules based on use case(s)
- Initiate mock-simulations
- Make adjustments to configuration and logic and refine data sets as necessary (iterative)

- Gather transaction metrics
- Assess key learnings
- Confirm business case for expansion

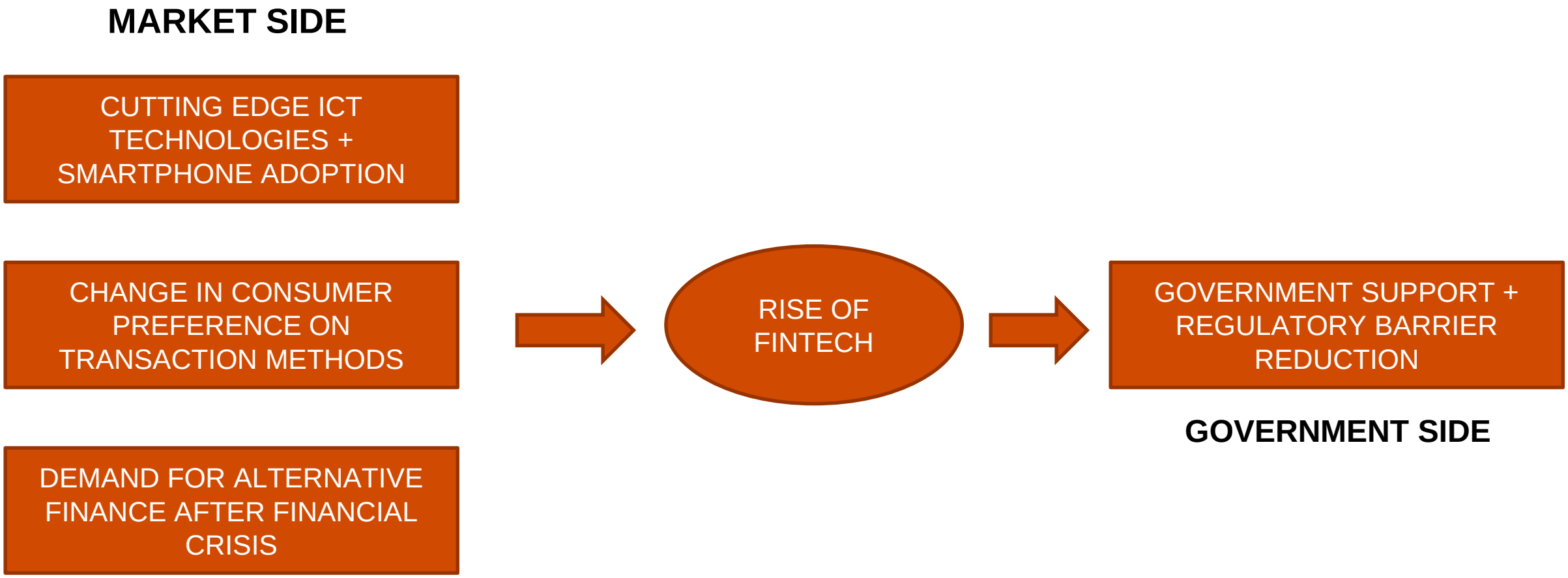
Establish action plan and finalize business case for moving forward on blockchain expansion, adoption, and implementation

Security issues with Blockchain

- Although Blockchain technology provides transaction security (by protecting data stored in the Blockchain ledger against tampering), it does not provide individual wallet or account security.
- Individual wallets or accounts remain susceptible to risks (e.g. stealing private keys)
- In addition, a malicious actor theoretically could take over more than 50% of network participant nodes, which in turn creates cybersecurity risks and threats to the larger Blockchain.
- Other risks include data confidentiality concerns; network participants will always have access to some of the metadata which in turn can reveal information about the type of activity and volume associated with the activity (although personal data is not revealed).

Drivers of financial innovation

Fintech's emergence



Fintech universe

2

Smart Contracts

What is a Smart Contract?

- A smart contract is ‘’a set of promises specified in digital form, including protocols within which the parties perform on these promises’’(Nick Szabo)
- Think of a vending machine, when money is paid the transaction cannot be stopped.
- According to Szabo, **Smart Contracts has 4 characteristics**:

  (a) Digital form: it is in a computer form (code data);

  (b) Embedded: contractual clauses are embedded as computer code in software;

  (c) Perfomance mediated by technological means; and

  (d) Irrevocable: once initiated cannot be stopped
- In an easier way, Smart Contracts are contracts **whose terms are encoded in computer language** instead of legal language. The terms of the smart contracts are **automatically enforced by a protocol that all nodes in the network follow**
- A Smart Contract **can be fully autonomous if all the objects** referred (such as currency, payments obligations, property titles, assets, licenses) **have a digital representation in the platform**

Smart Contracts Ecosystem

Current Status

A current language contract but with certain functions encoded in digital form e.g. payments or even entirely automated schedule such as Service Levels

At present, Smart Contracts carry out what they are programmed to do. They do not think independently or provide reasoned analysis and do not address ‘’grey areas’’ or contain the flexibility that parties will frequently expect from certain kinds of contracts

Example

E.g. In a typical procurement agreement, the supplier may offer the customer the benefit of an indemnity for defective products. Indemnity in such a contract would be difficult to encode as it would operate when a certain event happens, but the scope of the indemnity will be likely be subject to individual facts in question.

The **challenge** at the moment is connecting matters

Future Status

A contract entirely in code that dispenses with the natural language contract. This contract would be a piece of code that is legally recognized and enforceable on a standalone basis

Permissioned VS. Permissionless ledger?

- **Permissionless:** Anyone is free to download the software, submit messages for processing and/or be involved in the process of authentication, verification and reaching consensus.
- **Permissioned (or sometimes referred to as Private):** Participants are pre-selected or subject to pre-approval entry on satisfaction of certain requirements such as KYC/AML or on approval by an administrator of the distributed ledger.
- **Hybrid systems:** these systems relate to the degree of centralization that those responsible for setting up a distributed ledger wish to achieve. For example, anyone can download the requisite software and inspect the raw data but no one-except those with the required cryptographic key could inspect individual messages or transactions.

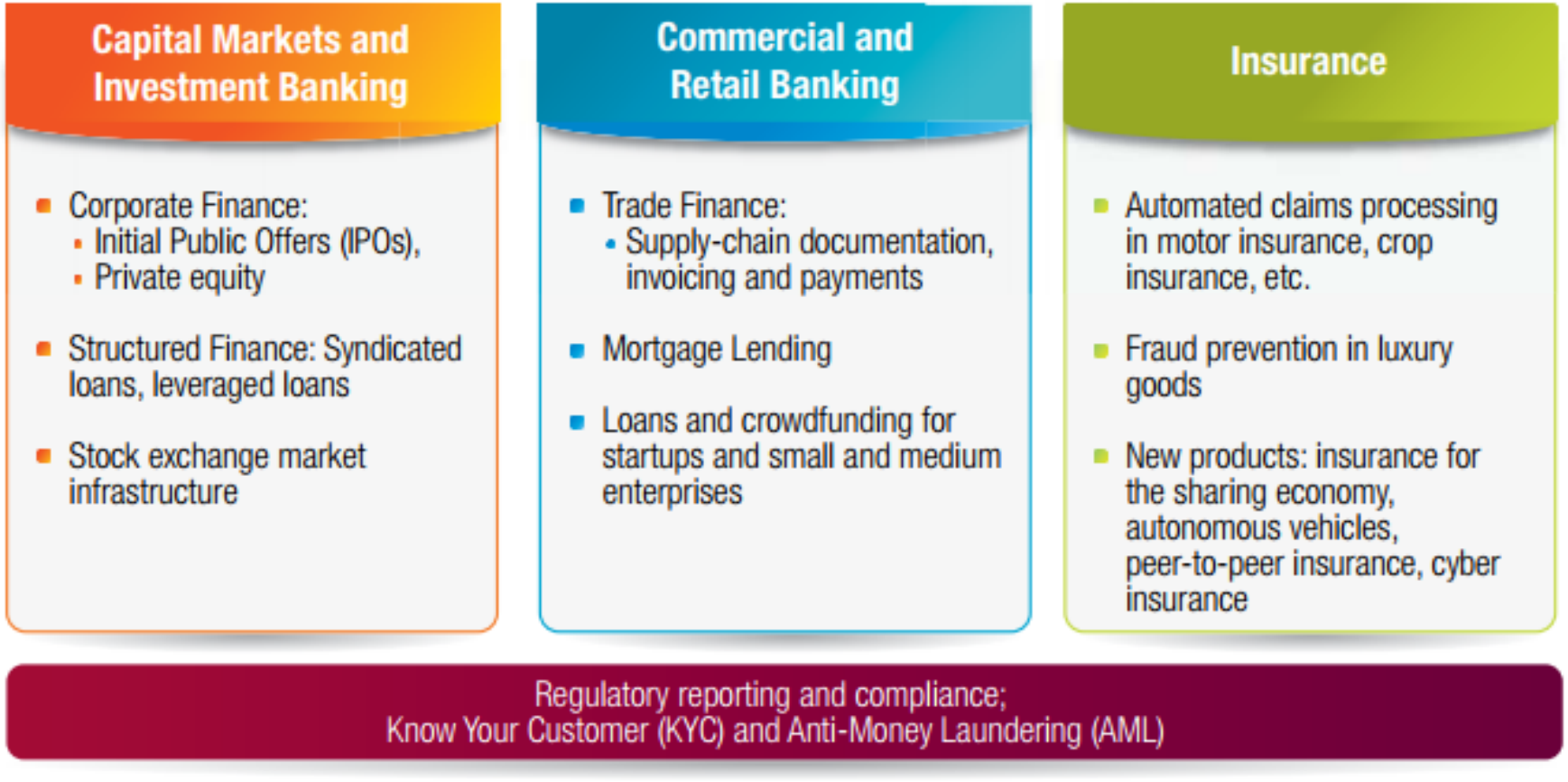
Consensus Mechanisms

- **Proof of work (Bitcoin):** works by having all miners solve a mathematical puzzles; the fist one to solve the formula will get rewarded. The problem is that PoW consumers a lot of electricity thus miners are coming together into mining tools; meaning Blockchain has become more centralized
- **Proof of Stake (e.g. Ethereum):** No need for everyone to compete together. No miners but validators who are chosen randomly. Validators have to stake their coin (think of it as a guarantee); it is a linear correlation meaning the system favors the rich. How to trust other validators= they lose their stake if they approve fraudulent transactions. Remember the stake should be higher than the transactions fees.

What is the 51% attack?

- Flaws with PoW : If I buy majority of Stakes in a Network then I control it and effect a fraud transaction. (you need 51%)
- Proof of Stake: makes the 51% less likely to happen

Application of Smart Contracts



Source: Capgemini Consulting Analysis

Practical Examples of Smart Contracts

(1) Securities and financial instrument clearing and settlement (financial services)

(2) Insurance claim processing (financial services)

(3) Electronic patient records (healthcare)

(4) Royalty distribution (music and media)

3 Perspectives for Smart Contracts

1. At the **developer level**

2. At the **platform developer or platform operator:** the agreement is a software ‘‘design, build and operate’’ agreement with elements of software licensing or transfer and/or service provision

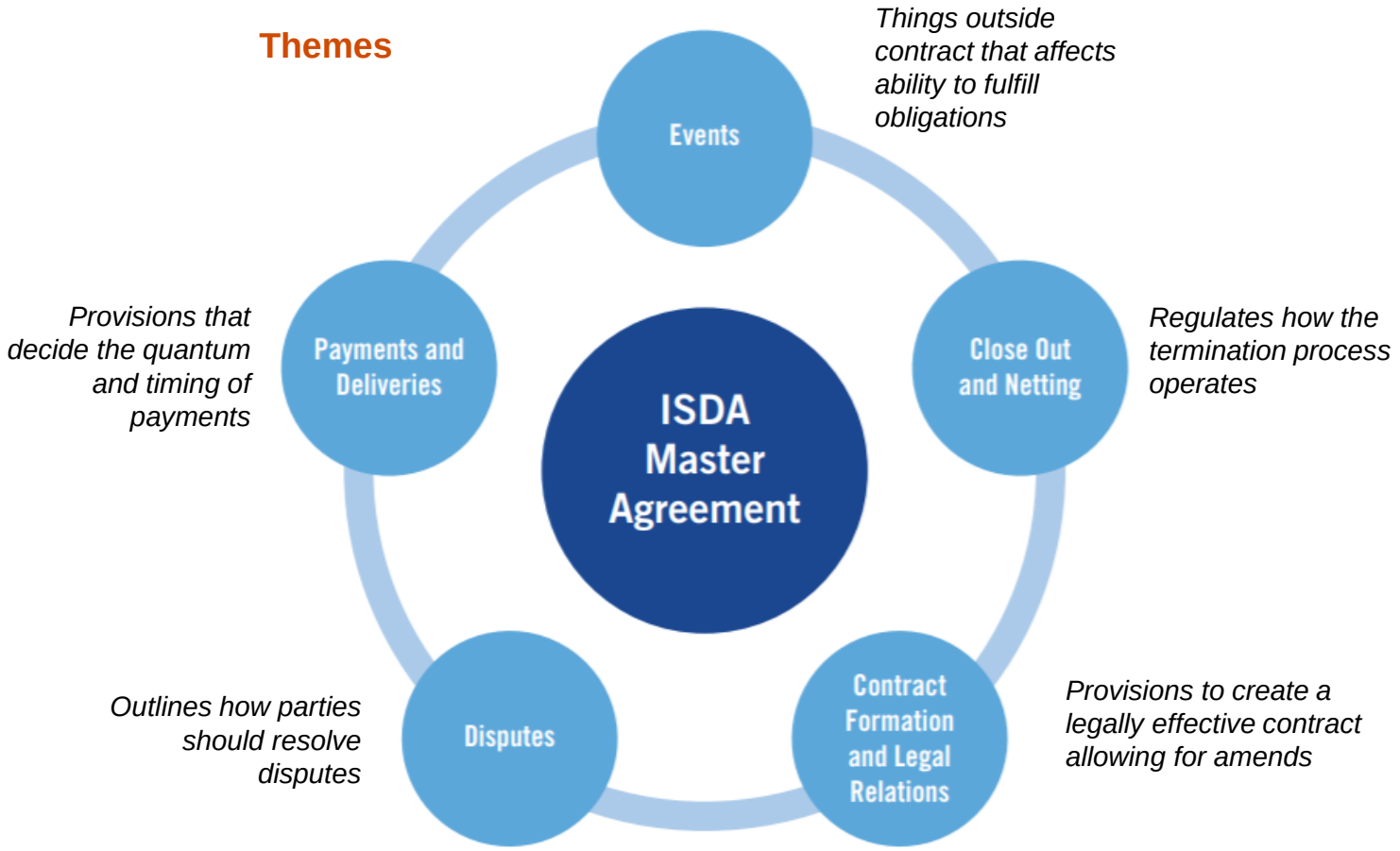
3. At the **platform operator or user contract level:** think of stock exchanges and other trading venues which have detailed membership agreements, contractually binding operational rules and a range of data licensing and system use

Case Study: ISDA Master Agreement

Background

- Standard contract used to govern all over-the-counter (OTC) derivatives transactions
- Transactions across different asset classes and products are often documented under the same agreement

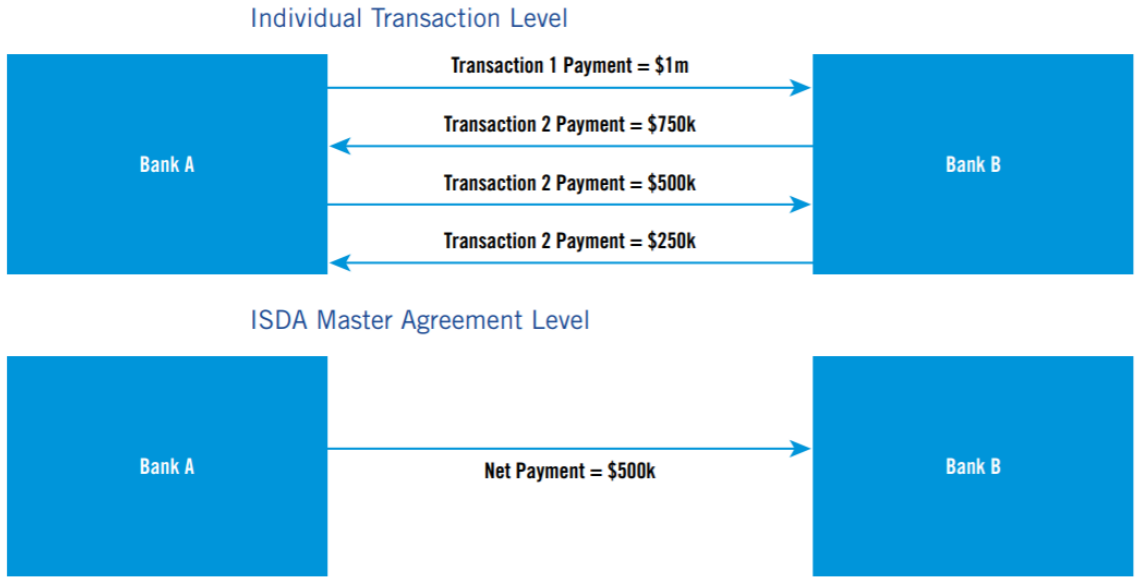
Themes



Source: ISDA Legal Guidelines For Smart Derivatives Contracts: The ISDA Master Agreement, Page 4

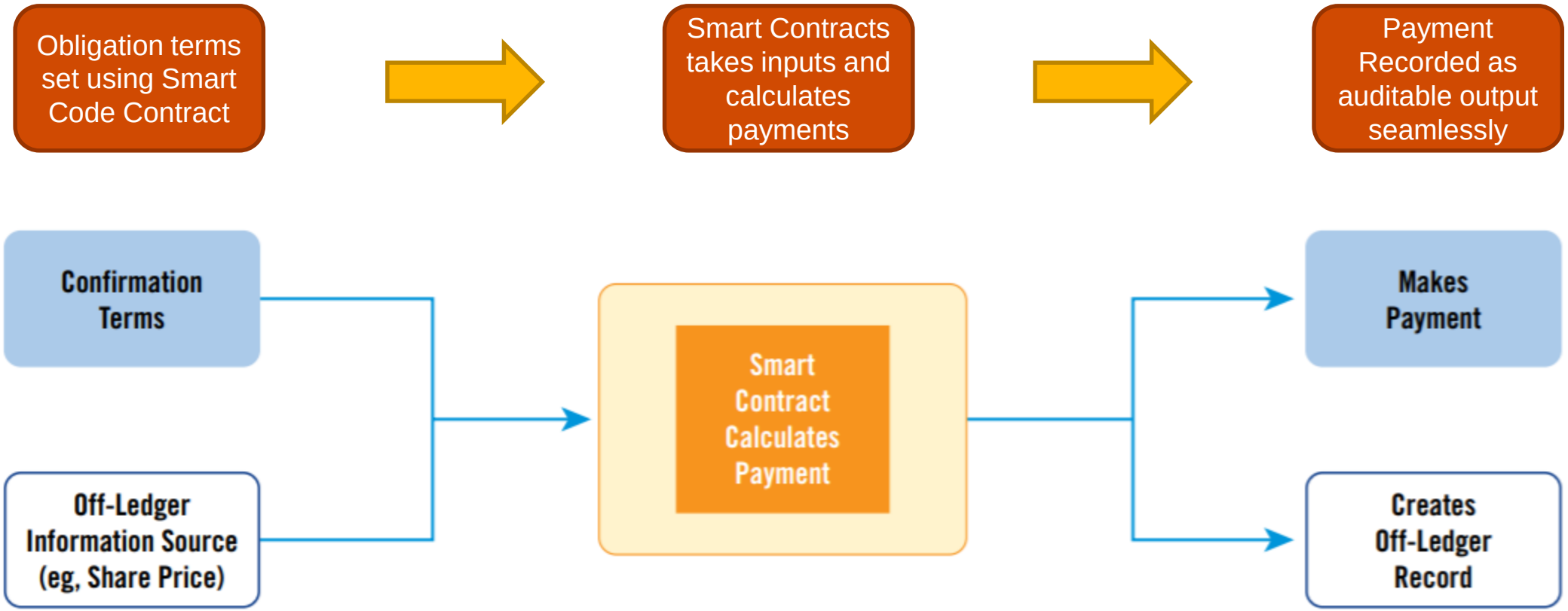
Use Case 1: Payment Netting

Traditional Contracts	ISDA Master Agreement
× Separate and distinct contracts	✓ Incorporated by reference into a single agreement
× No interdependency among contracts	✓ Interdependency among the various documents
× Payments made over several transactions	✓ Ability to net payment across multiple transactions



Source: ISDA Legal Guidelines For Smart Derivatives Contracts: The ISDA Master Agreement, Page 19

Use Case 2: Transaction Automation



Source: ISDA Legal Guidelines For Smart Derivatives Contracts: The ISDA Master Agreement, Page 22

How Courts Will Enforce Smart Contracts?

How Courts Will Enforce Smart Contracts?

- Compare Smart Contracts to Shrinkwrap and Clickwrap cases
- US courts for example have considered Clickwrap agreements to be enforceable recognizing that parties do not have to negotiate every term
- Clickwrap agreements are one that are formed over the internet typically when a website posts terms and conditions to which user clicks an ‘’I accept’’ button.

Potential Enforcement Problems

- No central administering authority to decide a dispute between participants to a smart contract;
- Difficulties in proving the existence of a smart contract in court proceedings where evidence exists only in electronic format on a distributed ledger;
- No obvious defendant; for example who would be responsible for system operational defects, corrupted messages, or defective programme logic that led to non-performance (or unexpected performance) of a smart contract.

Regulatory Challenges

Key regulatory challenges of smart contracts

- Currently, the regulatory focus in the cyberspace is on intermediaries such as telecom companies and internet service providers (ISP) such as Google, Microsoft etc.
- By regulating the intermediaries the regulators are indirectly regulating the end user i.e. consumer of the service/product
- This will be different with Decentralized ledger Technologies such as Blockchain as technically there are no intermediaries
- Big question: how will regulations apply to decentralization?

Key Questions

- Some people say regulations will not apply to Smart Contracts because of their decentralization nature
- Can regulations apply to code/software developers instead of traditional intermediaries?
- What about regulating end- users? E.g. Binary options: Binary options are required to be listed in the US according to the CFTC
- Who will responsible for not listing Binary Options? Code developers?