ECOM6023

eFinancial Services

LECTURE 9:
Blockchain and Crypto Currencies

Dr. Juergen Rahmel 2020-21

HSBC Germany / Hong Kong
IETC Information Engineering – Teaching and Coaching Ltd.

L9 – Blockchain and Crypto-CCY

Topics

- Bitcoin and other Crypto Currencies
- Blockchain basics
- Smart Contracts

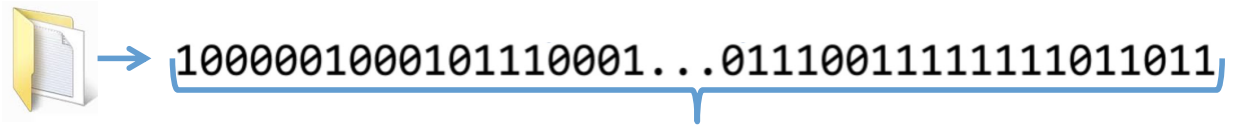
L9 – Blockchain and Crypto-CCY

Bitcoin – the underlying Cryptography

Prerequisite #1: hashing algorithms

one-way calculation of a Bit-string of any length into a Bit-string of a given length, i.e.

$h: \quad \Sigma^* \rightarrow \Sigma^n \qquad \Sigma = \{0, 1\}$



with the following properties:

- h must be efficiently computable
- similar texts should result in completely different hash values (pseudo randomization)
- there is no efficient way to calculate the preimage of h, i.e. generate the original text from the hash value
- the function must be collision free, i.e. no two texts can be efficiently found with same hash value

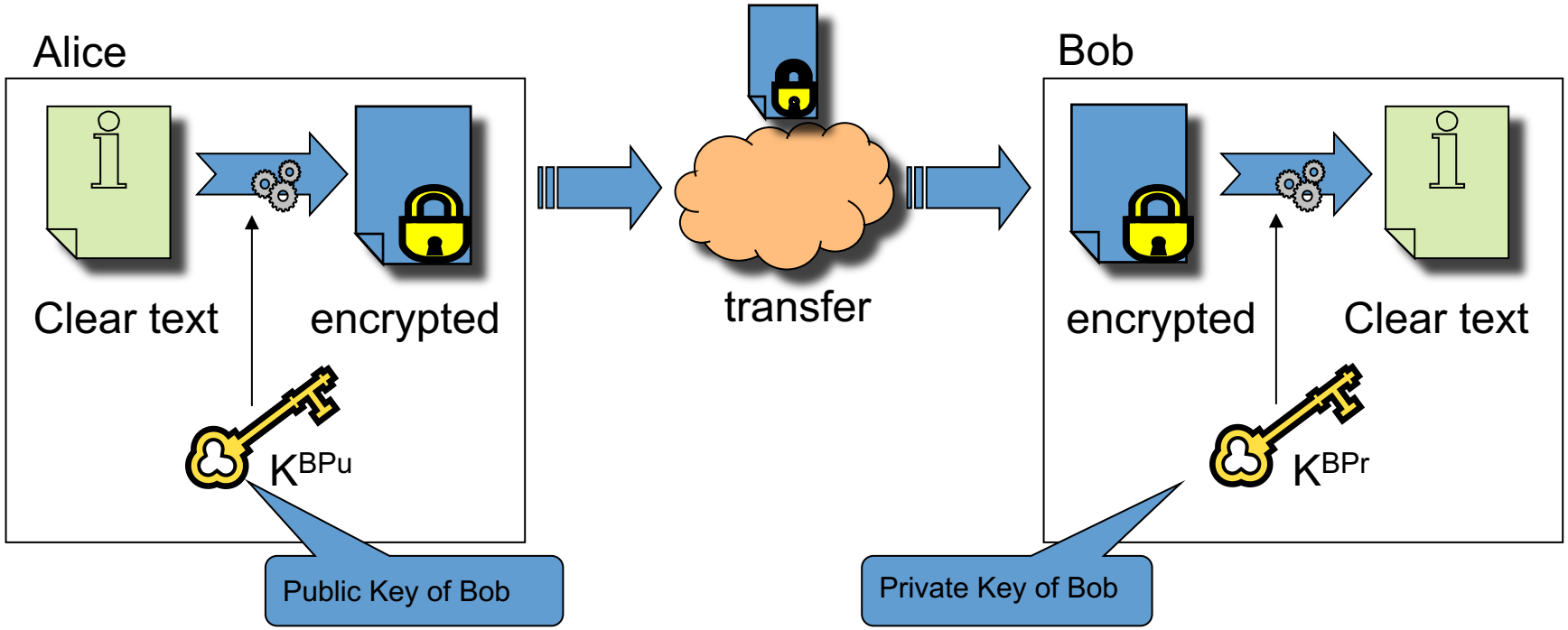
L9 – Blockchain and Crypto-CCY

Bitcoin – the underlying Cryptography

Prerequisite #2: private and public key algorithms

participants each have their own Key pairs, consisting of a public and a private Key.

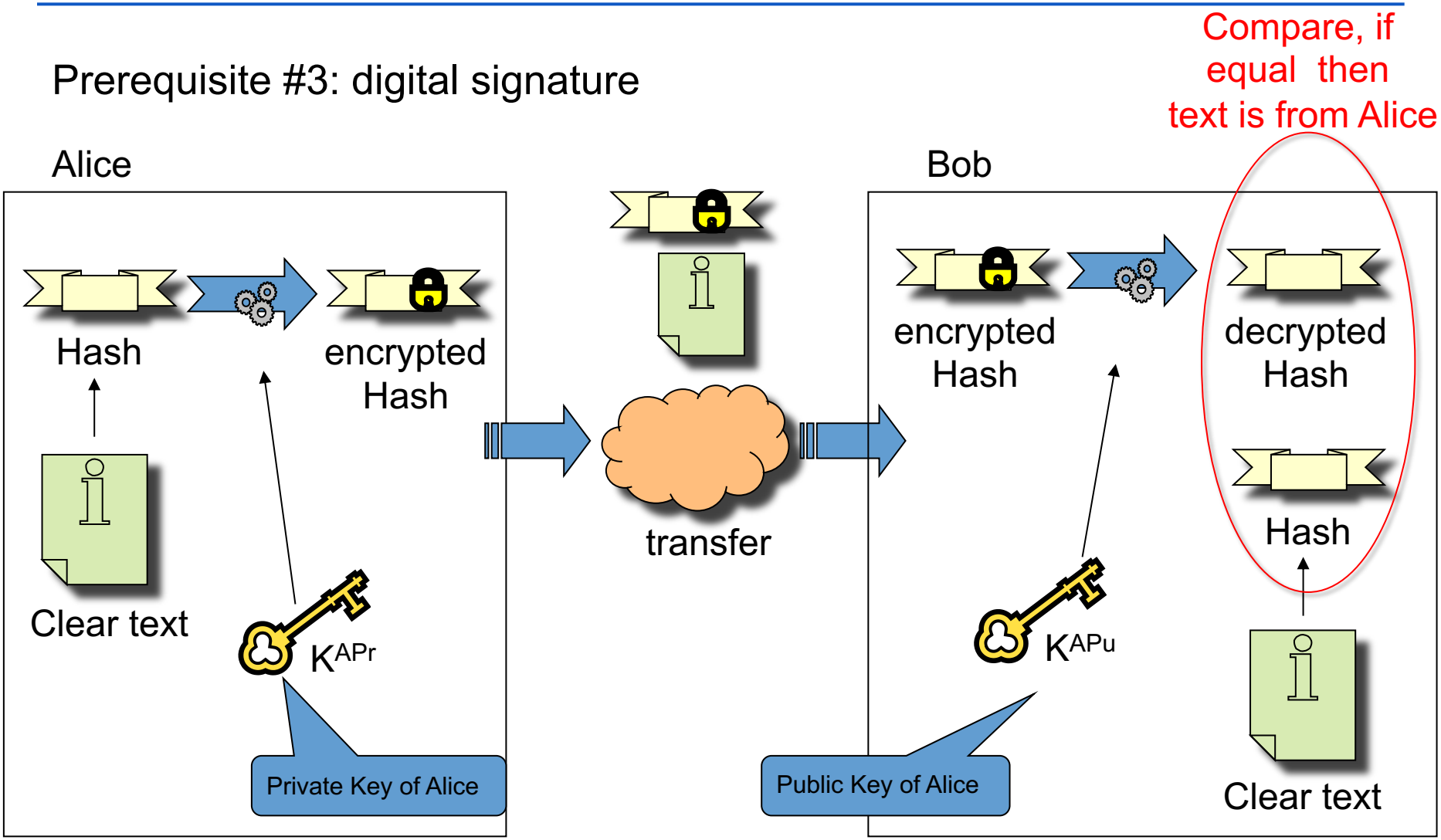
The private key is never shared, the public key can be distributed



L9 – Blockchain and Crypto-CCY

Bitcoin – the underlying Cryptography

Prerequisite #3: digital signature

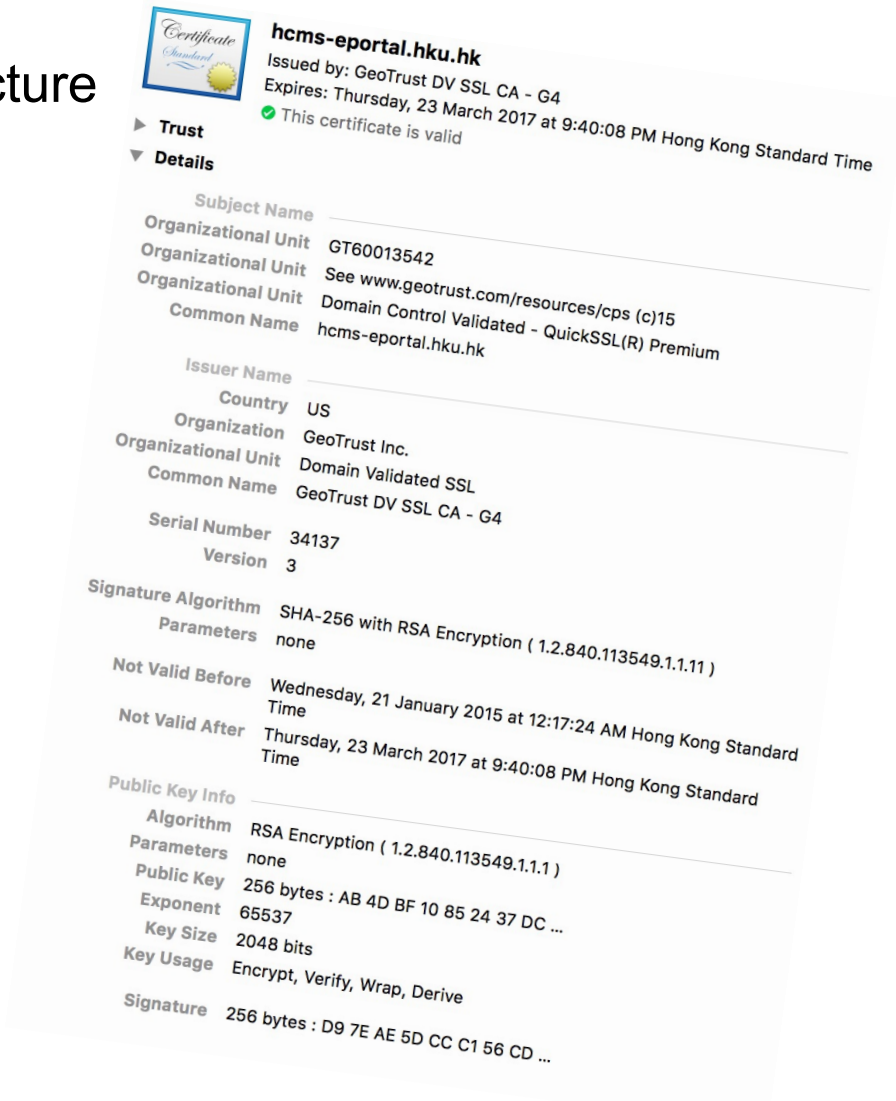


L9 – Blockchain and Crypto-CCY

Bitcoin – the underlying Cryptography

Prerequisite #4: Public Key Infrastructure

- For public Keys, the question is
  - who is associated with this Key?
  - who is confirming this?
- A Certificate is
  - a digital confirmation
  - about the guaranteed association
  - of a public cryptographic key to a person
  - and it is issued by a certificate authority
- However, the certificate does not confirm anything about
  - the content of signed documents
  - the trustworthyness of a requestor



L9 – Blockchain and Crypto-CCY

Bitcoin – What is a bitcoin?

Prof. Shamos, ECOM 6016:

> "A Bitcoin is a chain of titles to nothing"

But let's start at the beginning:

- For trading, storing and exchanging values, people need a common 'token' that represents value – otherwise all trade is only barter
- For such a token, you need something of value, or at least something that is so difficult to make/get/copy that everyone can associate a certain value to it. Examples:
  - a gold bar
  - a currency note or coin
  - a pack of cigarettes (where is that a currency?)
- In order to be of value, the difficulty of faking the token must be greater than the value of the token

L9 – Blockchain and Crypto-CCY

Bitcoin – What is a bitcoin?

A Bitcoin is one form of such a value-token.

Bitcoins are created by miners, when they solve a cryptographic problem:

- Bitcoin transactions need a confirmation in order to be validated
- Validation occurs in a distributed network and it involves finding a hash value that is smaller than a given threshold
- This computation is taking time and energy. The first node in the network finding such a small hash value is awarded bitcoins for the efforts – as a ‘token of appreciation’
- The miner thus is the first registered owner of those awarded bitcoins
- It can always be verified for which effort these bitcoins were awarded
- it is not possible to create ‘registered’ bitcoins without mining

L9 – Blockchain and Crypto-CCY

Bitcoin – What is a bitcoin?

Bitcoin Transactions:

Bob owes Alice money for lunch. He installs an app on his smartphone to create a new Bitcoin wallet. A wallet app is like a mobile banking app and a wallet is like a bank account.

To pay her, he needs two pieces of information: his private key and her public key.

Bob gets Alice's public key by scanning a QR code from her phone, or by having her email him the payment address, a string of seemingly random numbers and letters.*

The app alerts Bitcoin 'miners' around the world of the impending transaction. 'Miners' provide transaction verification services.

The miners verify that Bob has enough bitcoins to make the payment.

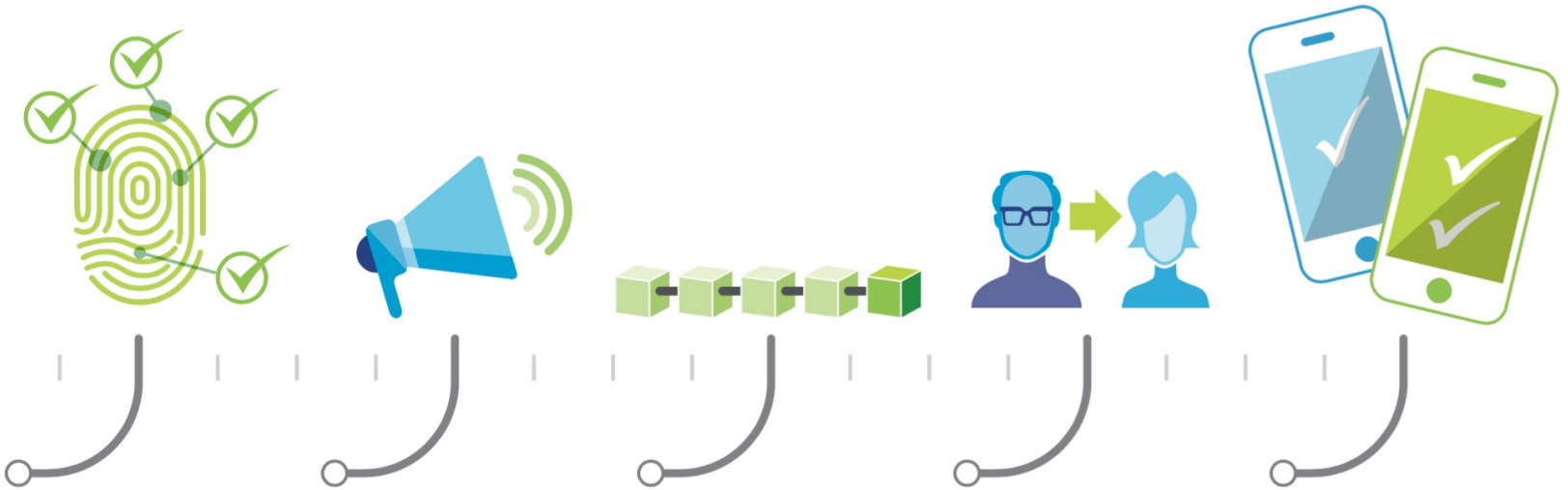
Many transactions occur in the network at any time. All the pending transactions in a given timeframe are grouped (in a block) for verification. Each block has a unique identifying number, creation time and reference to the previous block.

Source: Deloitte

L9 – Blockchain and Crypto-CCY

Bitcoin – What is a bitcoin?

Bitcoin Transactions:



The new block is put in the network so that miners can verify if its transactions are legitimate. Verification is accomplished by completing complex cryptographic computations.

When a miner solves the cryptographic problem, the discovery is announced to the rest of the network.

The algorithm rewards the winning miner with 25 bitcoins, and the new block is added to the front of the blockchain. Each block joins the prior block so a chain is made – the blockchain.

Within ten minutes of Bob initiating the transaction, he and Alice each receive the first confirmation that the bitcoin was signed over to her.

All the transactions in the block are now fulfilled and Alice gets paid.

Source: Deloitte

L9 – Blockchain and Crypto-CCY

Bitcoin – What is a bitcoin?

Bitcoin and value:

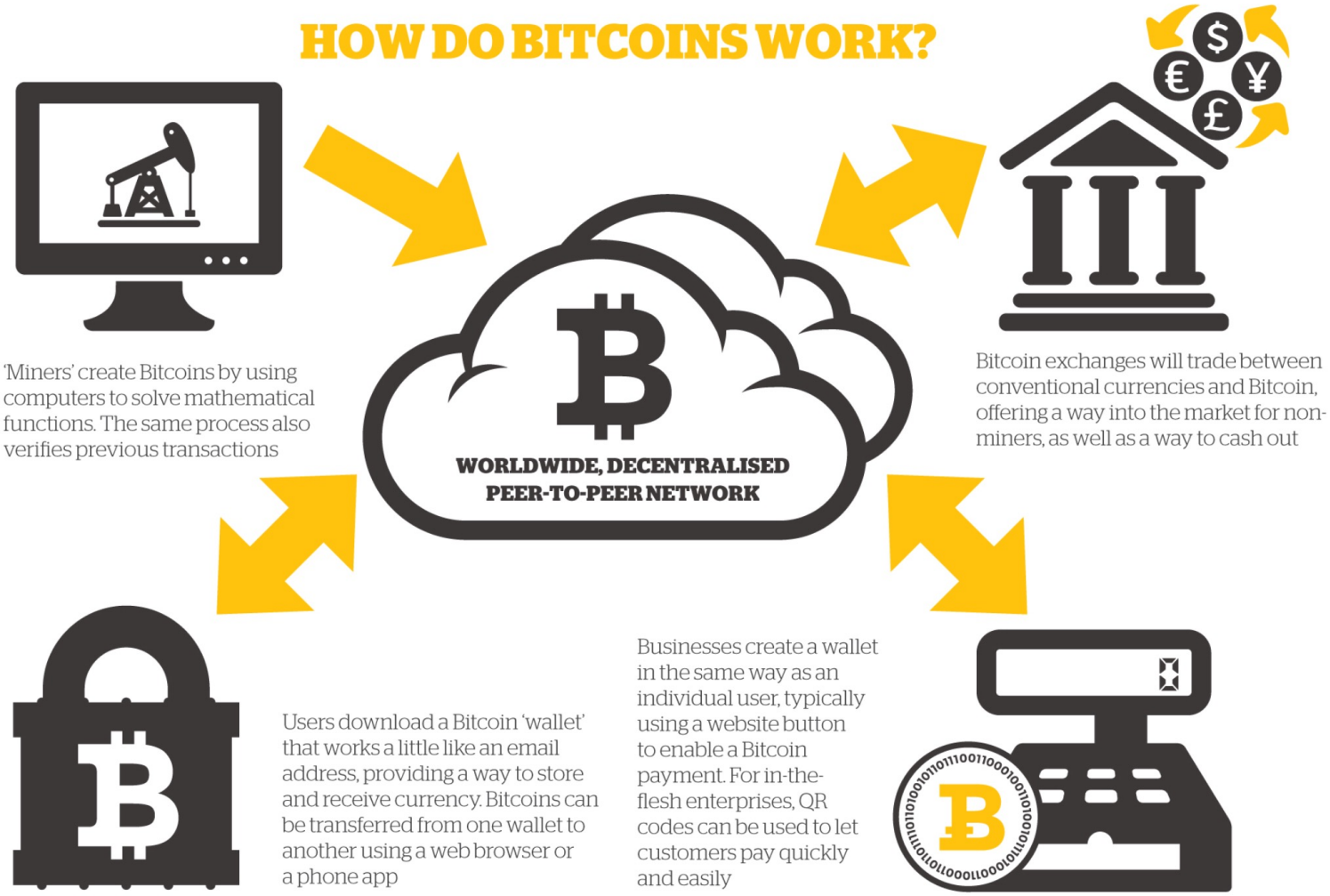
- the origin of a bitcoin is just an attestation to a miner of having done some computational work
  - there is 'nothing' attributable to this attestation; no coin, no bill, no bar
  - there is 'nothing' in your digital wallet (except your private key)

- Change of ownership is registered by the network into the chain of ownerships of a particular amount of bitcoins.
  - I got this bitcoin from A, who got it from B, who got it from C, who got it from …..

L9 – Blockchain and Crypto-CCY

Bitcoin – What is a bitcoin?

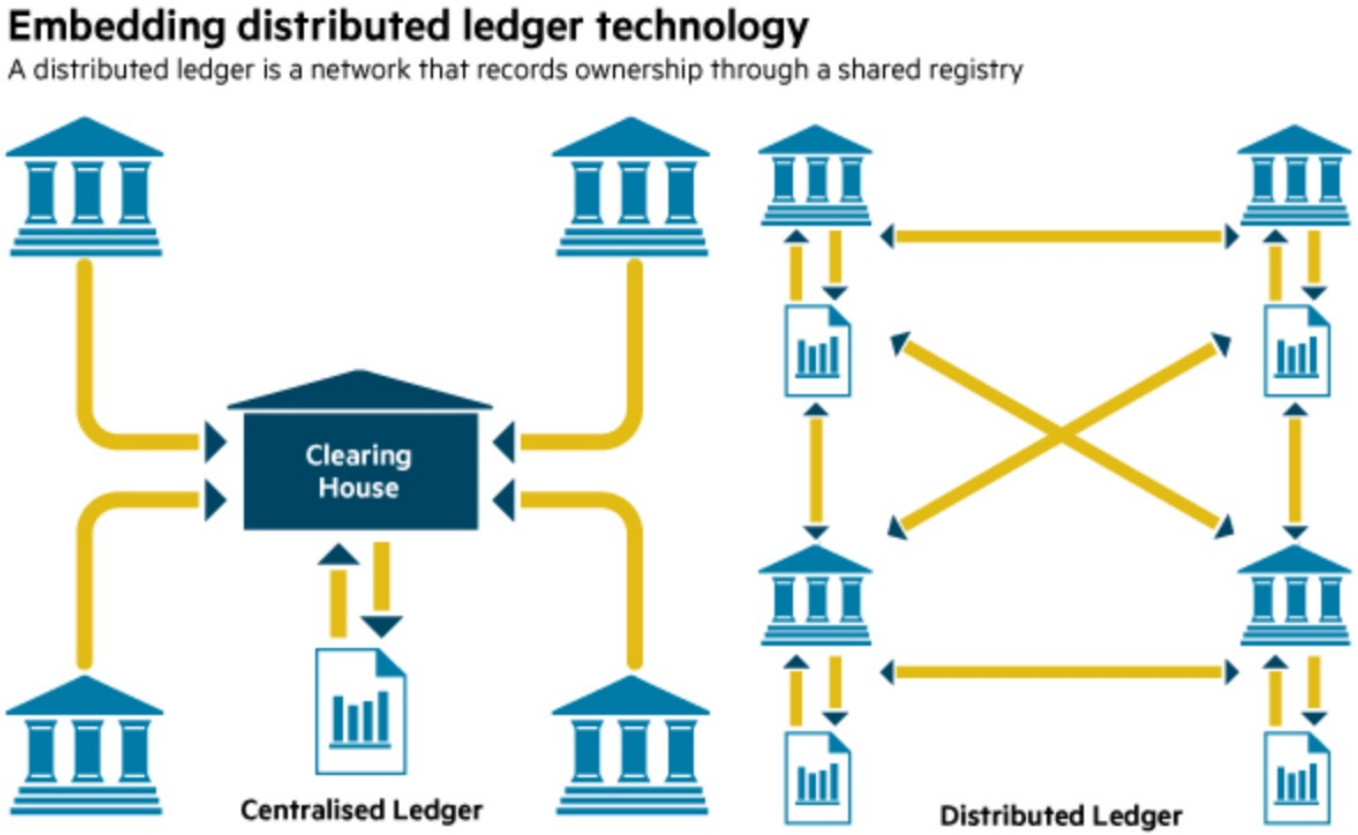
Bitcoins:



L9 – Blockchain and Crypto-CCY

Bitcoin – What is a bitcoin?

Registry of Bitcoins:



In contrast to today's networks, distributed ledgers eliminate the need for central authorities to certify ownership and clear transactions. They can be open, verifying anonymous actors in the network, or they can be closed and require actors in the network to be already identified. The best known existing use for the distributed ledger is the cryptocurrency Bitcoin

FT graphic. Source: Santander InnoVentures, Oliver Wyman & Anthemis Partners

L9 – Blockchain and Crypto-CCY

Bitcoin – … and other Crypto Currencies

Crypto Currencies:

#	Name	Price	Change	Chart	Trade
1	Bitcoin BTC	HK$410,255.91	-0.21%		Buy
2	Ethereum ETH	HK$12,612.35	+2.33%		Buy
3	Litecoin LTC	HK$1,365.93	-1.00%		Buy
4	Bitcoin Cash BCH	HK$3,709.50	+1.26%		Buy

L9 – Blockchain and Crypto-CCY

Crypto Currencies – typical properties

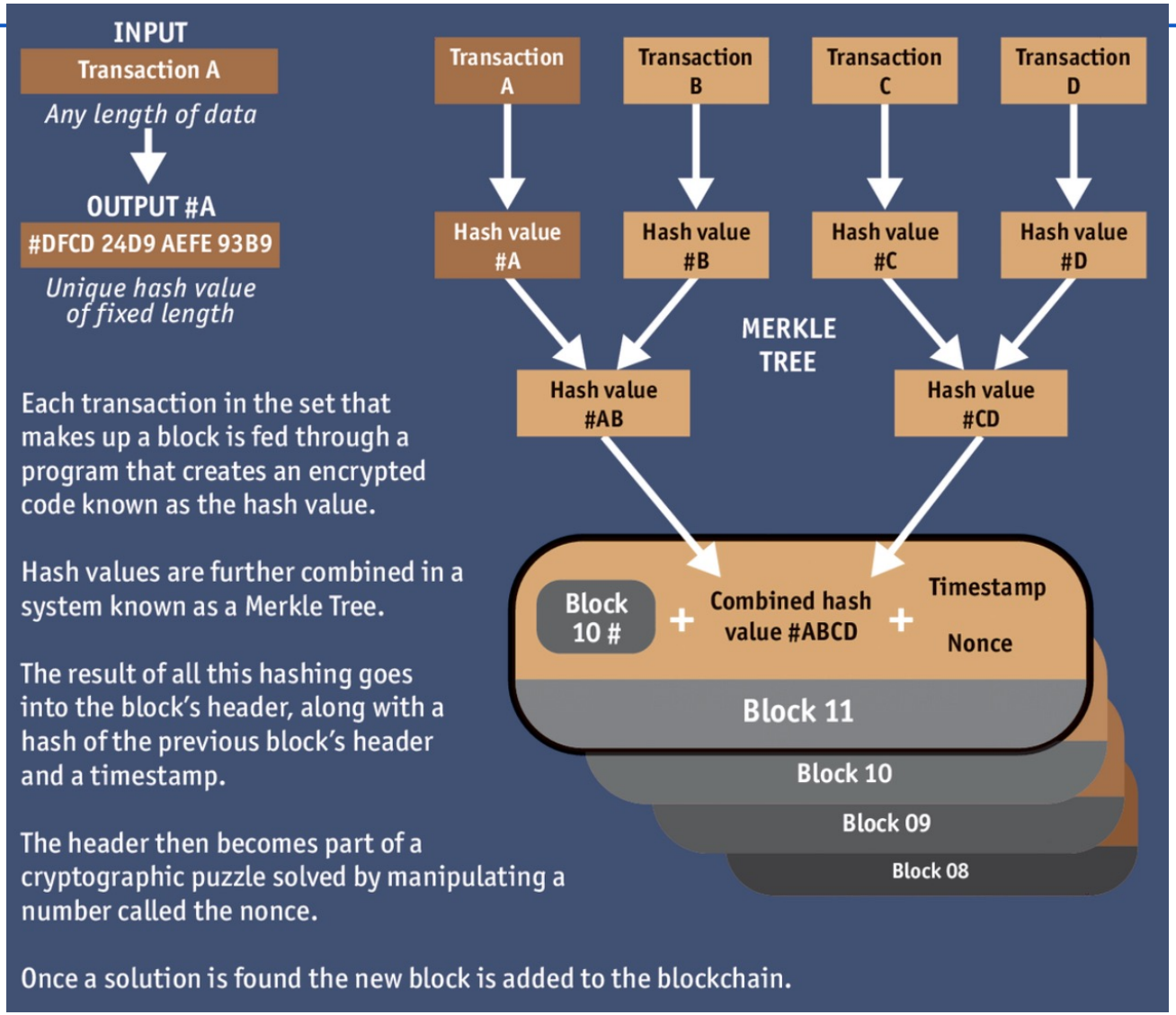
For most cryptocurrencies, specific attributes include the following:

- The code's resistance to counterfeiting.
- The network's ability to prevent "double- spending" (that is, spending money you do not own by use of forgery or counterfeiting) by verifying that each transaction is added to a distributed ledger or a blockchain.
- The limited supply, and the market's ability to divide single units into smaller fractions on a practically unlimited basis.
- The nearly instantaneous and irreversible transmission of value that takes place over the Internet, without the need for a trusted third-party intermediary.
- The decentralized network, which provides network security and transaction verification.
- The incentives embedded in the network protocol, which encourage participants to contribute computing resources for network support.
- The publicly available knowledge that a transaction has been posted to a global public transaction ledger.
- The personal data security enabled by public-private key cryptography.
- The dedicated core team of developers and miners who continually support and improve the code, help secure the network, and validate transactions.

L9 – Blockchain and Crypto-CCY

Blockchain

- The principle (as used for e.g. bitcoins)



L9 – Blockchain and Crypto-CCY

Blockchain

- Blockchain principle:

- Transactions are distributed into a network of computational nodes
  - thus, there is no central instance who ‘controls it all’

- After verification, all nodes add the confirmation block into their existing chain of blocks
  - thus, each node ‘knows it all’ (=every single transaction, all history)
  - future verification happens based on majority consensus, thus no single node can cheat
    - pls note: there is no ‘balance’ or snapshot of holdings on user basis, only historic transactions

- The use case of blockchain is characterised by the following:
  - change of ownership is important to know and verify
  - total amount of ownership of participants is less important

L9 – Blockchain and Crypto-CCY

Blockchain – Use Cases

Selected Potential Blockchain Use Cases

Financial Institutions	Corporates	Governments	Cross-industry
International payments	Supply chain management	Record management	Financial management & accounting
Capital markets	Healthcare	Identity management	Shareholders' voting
Trade finance	Real estate	Voting	Record management
Regulatory compliance & audit	Media	Taxes	Cybersecurity
Anti-money laundering & know your customer	Energy	Government & non-profit transparency	Big data
Insurance		Legislation, compliance & regulatory oversight	Data storage
Peer-to-peer transactions			Internet of Things

Source: Moody's Investors Service

L9 – Blockchain and Crypto-CCY

Blockchain – Smart Contracts

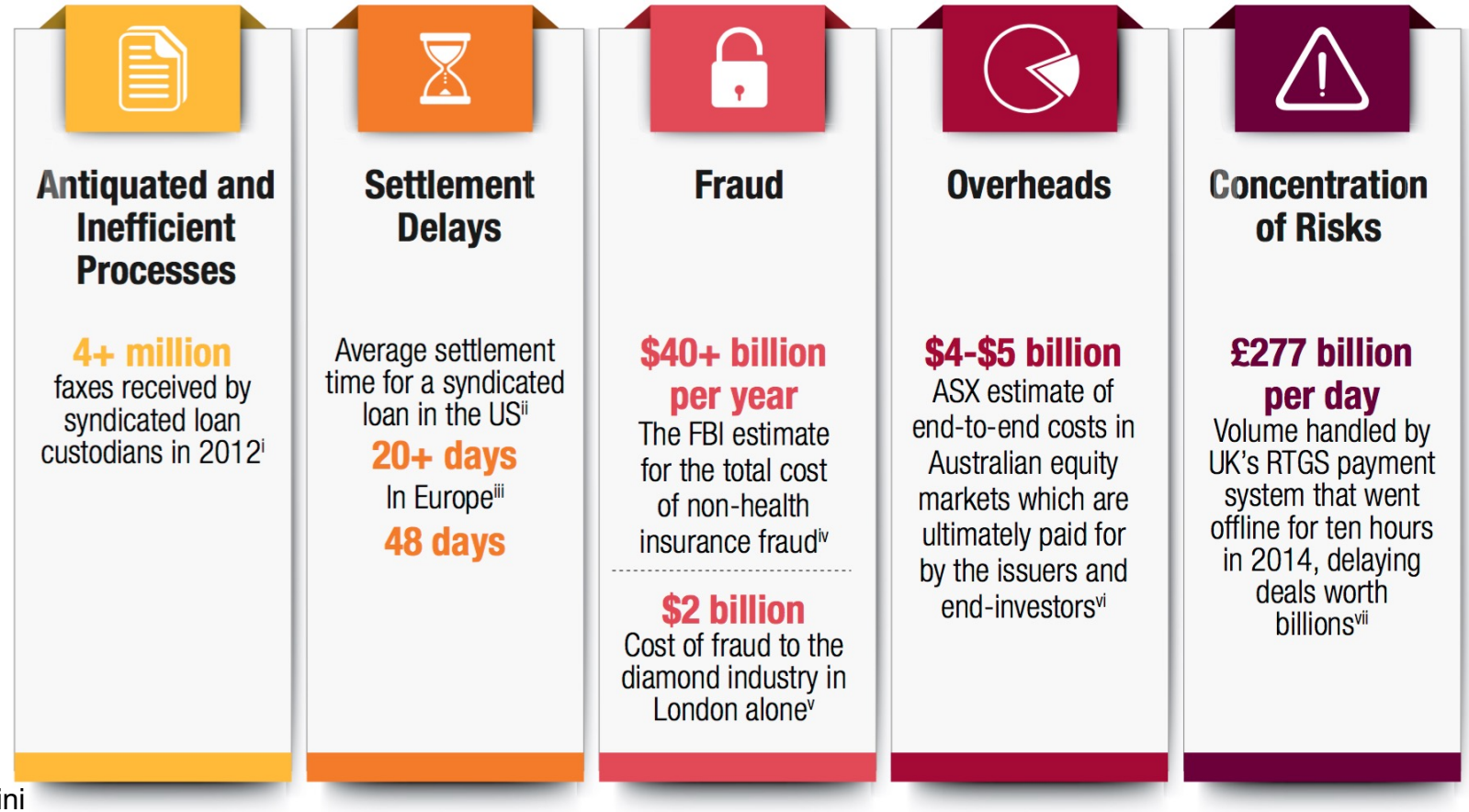
Smart contracts have been designed to automate transactions and allow parties to agree with the outcome of an event without the need for a central authority. Key features of smart contracts are: programmability, multisig authentication escrow capability and oracle inputs:

- A smart contract automatically executes based on programmed logic
- Multisig allows two or more parties to the contract to approve the execution of a transaction independently – a key requirement for multi-party contracts
- Escrow capability ensures the locking of funds with a mediator (e.g. a bank or an online market) which can be unlocked under conditions acceptable to contracting parties. Sometimes, external inputs such as prices, performance, or other real-world data may be required to process a transaction, and oracle services help smart contracts with inputs such as these.

L9 – Blockchain and Crypto-CCY

Blockchain – Smart Contracts

- potential issues with existing financial contracts:

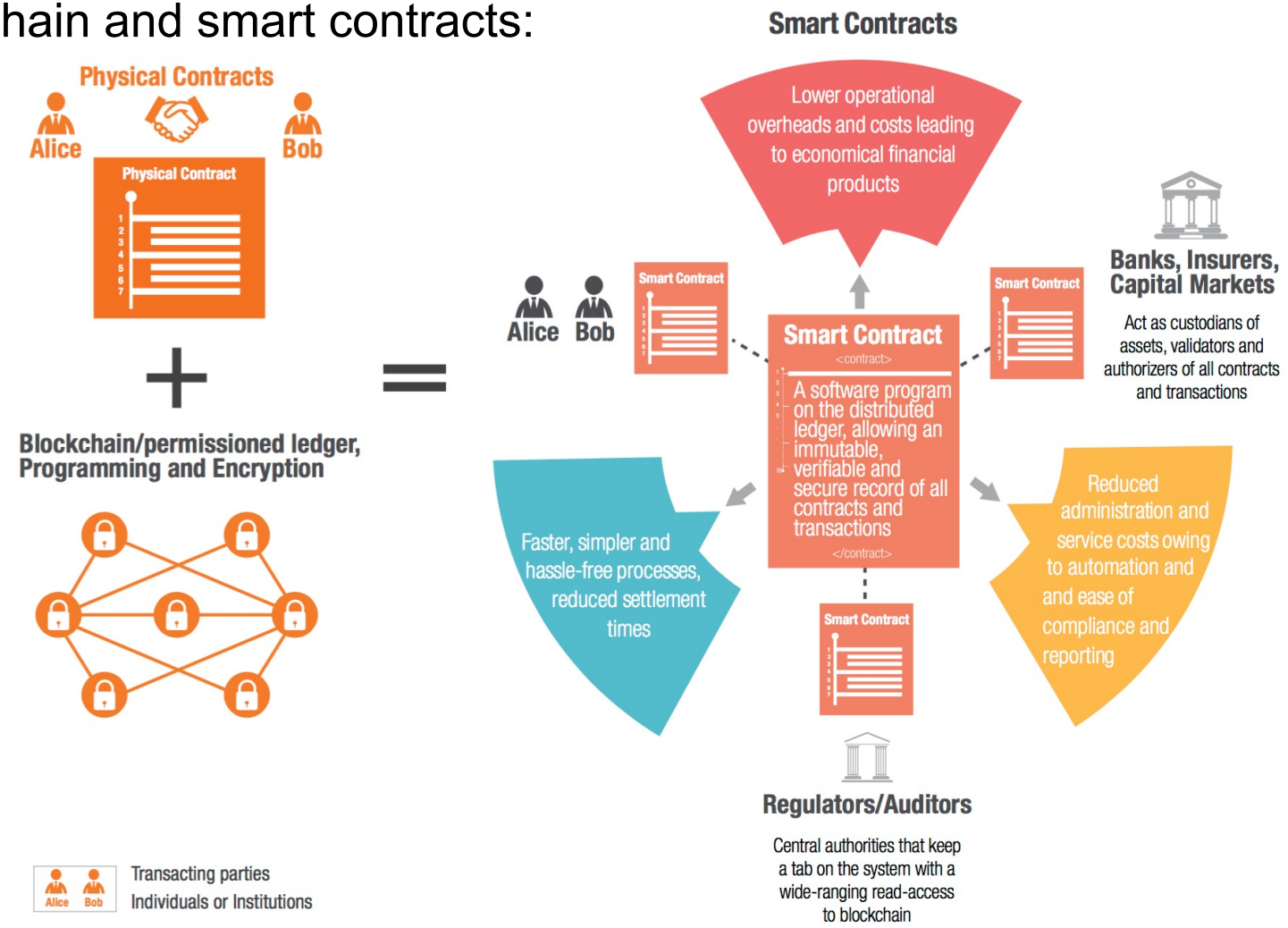


Source: Cap Gemini

L9 – Blockchain and Crypto-CCY

Blockchain – Smart Contracts

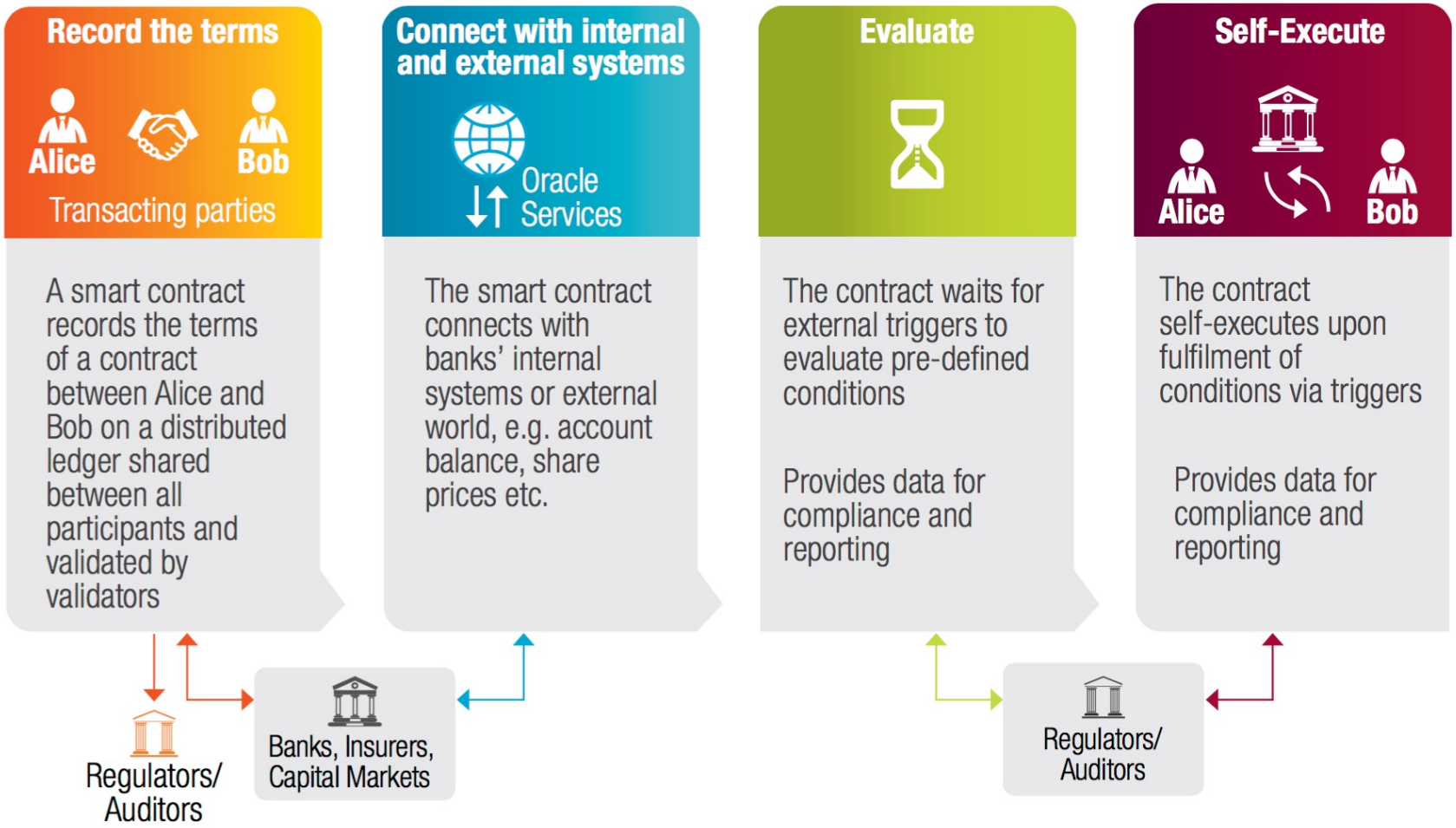
- Blockchain and smart contracts:



L9 – Blockchain and Crypto-CCY

Blockchain – Smart Contracts

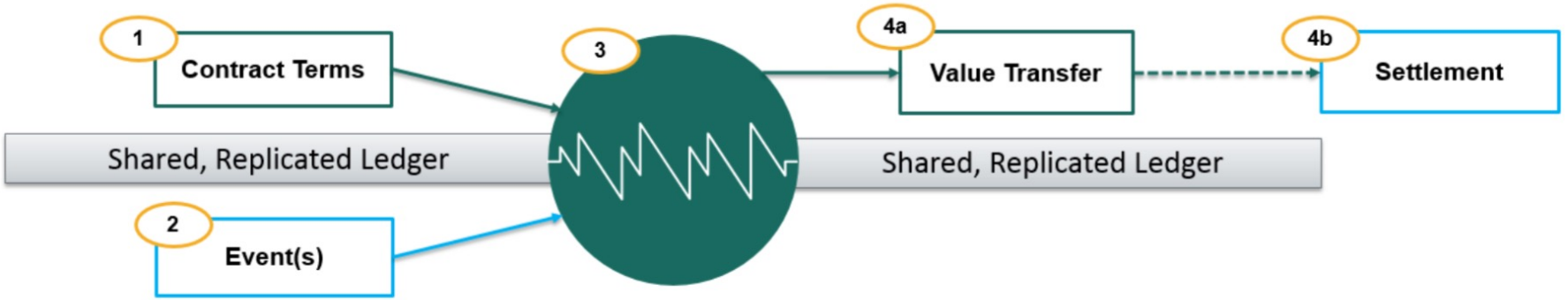
- Life cycle of smart contracts:



L9 – Blockchain and Crypto-CCY

Blockchain – Smart Contracts

- Blockchain and smart contracts:



1

- Counterparties establish obligations and settlement instructions
- Assets put under custody of smart contract
- Conditions for execution *("If…then…")*

2

- Event triggers contract execution
- Event can refer to:
  - Transaction Initiated
  - Information Received

3

- Terms of contract (Business Logic) dictate movement of value based on conditions met

4a

- Value transferred to intended recipient as dictated by contract terms
- For digital assets on the chain (e.g. Bitcoin) accounts are atomically settled

4b

- For assets represented off the chain (e.g. Securities, Fiat), accounts are considered settled when accounts off-chain match settlement instructions
- Changes to accounts will be reflected on ledger

External to Smart Contract

Source: Jo Lang / R3 CEV

L9 – Blockchain and Crypto-CCY

Digital Assets

Tokenisation

- Tokenization of assets → process of issuing a blockchain token (**security token**), which digitally represents a real tradable asset
- Created through a type of **Initial Coin Offering (ICO),** sometimes referred to as a **Security Token Offering (STO)** to distinguish it from other types of ICO
- STO: used to create a digital representation – a security token – of an asset

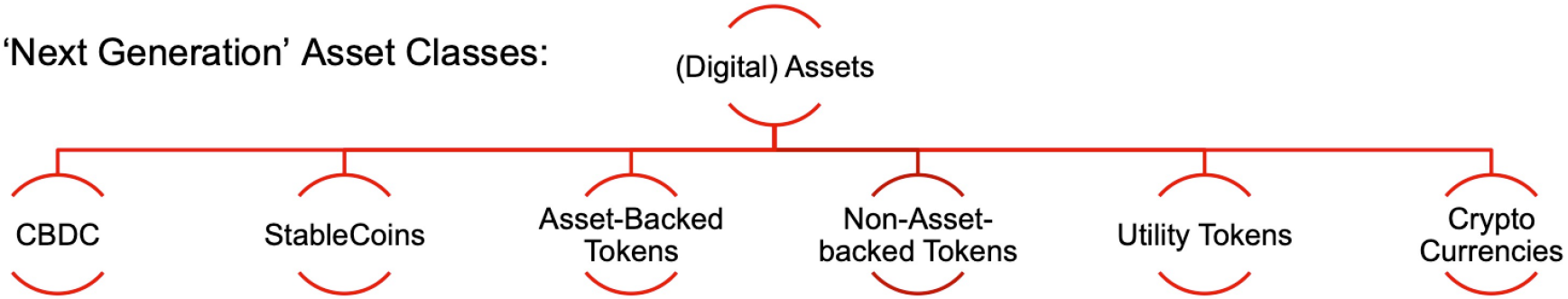
→ A security token could represent a share in a company, ownership of a piece of real estate or participation in an investment fund

→ Can be traded on a secondary market

L9 – Blockchain and Crypto-CCY

Digital Assets

– 'Next Generation' Asset Classes:



Central Bank Digital Curreny: Digital store of value (money) and method of exchange issued by a central bank.

A stablecoin refers to a new class of cryptocurrencies which attempt to offer price stability and/or are backed by reserve asset(s).

Asset-backed tokens facilitate the cost-effective and secure trading of real-world assets on the blockchain. Its value derives from the fractional ownership of the underlying asset which backs it.

Non-Asset-backed tokens represent typically claims and rights – e.g. of (re)payment – between parties. Again, tokens will allow for fractional exchange of such claims.

A utility token is a digital token of cryptocurrency that is issued in order to fund development of the cryptocurrency and that can be later used to purchase a good or service offered by the issuer of the cryptocurrency.

Cryptocurrency is a digital medium of exchange which uses crypto functions to conduct financial transactions. Cryptocurrencies leverage blockchain technology to gain decentralization, transparency, and immutability.

L9 – Blockchain and Crypto-CCY

Digital Assets - Benefits

- **Greater liquidity**

  Especially private securities or illiquid assets can be traded on a secondary market of the issuer‘s choice. This access to a broader base of traders increases the liquidity , benefiting investors who consequently have more freedom and sellers because the tokens benefit from the “liquidity premium“, thereby capturing greater value from the underlying asset.

- **Faster and cheaper transactions**

  Certain parts of the exchange process are automated because the transaction of tokens is completed with smart contracts. This can reduce the administrative burden involved in buying and selling, with fewer intermediaries needed, leading to faster deal execution and lower transaction fees.

- **More transparency**

  A security token is capable of having the token-holder‘s rights and legal responsibilites embedded directly onto the token, along with an immutable record of ownership. This allows you to know with whom you are dealing, what your and their rights are and who has previously owned this token.

- **More accessible**

  Thanks to reduced minimum investment amounts and periods, tokenization could open up investment in asset to a wider audience. Tokens are highly divisible, meaning invstors can purchase tokens that represent small percentages of the underlying assets. If each order is cheaper and easier to process, it will open the way for a significant reduction of minimum investment amounts.

  Since investors can exchange their tokens, the higher liquditiy could also reduce minmum investment periods.

L9 – Blockchain and Crypto-CCY

Digital Assets

- **Regulatory alignment**

  Security regulations are typically technology agnostic, meaning that security tokens can fall under the full scope of relevant security regulations, which can vary significantly. This is true for the creation and initial sale of the tokens and trading them on secondary markets. Consequently, many of the advantages of tokenization are underminded if regulations prevent the free and international exchange of tokens. Compliant methods of creating and exchanging of tokens are needed in a domestic and international scope.

- **Solutions, Markets**

  Some implementation checks if a trade is compliant by taking into account who the buyer and seller are and where the trade occurs. US SEC and EU‘s ESMA have made comments in this area. Meanwhile Switzerland and Malta have made more progressive plans to accomodate new marketplaces for tokenized securities.

- **Consequences**

  A lack of scrutiny can allow scams and open the door to hackin which could harm investors and the borader economy, discourage investors and cripple the token economy completely.

L9 – Blockchain and Crypto-CCY

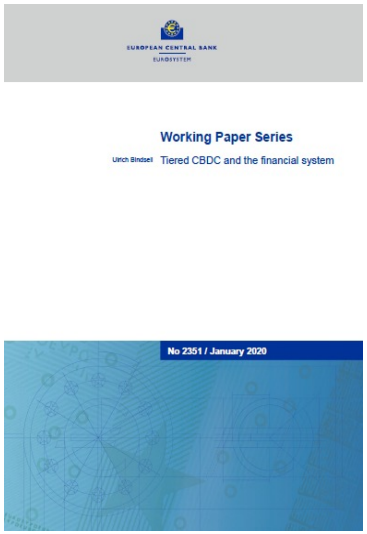
Digital Assets – potential role for Banks

Financial institutions will have to choose where to play in the value chain. They could…

- advise issuers on how to structure their token
- be a safe keeper of the tokenized asset (art, real estate property etc.)
- leverage their expertise as custodian banks
- pay agents to create life cycle vent transactions on the distributed ledger
- implement life cycle processing in smart contracts and deploy them on a blockchain platform
- offer services to maintain customer accounts in cryptocurrencies and tokens
- act as central distributors faciliating access for their clients to transact on diverse tokenization platforms or token exchanges

L9 – Blockchain and Crypto-CCY

Digital Assets – Currencies - Sample Literature

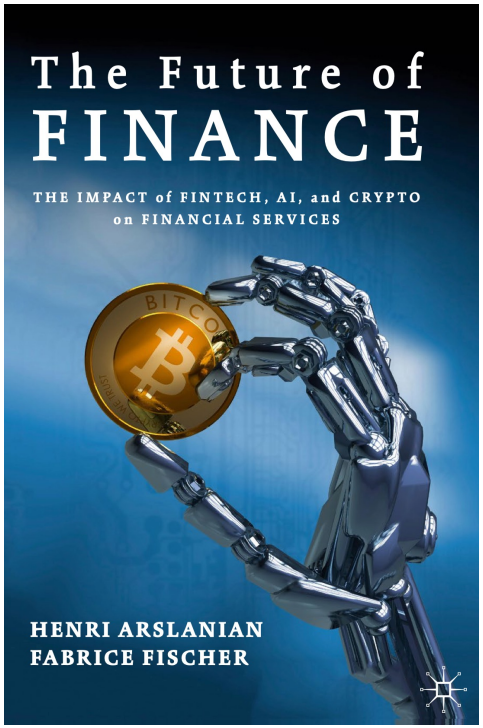


ECB Working Paper: Tiered CBDC and the financial system

This paper first reviews the advantages and risks of such CBDC. It then discusses two prominent arguments against CBDC, namely (i) risk of structural disintermediation of banks and centralization of the credit allocation process within the central bank and (ii) risk of facilitation systemic runs on banks in crisis situations. Two-tier remuneration of CBDC is proposed as solution to both issues, and a comparison is provided with a simple cap solution and the solution of Kumhof and Noone (2018). Finally, the paper compares the financial account implications of CBDC with the ones of crypto assets, Stablecoins, and narrow bank digital money, in a domestic and international context.

L9 – Blockchain and Crypto-CCY

Digital Assets – Currencies - Sample Literature



You all should have received this eBook / Link

Look into Part III and Part V for insights on Blockchain, Crypto Assets and future developments