Of bovines, blockchain, 'smart contracts' and Ghenghis Khan

June 2017

What the fork?

Most presentations on blockchain will attempt to explain:

- The Byzantine general’s problem
- Hashing and SHA-256
- Merkle Tree
- Private and public key encryption and decryption
- Proof of Work consensus mechanism
- Nonce
- Bitcoin mining
- Seigniorage
- Halving
- Sybil attack
- Forking

Do you know the thermodynamic principles by which an internal combustion engine works?

Does this stop you from driving a car?

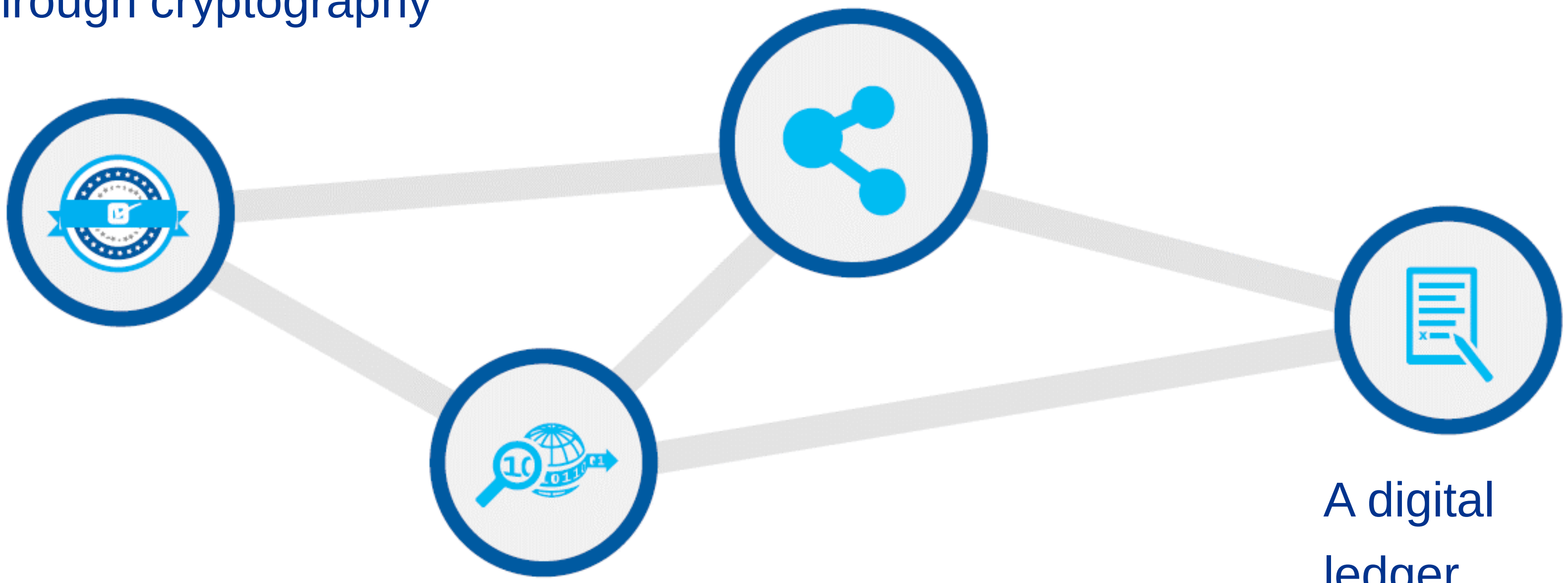
Do you know the routing protocols for IPv6?

Does this stop you from shopping on the Internet?

Do you know how distributed ledger technology works?

Do you really need to?

There are four cornerstone features



Authenticity through cryptography

Consortium shared database

Distributed trust model

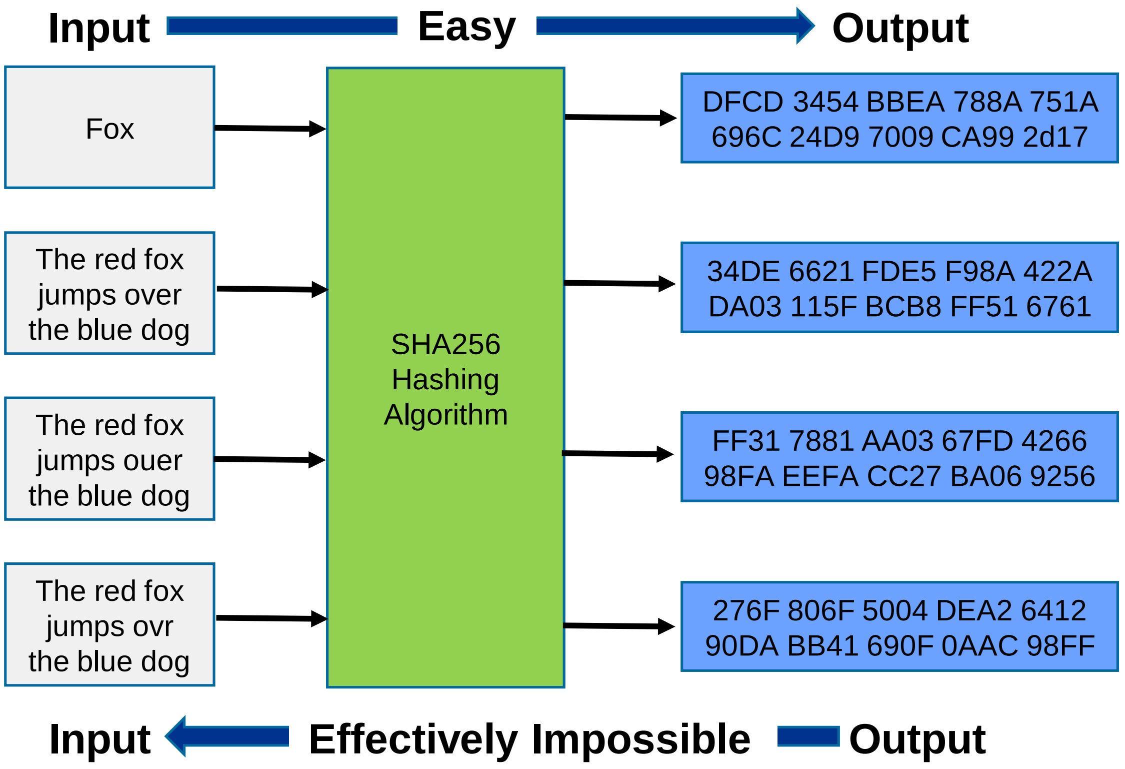
A digital ledger

A distributed trust protocol works for knowledge transfer, not just currency

	The blockchain
Confirm ownership of [knowledge] assets by any party to a transfer	☑
Confirm the value of the [knowledge] transfer is legitimate	☑
Validate transfers, agreed by all parties using a **consensus mechanism**	☑
Timestamp, encrypt and protect all records of every transfer	☑
Transparently share the results and history of transfers with appropriate parties	☑
Maintain privacy of counterparties to any transfer	☑
Prevent anyone trying to perform the same transfer more than once	☑
Prevent anyone later denying that they were a party to a transfer (either side)	☑
Ensure no one can tamper or modify the record of the transfer once validated	☑
Provide permanent availability of the transfer network across all borders	☑
Be architected in a similar fashion to the Internet, with no single point of failure	☑

Let's take a moment to understand 'hashing'

- The foundation of blockchain is **hashing** and **encryption**
- Hashing is a long-established and well-proven computing technique
- Hashing is a **one-way process**, creating fixed length hexadecimal data from source information
- The original information cannot be discerned or re-created from the hash data



Input → **Easy** → **Output**

Fox → SHA256 Hashing Algorithm → DFCD 3454 BBEA 788A 751A 696C 24D9 7009 CA99 2d17

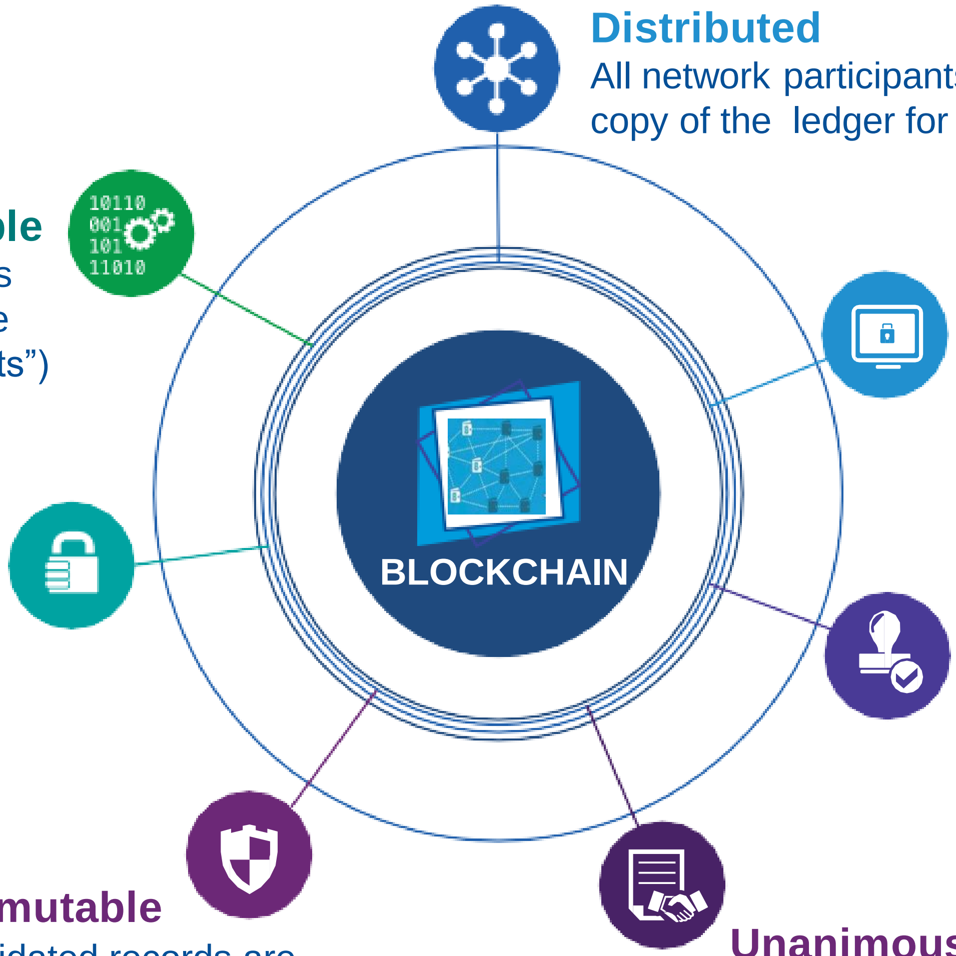
The red fox jumps over the blue dog → SHA256 Hashing Algorithm → 34DE 6621 FDE5 F98A 422A DA03 115F BCB8 FF51 6761

The red fox jumps ouer the blue dog → SHA256 Hashing Algorithm → FF31 7881 AA03 67FD 4266 98FA EEFA CC27 BA06 9256

The red fox jumps ovr the blue dog → SHA256 Hashing Algorithm → 276F 806F 5004 DEA2 6412 90DA BB41 690F 0AAC 98FF

Input ← **Effectively Impossible** ← **Output**

There is much good news amidst this jargon



Distributed
All network participants have a full copy of the ledger for full transparency

Anonymous
The identity of participants is (supposed to be) either pseudonymous or anonymous

Time-stamped
Transaction timestamp is recorded a block

Unanimous
All network participants agree to the validity of each of the records

Immutable
Any validated records are irreversible and cannot be changed

Secure
All records are individually encrypted

Programmable
A blockchain is programmable ("Smart Contracts")

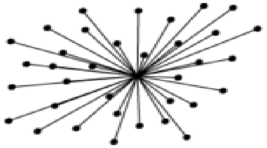
It's the '90s again … an explosion of solutions

Since 2008, blockchain technology was created to enable cryptocurrency transactions with Bitcoin, and has been gaining momentum with R&D activities and applications across industries.

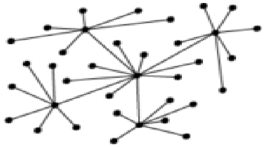
Permissioned **Permissionless**

Traditional Centralized Database Ledgers	Permissioned Private Ledgers	Permissioned Public Ledgers	Permissionless Public Ledgers
• Consensus by automated or manual reconciliation using intermediaries • Record is not immutable • Must be reconciled with other ledgers to settle transactions	• Consensus by PBFT or other mechanism • Decentralised, only permissioned entities may read and write the ledger	• Consensus by Proof of Work, Proof of Stake, Voting Pools or other mechanism • Decentralised, only permissioned entities may write the ledger, but anyone may view the ledgers contents	• Consensus by Proof of Work • Distributed, anyone can read and write the ledger, as long they meet certain criteria and follow certain rules
ORACLE DATABASE Microsoft SQL Server redhat	Chain Digital Asset Holdings	ripple Axoni stellar	ethereum ₿

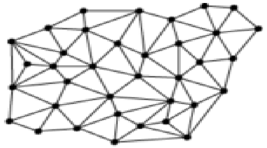
High throughput **Low throughput**



Centralised



Decentralised



Distributed

KPMG

The blockchain / DLT ecosystem is crowded

Use Case Developers, Development Platforms and APIs

Digital Asset Holdings
R3 CEV
Counterparty
ETHEREUM
Chain
eris INDUSTRIES
Tendermint
HYPERLEDGER
HEDGY
MultiChain
Microsoft Azure
Gem

Cyrptocurrency and Payment Ecosystem

coinprism
bitpay
stellar
21.co
ripple
Counterparty

Exchanges

EmerCoin
itBit
kraken bitcoin exchange
BITFINEX

Prediction Markets

augur

Security and Asset Trading Platforms, Settlements and Clearing

Digital Asset Holdings
Chain
openchain
SETL

Smart Contracts

Digital Asset Holdings
symbiont
ETHEREUM
clearmatics
Mirror
Counterparty
eris INDUSTRIES

Digital Content/Documents, Storage and Delivery

factom
Bitproof.io

Playbox Providers

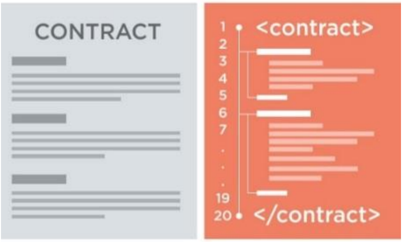
Microsoft Azure
CONSENSYS
ETH BaaS
IBM Bluemix
amazon web services
Chain

Existing Established FS Infrastructure

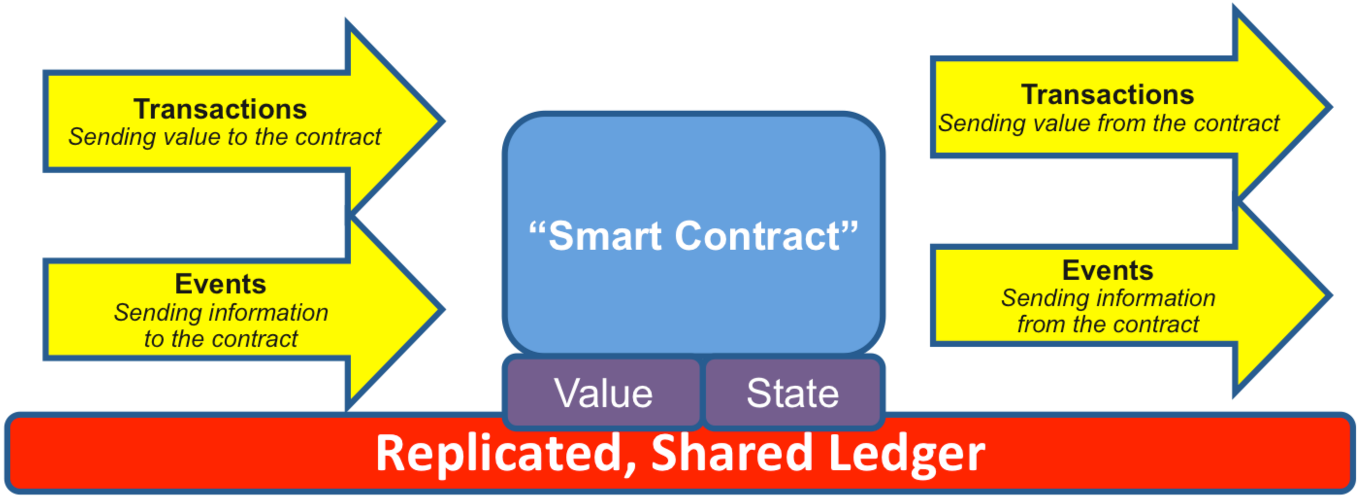
DTCC
ICAP
NASDAQ
DEUTSCHE BÖRSE GROUP
London Stock Exchange
ASX
ACH Automated Clearing House
SWIFT

KPMG

What exactly is a 'smart contract'?



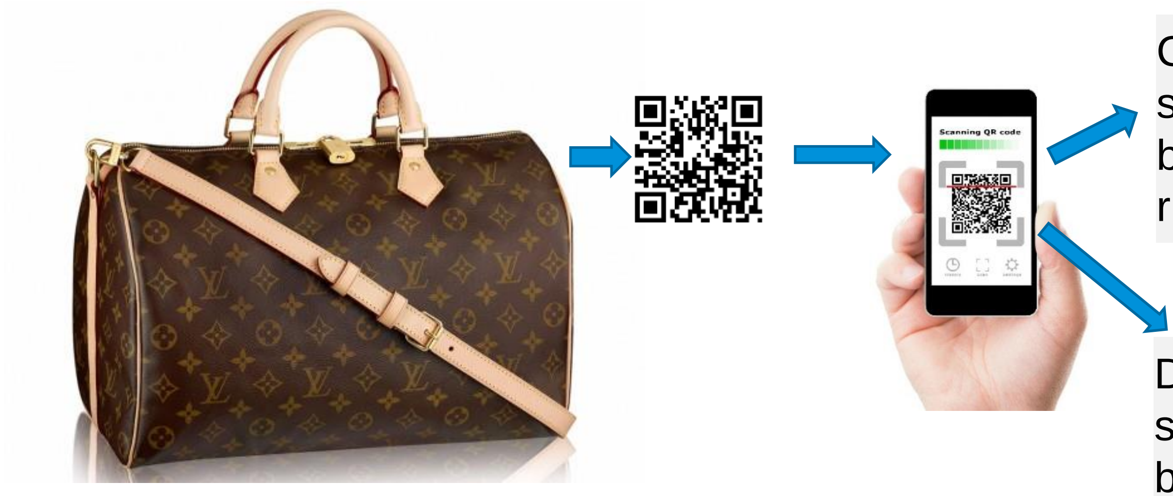
- **Smart contracts** are **self-executing** protocols that work with a **blockchain** to **enforce performance** of a contract with certainty and resilience
  - Neither a paper nor digital document on a server, but a computer program
  - Executed by the entire blockchain network
  - Can easily contain the same level of detail as a physical contract
- Triggered by an **event**, the code in the blockchain **automatically executes** the fulfillment of a **previously agreed arrangement**
  - Negotiate prices and monitor inventory levels
  - Enact renewal or termination clauses
- **Replace expensive, manual effort with automation**


Transactions
Sending value to the contract
Events
Sending information to the contract
"Smart Contract"
Value
State
Transactions
Sending value from the contract
Events
Sending information from the contract
Replicated, Shared Ledger

Digital ledgers revolutionise supply chains

Digital ledgers have huge potential in supply chains – for provenance of goods, proving the integrity of items and enabling a full chain-of-custody type solution.

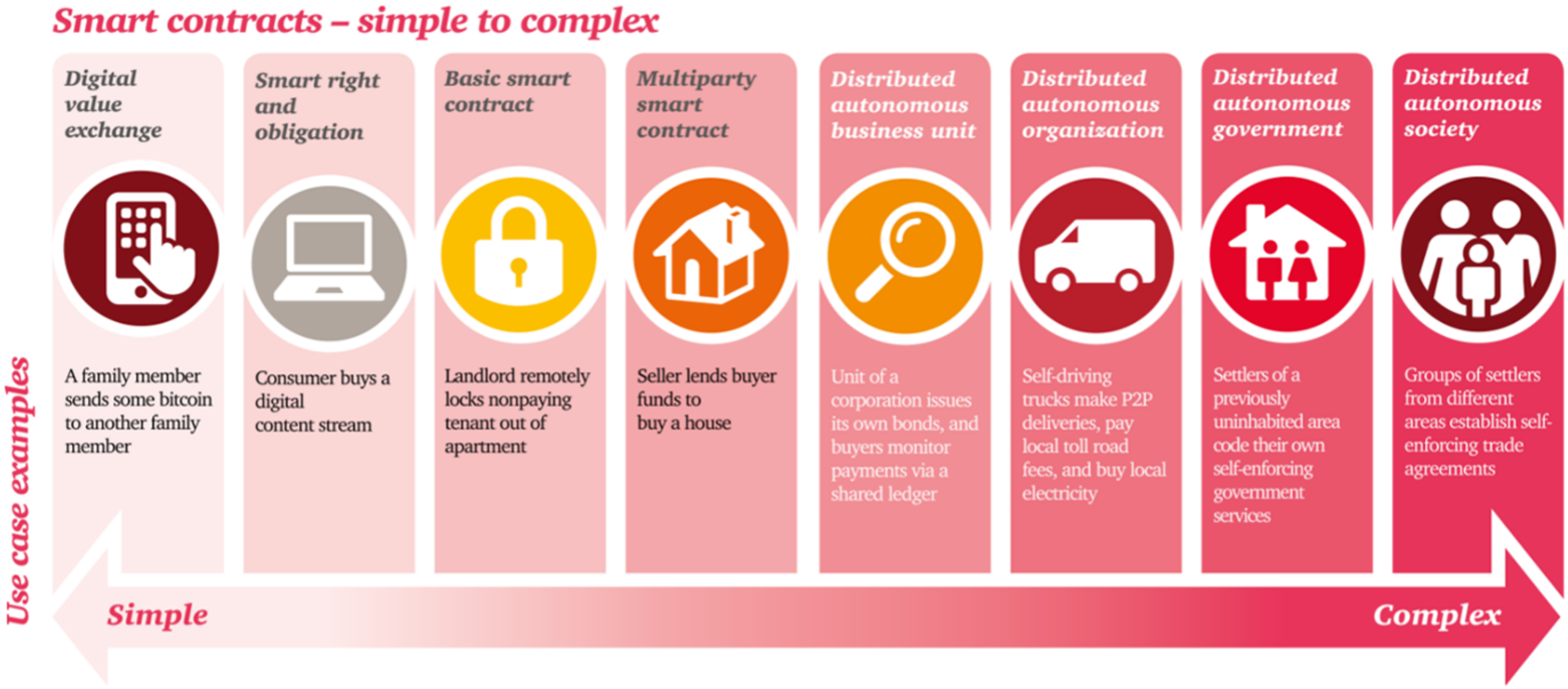
Is this handbag a real Louis Vuitton of not?



Confirmed. According to LVMH supply chain blockchain, this bag is in the right place at the right time.

Disproved. According to LVMH supply chain blockchain, this bag has to be a fraud. It is not where it should be right now.

Smart contracts can come in many forms …



Smart contracts – simple to complex

Use case examples

Digital value exchange
A family member sends some bitcoin to another family member

Smart right and obligation
Consumer buys a digital content stream

Basic smart contract
Landlord remotely locks nonpaying tenant out of apartment

Multiparty smart contract
Seller lends buyer funds to buy a house

Distributed autonomous business unit
Unit of a corporation issues its own bonds, and buyers monitor payments via a shared ledger

Distributed autonomous organization
Self-driving trucks make P2P deliveries, pay local toll road fees, and buy local electricity

Distributed autonomous government
Settlers of a previously uninhabited area code their own self-enforcing government services

Distributed autonomous society
Groups of settlers from different areas establish self-enforcing trade agreements

Simple — *Complex*

… and if we can deliver on 'distributed trust', there might be far less need for

- ➢ Escrow
- ➢ Underwriters
- ➢ Notaries
- ➢ Clearance systems
- ➢ Intermediaries
- ➢ Brokers
- ➢ Exchanges
- ➢ Arbitrators
- ➢ Regulators ?
- ➢ Bankers ?
- ➢ Accountants ?
- ➢ Auditors ?

KPMG

Reality in summary

- New technologies with dramatic impacts across many industries
- Many blockchains, not just ‘The’ public blockchain underpinning Bitcoin
- Many potential uses for different types of blockchains
- There is enough traction now to sustain growth
- New developments are more suitable for enterprises and regulated sectors
  - **Distributed Ledger Technologies (DLTs) or Blockchain 2.0** will gain more traction
  - Some of these can form the backbone of emerging ‘**Smart Contract**’ solutions
- There are multiple use cases for DLTs as well
- It is still very early days, but the potential disruptive impact is significant enough to warrant assessment, experimentation and implementation by firms today
- In all this, the role of governments, not just regulators, has yet to be standardised
  - This role could spell success or failure in a given jurisdiction

- **But being human still means something …**

… and to detest traffic is entirely human

KPMG

Thank you