

Introduction to Blockchain and its Disruptive Potential

WFEO-CIC International Seminar on Internet of Things 2017



Presented by : Abdul Fattah Yatim MIEM

WFEO – 13 May 2017

Outline

- **Overview – Recent Developments**
- **Bitcoin and Blockchain Highlights**
- **Technologies Used in Bitcoin**
- **Chaining of Blocks, Immutability and Distributed Databases**
- **Country Initiatives and White Papers**
- **Use Cases – IoT, Smart Cities, Smart Contracts**
- **Some Elements Common to All Blockchains**
- **ISO Standards Committee on Blockchain**
- **Summary**

About Myself



CAREER HISTORY

- National Electricity Board (LLN, now TNB)- 1978 -1983
- Esso Malaysia (now Exxon) - 1984 -1995
- System Consultancy Services Sdn Bhd (Consultant to Malaysian Armed Forces) - 1996 -2002
- Freelance Consultant - 2003 – Present

SPECIALIZATION

- Strategic Planning (Business and ICT)
- Information Security Management
- Business Continuity Management
- Risk Management
- Change Management

PROFESSIONAL MEMBERSHIPS

- Member, Institution of Engineers Malaysia
- Member, Malaysian Society for Engineering and Technology
- Professional Member, Organisation of Islamic Cooperation – Computer Emergency Response Team (OIC-CERT)

Presentations, Articles, Committee on Blockchain

TALKS

- Malaysia Industry-Government Group for High Technology - MiGHT – 7 Dec 2016
- Minister of Ministry of Science, Technology and Innovation – 13 January 2017
(together with Secretary General, Directors, Senior Management of MOSTI)
- Institution of Engineers, Malaysia – 4 March 2017
- Academy of Sciences Malaysia – 31 March 2017
- Blockchain Conference – Malaysia – 9 April 2017

ARTICLES

- Institution of Engineers Malaysia – Jurutera Bulletin (March 2017)

COMMITTEE

- **Chairman of Standards Committee on Blockchain and Distributed Ledger Technologies (TC/G/15), Department of Standards Malaysia (Mirror Committee to ISO/TC 307 committee on Blockchain and Distributed Ledger Technologies)**
- Task Force in Ministry of Science, Technology and Innovation to prepare Cabinet Paper on Blockchain for the Minister to present to the Malaysian Cabinet.

INTRODUCTION TO BLOCKCHAIN AND ITS DISRUPTIVE POTENTIAL

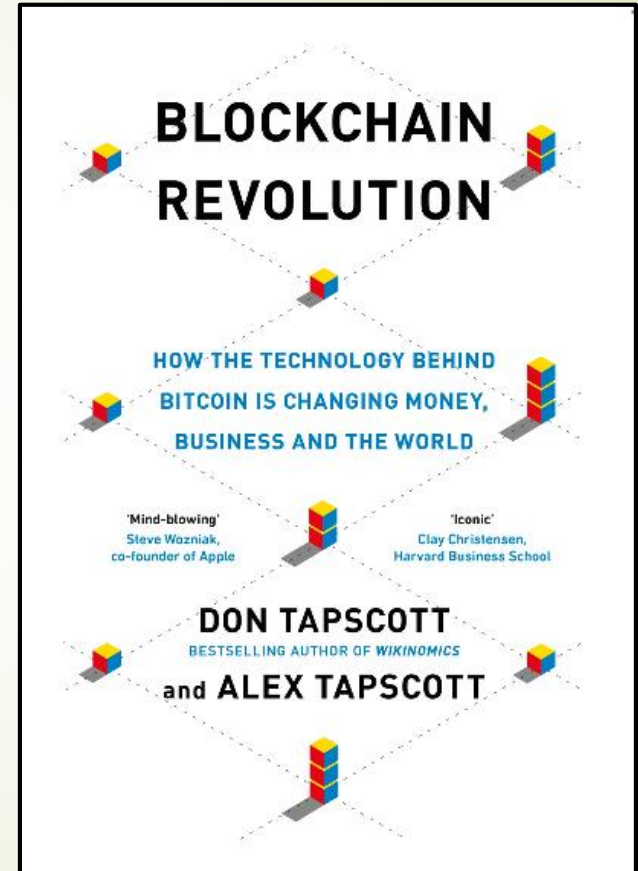
OVERVIEW – RECENT DEVELOPMENTS

Blockchain Revolution

“The Blockchain today is what the World Wide Web was in 1992. Blockchain will impact all aspects of society just as the WWW has impacted and engrained in today’s economy, government and society, but in a shorter timeframe....

Blockchain enables Internet of Information to enhance to Internet of Value.”

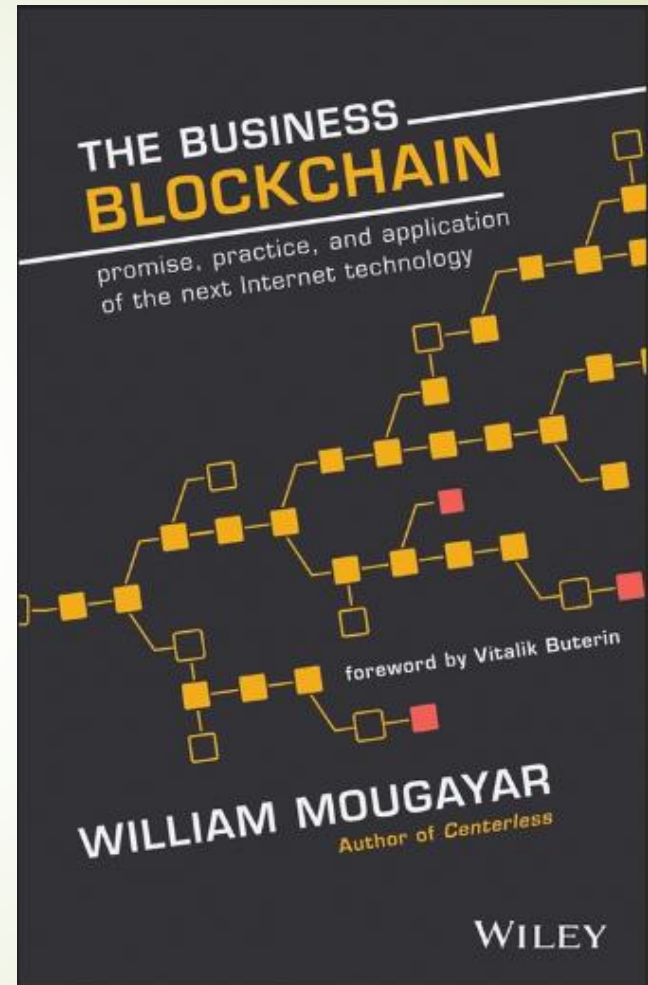
(Paraphrased quote from a few speakers and authors including Don Tapscott and Alex Tapscott, co-authors of “Blockchain Revolution – How the Technology Behind Bitcoin is Changing Money, Business and The World”).



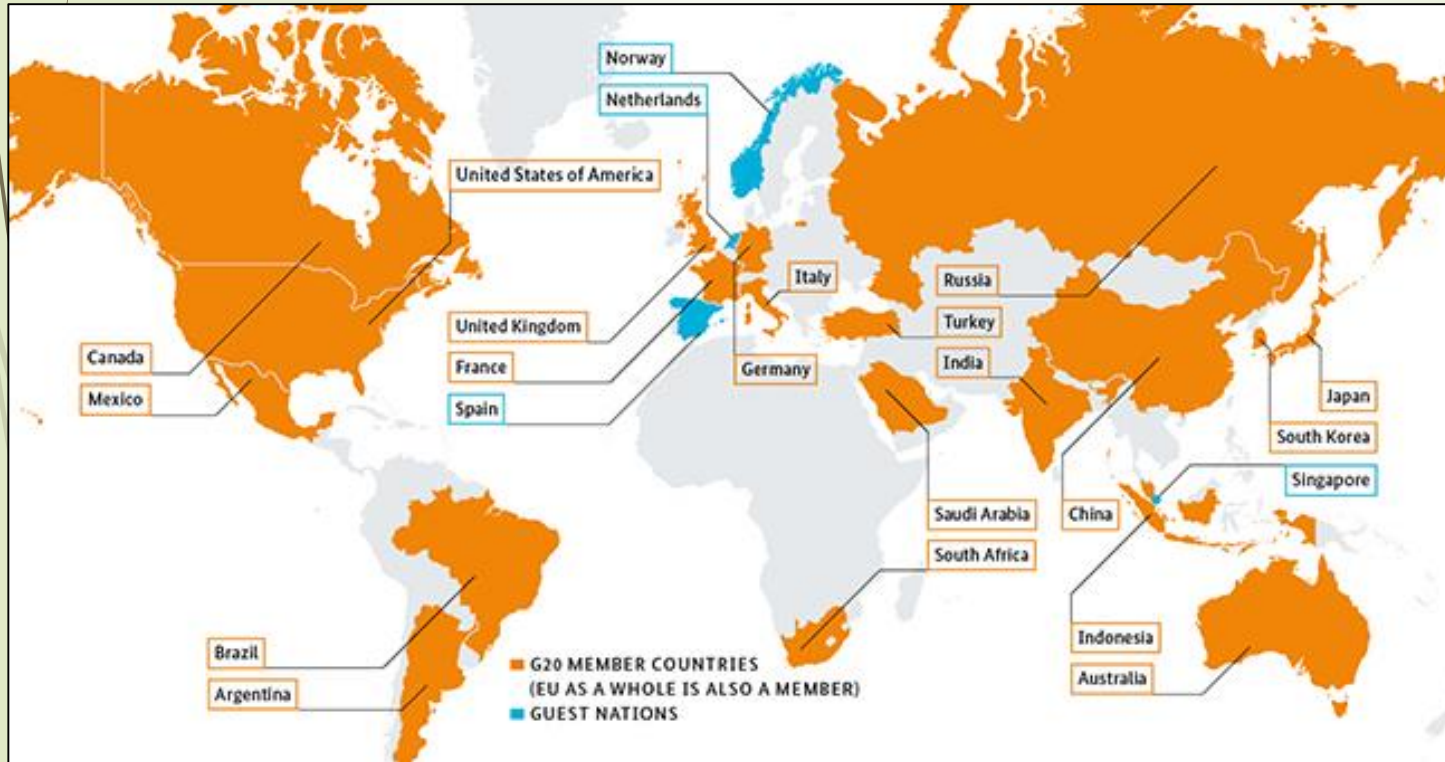
Business Blockchain

“The Blockchain is part of the history of the Internet. It is at the same level of the World Wide Web in terms of importance, and arguably might give us the Internet the way it was supposed to be: more decentralized, more open, more secure, more private, more equitable and more accessible. Ironically many Blockchain applications also have a shot at replacing legacy web applications, at the same time as they will replace legacy businesses that cannot loosen their grips on heavy-handed centrally enforced trust functions.

No matter how it unfolds, the Blockchain’s history will continue to be written well after you finish reading this book, just as the history of the Web continued to be written well after its initial invention. But here’s what makes the Blockchain’s future even more interesting: **you are part of it.**”



G20 - Overview



The G20 is the central forum for international cooperation on financial and economic issues. The G20 countries account for **more than four-fifths of gross world product** and **three-quarters of global trade**, and are home to almost **two-thirds of the world's population**.

Digitalization

The G20 Countries Should Engage with Blockchain Technologies to Build an Inclusive, Transparent, and Accountable Digital Economy for All

Julie Maupin (Centre for International Governance Innovation (CIGI))

March 16, 2017 | Last updated: March 20, 2017

Blockchain technologies hold the key to building an inclusive global digital economy that is auditably secure and transparently accountable to the world's citizens. At a time when governments must fight to restore the public's faith in cross-border economic cooperation, blockchains can play a critical role in strengthening economic resilience while ensuring the global economy works to the benefit of all. The G20 must take decisive steps to harness this technology in service of its policy goals across the core focus areas of economic resilience, financial inclusion, taxation, trade and investment, employment, climate, health, sustainable development, and women's empowerment. Failure to do so risks further fragmenting the global economy, undermining public trust in international economic institutions, and pushing the most cutting-edge blockchain developments into dark web deployments that are beyond the reach of government influence. By acting now to embrace blockchains' socially beneficial properties and minimize their potential downside risks, the G20 governments can lay the foundation for a just, prosperous, and truly shared global economy.

G20 Insights

“Often referred to as “the Internet of Value”, **blockchains also hold the key to integrating other emerging technologies** identified by the G20’s Blueprint for Innovative Growth as ushering in a “New Industrial Revolution” (NIR, also known as “Industry 4.0”). These include innovations such as **“the Internet of Things (IoT), Big Data, cloud computing, Artificial Intelligence (AI), robotics, additive manufacturing, new materials, augmented reality, nanotechnology and biotechnology.”** Since blockchain technologies promise to be the glue that binds the NIR together, the G20 countries must take the lead in forging effective technology-regulatory synergies for blockchain as a matter of priority.”

Top 10 Disruptive Technology Trends for 2017 – Gartner

AI and Advanced Machine Learning

Intelligent Apps

Intelligent Things

VR and AR

Digital Twin

Blockchain and Distributed Ledgers

Conversational System

Mesh App and Service Architecture

Digital Technology Platforms

Adaptive Security Architecture

Top 10 Emerging Technologies of 2016 – World Economic Forum

Nanosensors and the Internet of
Nanothings

Next Generation Batteries

The Blockchain

Two Dimensional Materials

Autonomous Vehicles

Organs-on-chips

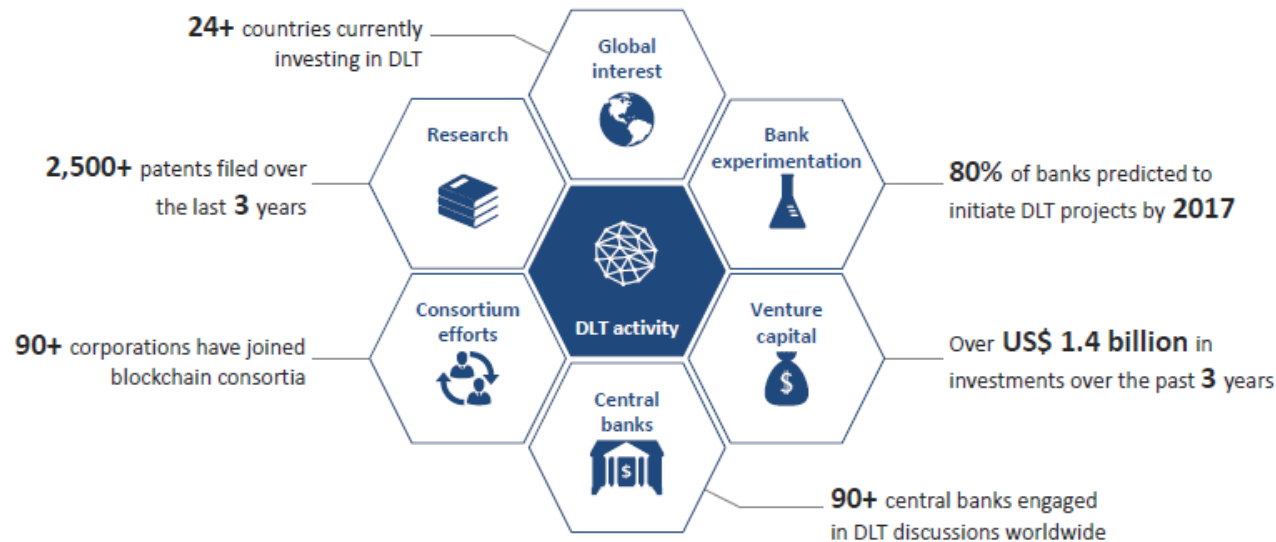
Perovskite Solar Cells

Open AI Ecosystem

Optogenetics

Systems Metabolic Engineering

Distributed ledger technology (DLT), more commonly called “blockchain”, has captured the imaginations, and wallets, of the financial services ecosystem



Awareness of DLT has grown rapidly, but significant hurdles remain to large-scale implementation



An uncertain and unharmonized regulatory environment

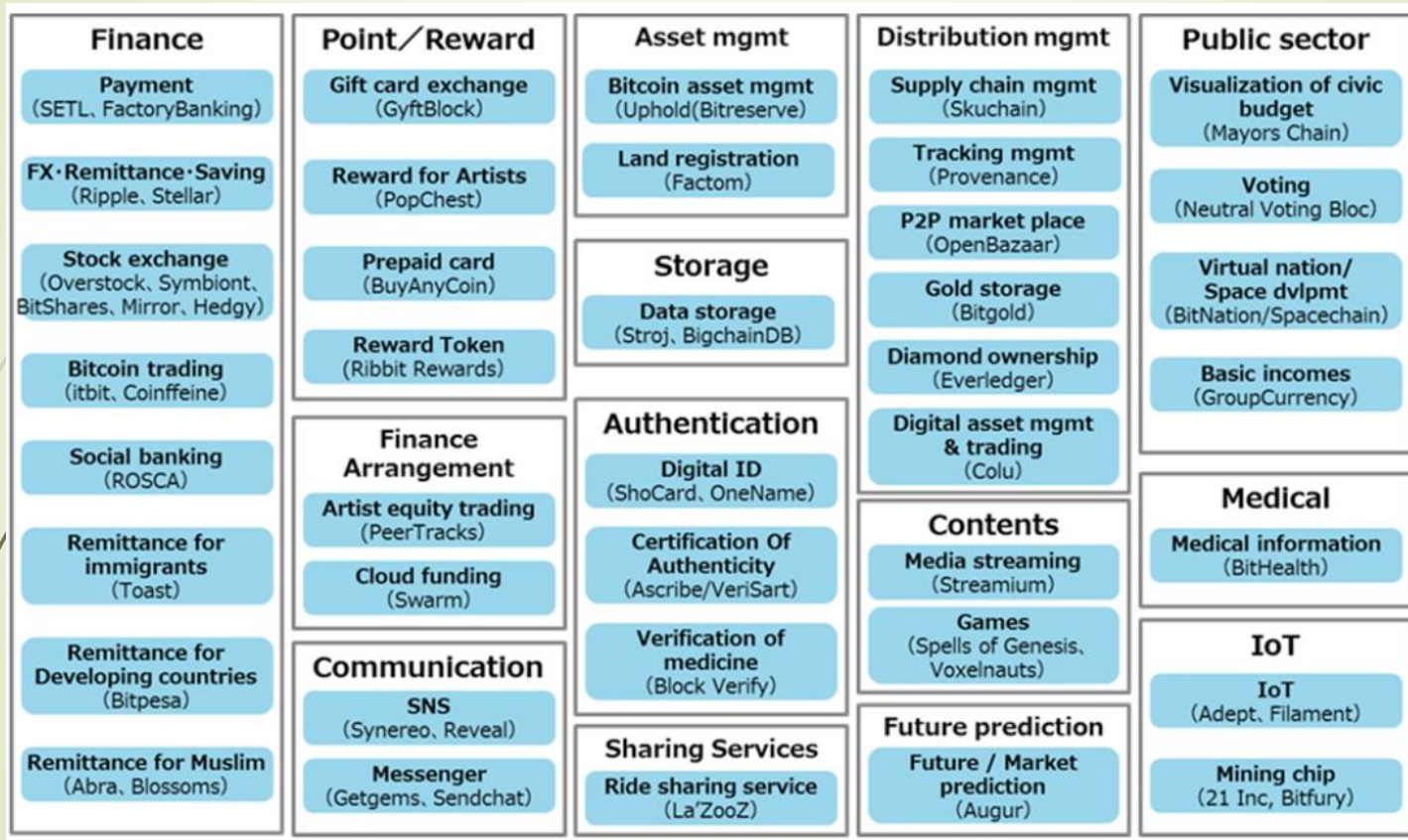


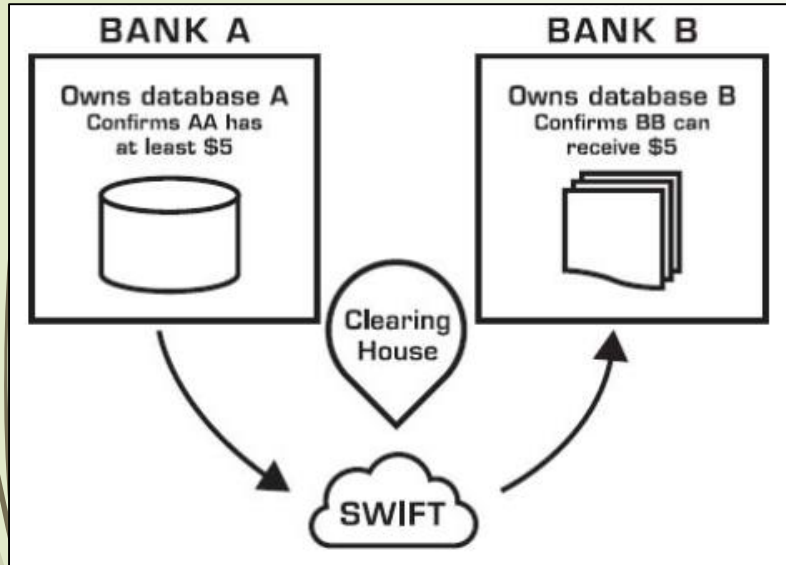
Nascent collective standardization efforts



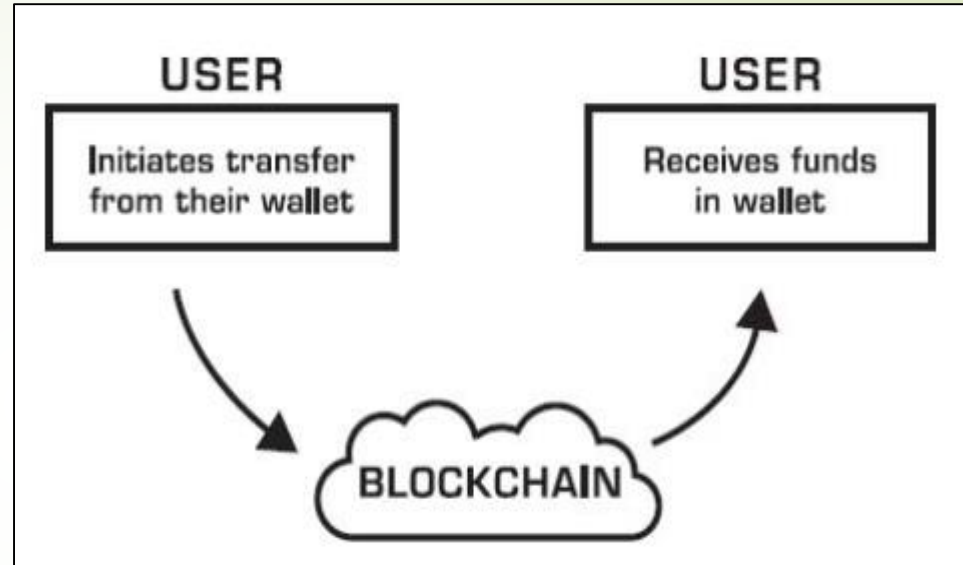
An absence of formal legal frameworks

Some Use Cases and Services of Blockchain (As of End – 2015)





Current funds transfer – Two banks have two separate databases which updates via clearing house.

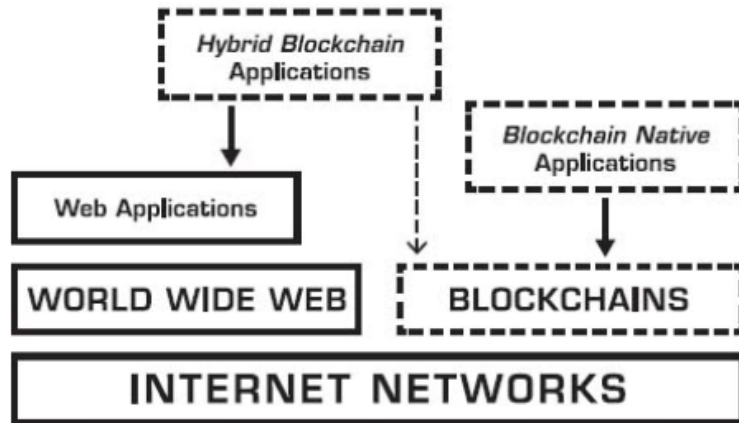


Blockchain contains one version of truth with users transacting directly via Blockchain.

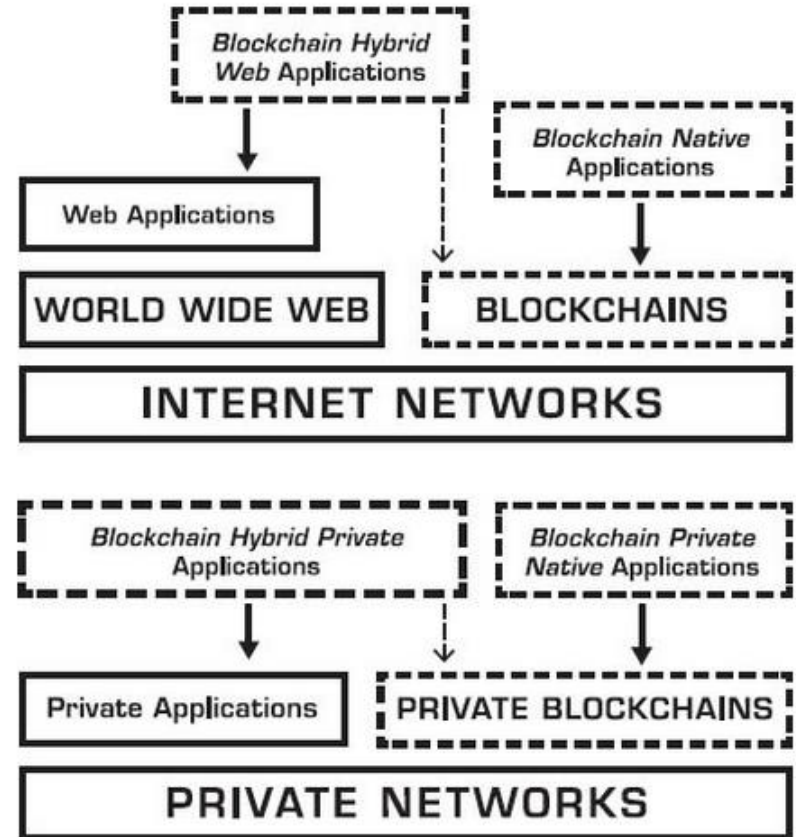
BLOCKCHAINS, LIKE THE WEB,
NEED THE INTERNET



FLAVORS OF BLOCKCHAIN APPLICATIONS



FOUR TYPES OF
BLOCKCHAIN APPLICATIONS



Source : The Business Blockchain, Promise, Practice and
Application of the Next Internet Technology by William Mougayar

INTRODUCTION TO BLOCKCHAIN AND ITS DISRUPTIVE POTENTIAL

BITCOIN AND BLOCKCHAIN HIGHLIGHTS

Bitcoin and Blockchain Highlights

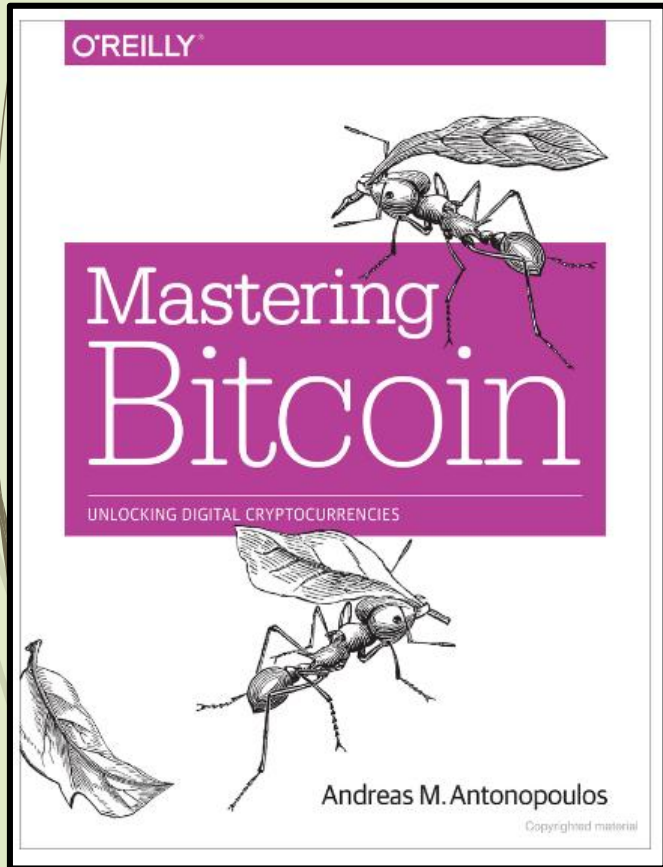
- ❖ To understand Blockchain, we have to understand the origin of it in Bitcoin.
- ❖ Bitcoin system originated from a person or persons known by the identity Satoshi Nakamoto who produced a paper titled “Bitcoin: A Peer-to-Peer Electronic Cash System” in 2008 and produced the open source code for such a system.
- ❖ Bitcoin is a cryptocurrency and bitcoins are ‘generated’ as a reward to nodes that solve a “proof of work” mathematical problem to add blocks containing a group of validated transactions to the chain of blocks. (Note that the term “blockchain” does not exist in Satoshi’s paper but the paper mentions about blocks and chains.)
- ❖ Industry observers and strategists have noted that beyond Bitcoin, it is the Blockchain underlying technology that holds promise for far wider use including commerce, government services and Internet of Things (IoT).
- ❖ Blockchain technology reduces or eliminates the need for a central trusted party or intermediaries to “facilitate” transactions (financial, contracts, ownership, identities etc). Intermediaries include some functions in banks, stock exchanges, government and notaries.
- ❖ Blockchain has of late been an overused term and some solutions out there may not actually be Blockchain based solutions. However it is noted that there is no common definition of Blockchain agreed as yet. Hence the need for standard definition.

Bitcoin Characteristics

- ❖ Each bitcoin or part of a bitcoin is associated to an owner by digital signatures (public and private keys). Important : If the owner does not back up his private key and he loses the private key, his bitcoin is lost forever.
- ❖ What **character or category** bitcoin is in depends on the **eyes or perception** of the people looking at it, or in some cases, the jurisdictions (government regulators) that define it.
- ❖ Hence to some people:
 - ❖ Bitcoin is a (crypto)currency where people use it to buy and sell goods, or
 - ❖ Bitcoin is a commodity like gold, whereby the price fluctuates depending on supply and demand and people buy and sell bitcoins with that expectation and risk in mind, or
 - ❖ Bitcoin is an asset like real estate*

* Note : Israel defined bitcoin as a taxable asset. <https://www.cryptocoinsnews.com/israel-tax-authority-deems-bitcoin-taxable-asset/>

Recommended Reference for Bitcoin



“Mastering Bitcoin”* - A good reference for those who want to know the internals of the Bitcoin system.

The author Andreas Antonopoulos was in Technology Park Malaysia on 22nd February 2017 to give a talk.

INTRODUCTION TO BLOCKCHAIN AND ITS DISRUPTIVE POTENTIAL

TECHNOLOGIES USED IN BITCOIN

Blockchain Technology Bases

Blockchain is based on established technologies, cleverly integrated resulting in a robust solution that essentially eliminates reliance of trust on specific entities, but essentially assigns **trust** to the community at large having the Blockchain. The established technologies are:

- ❖ **Distributed Databases**
 - Database of Blocks of Transactions that are Timestamped
- ❖ **Cryptographic Tokens**
 - Public Key Infrastructure (Public and Private Keys)
- ❖ **Cryptographic Hash algorithms**
 - Like a signature for a text string or data file
- ❖ **Peer to Peer Architecture**
 - Every node is a client and server
- ❖ **Consensus Mechanism**
 - Agreement on what event or transaction happened and when and collectively endorse them
- ❖ **Programming Language**
 - Ability to program activities eg if-then-else etc (limited applicability to Bitcoin system)

Cryptographic Hash Algorithm

Cryptographic hash algorithm is widely used in Bitcoin Blockchain.

The SHA (Secure **Hash** Algorithm) is one of a number of cryptographic **hash** functions. A cryptographic **hash** is like a signature for a text or a data file.

SHA-256 algorithm is used in bitcoin and generates an almost-unique, fixed size 256-bit (32-byte) **hash**. **Hash** is a one way function – it cannot be decrypted back.

Input	SHA-256	Hash
The quick brown fox jumps over the lazy dog	>	d7a8fbb307d78094 69ca9abcb0082e4f 8d5651e46d3cdb76 2d02d0bf37c9e592
The quick brown fox jumps over the lazy dog.	>	ef537f25c895bfa7 82526529a9b63d97 aa631564d5d789c2 b765448c8635fb6c

Use of Hash Function in Bitcoin

❖ Bitcoin Transaction

- ❖ Producing the public bitcoin address by hashing the public key.
- ❖ Producing a transaction digest for use as the input in signing a transaction.

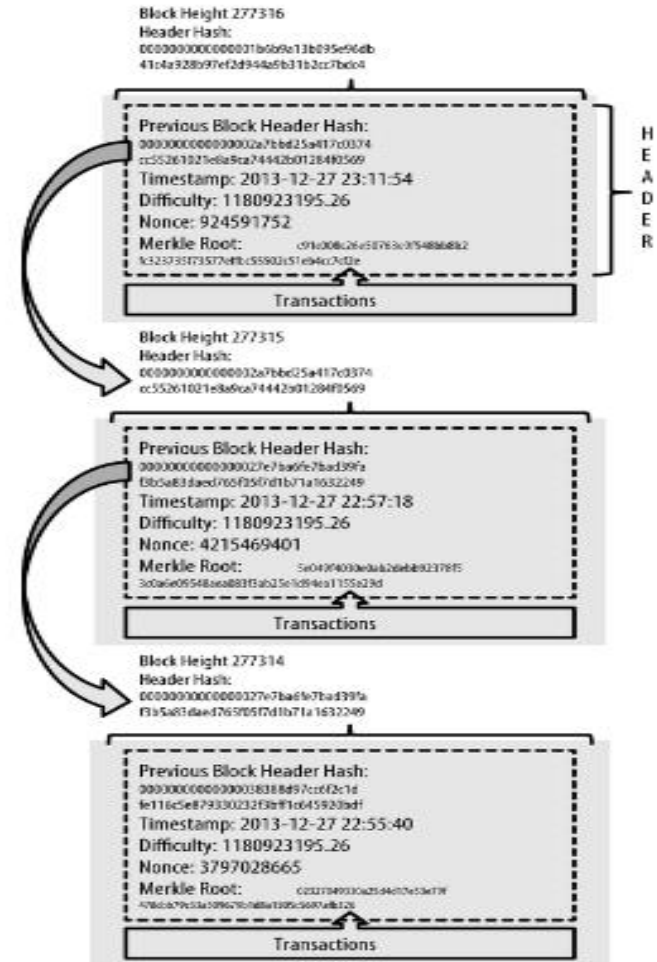
❖ Block Creation

- ❖ Producing the Merkle tree root for authenticating the transactions in a block (using hashes all the way up the tree).
- ❖ Producing the hash of the previous block to use in the block header.
- ❖ Producing the double hash of the block (with nonces) to find a block that satisfies the difficulty needed in mining.

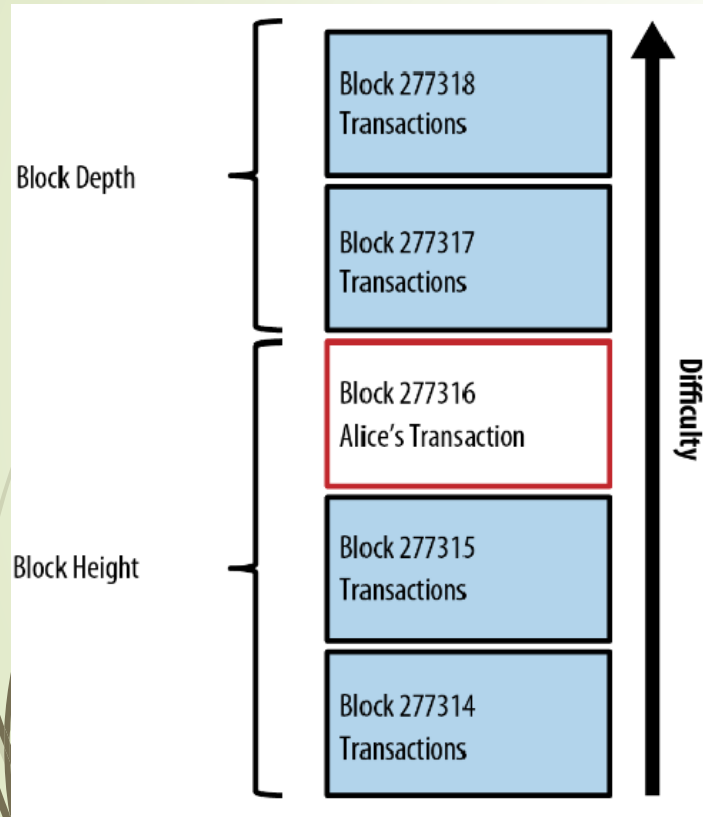
INTRODUCTION TO BLOCKCHAIN AND ITS DISRUPTIVE POTENTIAL

***CHAINING OF BLOCKS, IMMUTABILITY AND
DISTRIBUTED DATABASES***

Blocks linked in a chain by reference to the previous block header hash



Block Height and Transaction Immutability

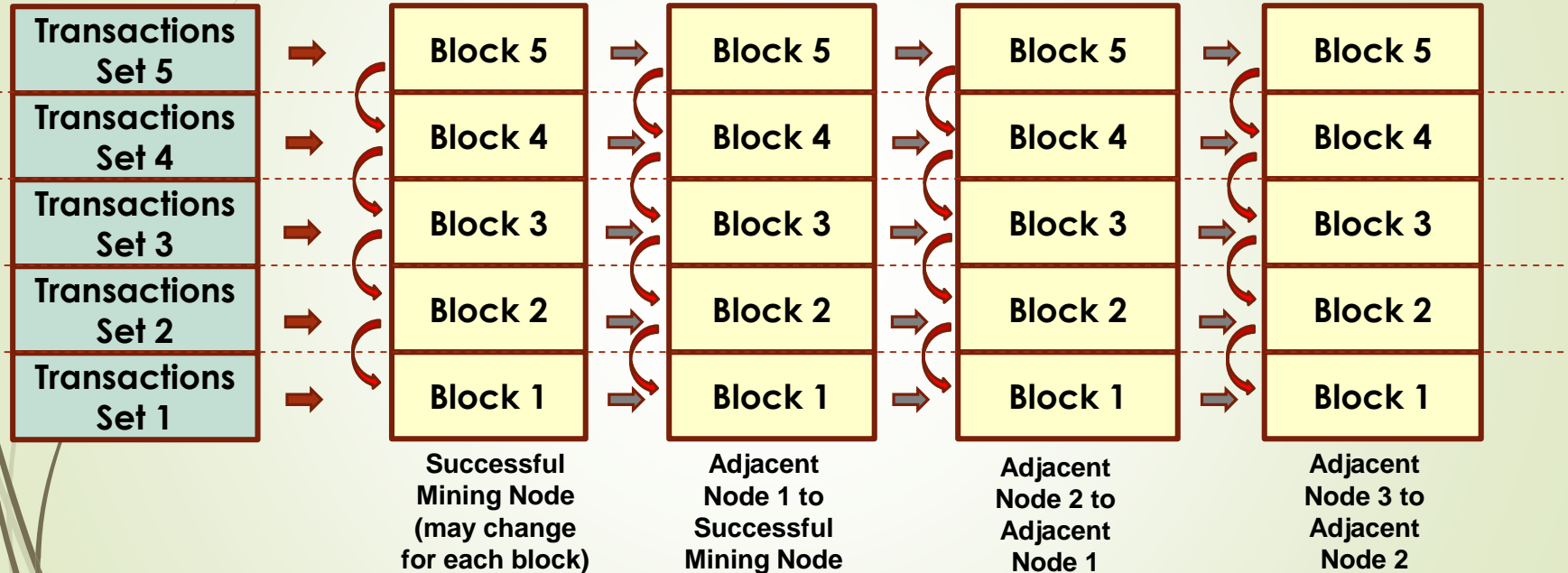


1. Blocks are normally referenced from their Block height number, ie how many blocks from the first block created in 2009.
2. Block depth is the depth of the Block of Interest (which contains Alice's Transaction) from the latest Block.
3. The deeper a particular block is from the latest block, the more difficult it is to alter the transactions in that Block.
4. **This does not mean that the later Blocks are easier altered.** This illustration just explains that it is relatively more difficult to alter (double spend etc) the transactions as we go deeper in the earlier chain of Blocks.
5. This makes the records '**immutable**' or **cannot be modified after creation.**

Bitcoin, Blockchain and Distributed Ledger

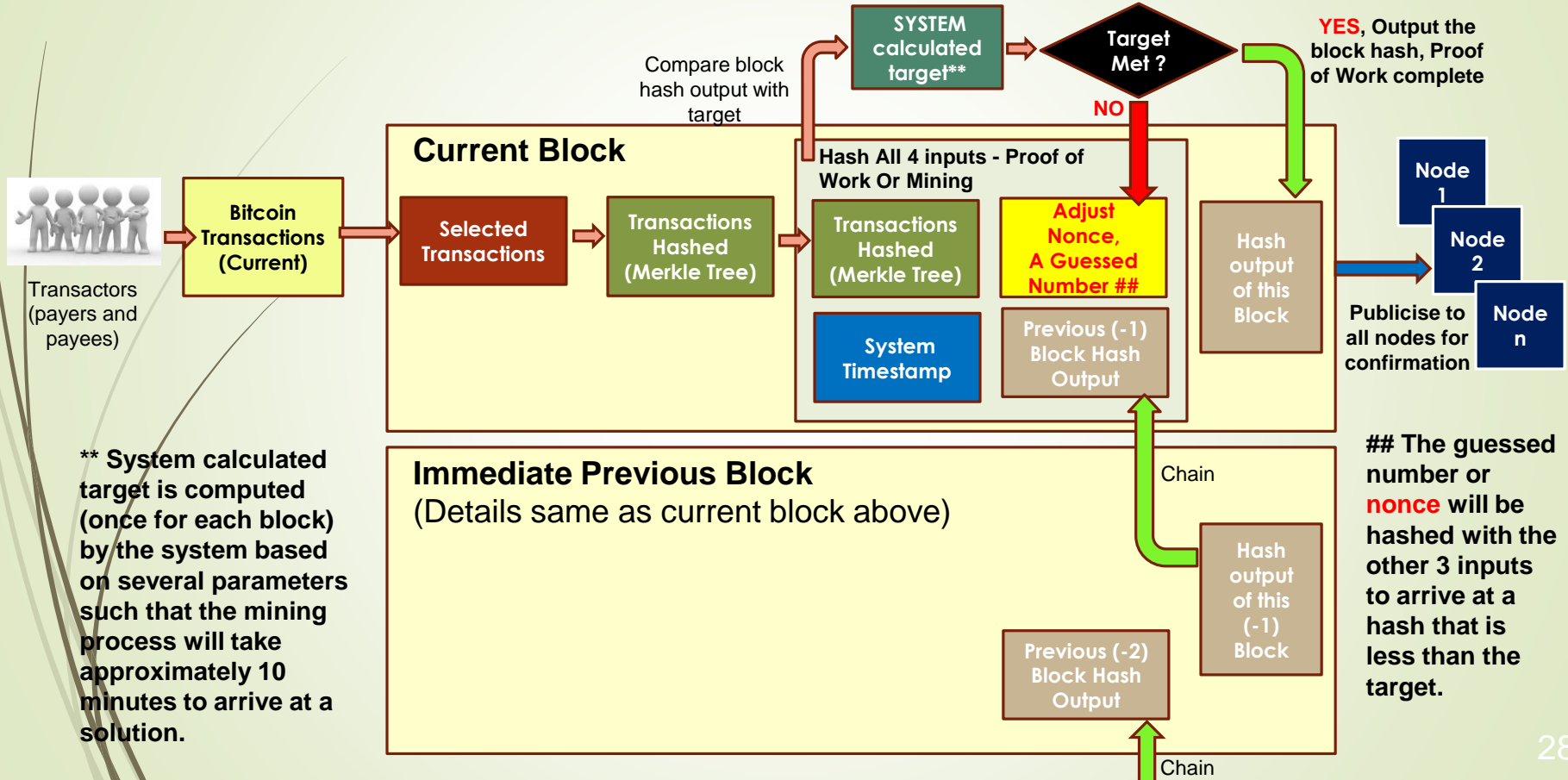
- In this presentation, the term '**Blockchain**' is taken to mean '**Blockchain AND Distributed Ledgers**'

All Blockchain and Mining Nodes will get a copy of the transactions



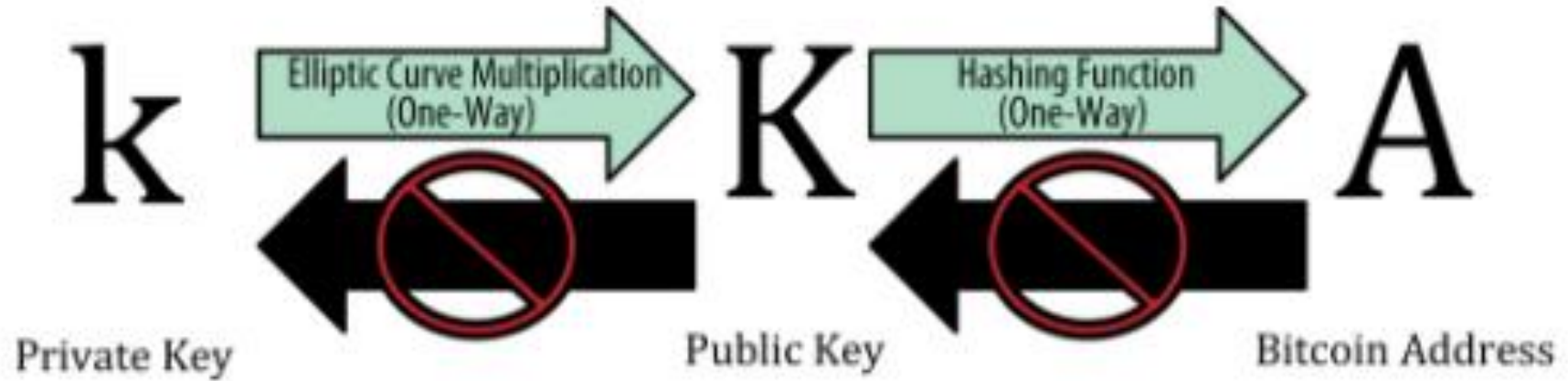
Blocks information from successful mining node are verified and 'assembled', as information on successfully mined block is passed to adjacent nodes and so on. Improper (unverifiable, non compliance etc) block information will not be passed to adjacent nodes for block formation.

Block Generation and Block Chaining Overview



Private Key, Public Key and Bitcoin Address Relationship

Transaction Level Security



Recipient of Bitcoin uses Private Key, Public Key and Bitcoin Address to ensure receipt of Bitcoins from the sender of the Bitcoins. The Private Key can generate the Public Key but from Public Key, the Private Key cannot be derived.

The Bitcoin Address (which is conveyed to the sender of Bitcoin) is derived from the Public Key. However the Public Key cannot be derived from the Bitcoin Address.

These are main security features **at the transaction level**.

Blockchain Block Hash Header Target

At the time of writing, the network is attempting to find a block whose header hash is less than `0000000000000004c296e6376db3a241271f43fd3f5de7ba18986e517a243baa7`. As you can see, there are a lot of zeros at the beginning of that hash, meaning that the acceptable range of hashes is much smaller, hence it's more difficult to find a valid hash. It will take on average more than 150 quadrillion hash calculations per second for the network to discover the next block. That seems like an impossible task, but fortunately the network is bringing 100 petahashes per second (PH/sec) of processing power to bear, which will be able to find a block in about 10 minutes on average.

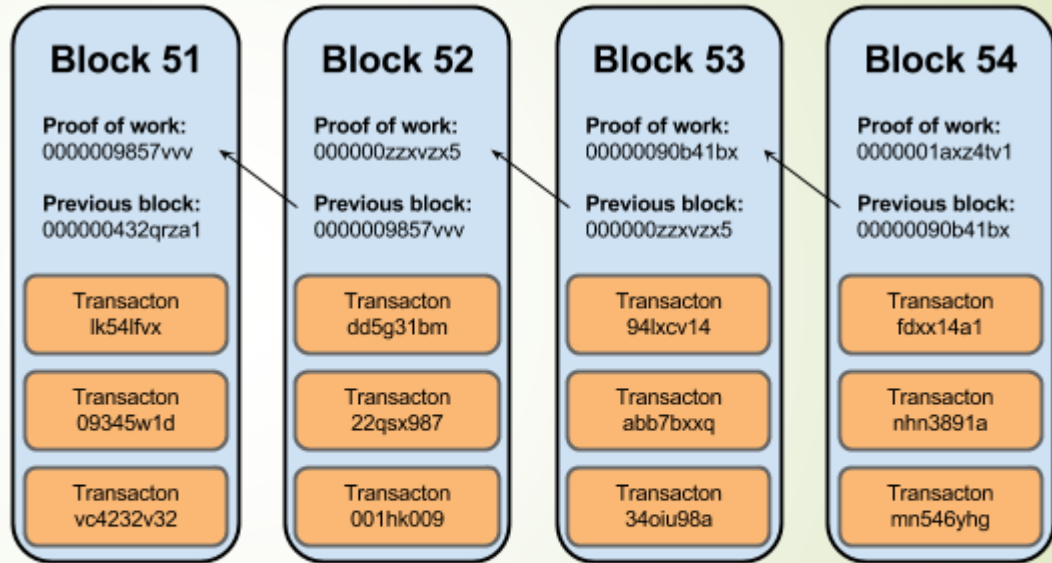
Blocks Linkage In a Chain (Blockchain) Through Proof of Work

The **Proof of Work** is a computationally intensive process called **mining** and all mining nodes will 'race' to generate the proof of work block after block.

After a block is formed resulting from a successful proof of work effort (and communicated to other nodes to accept/confirm the block), it would become very difficult for earlier transactions in earlier blocks to be altered, hence assuring its security (integrity or immutability).

Miners who successfully completed Proof of Work will be rewarded with 12.5 bitcoins and transaction fees.

Note : Alternatives to Proof of Work in some other Blockchain solutions are **Proof of Stake** and **Proof of Importance**.

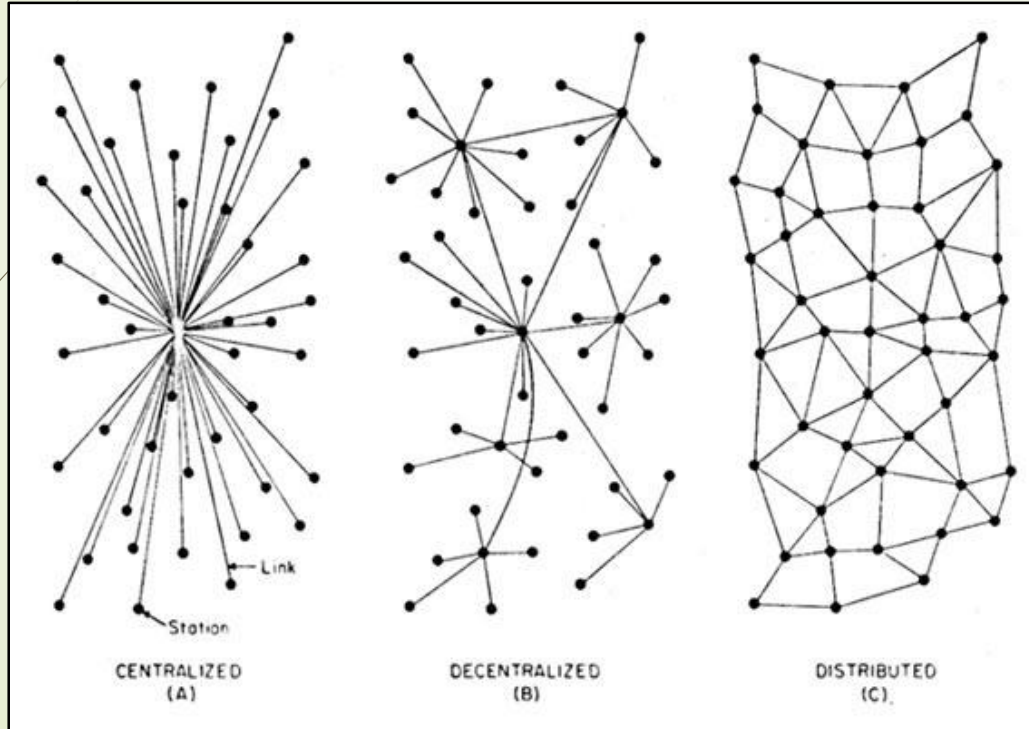


more secure

less secure

Blocks are "more secure" as you go further back in the chain

Centralized, Decentralized and Distributed Databases or Data Storage



Blockchain is stored distributed across many nodes hence 'distributed ledger', unlike most databases today which are centralized. The blockchain in each node is generated based on information publicised from the successful mining node.

Summary of Transaction Immutability Through Blockchain

- ❖ Each mining node verifies transactions and uses previous block header hash and timestamp before it starts mining.
- ❖ Mining nodes will mine concurrently to solve a 'mathematical problem' (each with its own set of transactions which may vary from other nodes).
- ❖ The node that first successfully mined (that solves the mathematical problem) and create the block, will relay its block information (transactions, previous block header hash, timestamp and mathematical solution called 'nonce') to the adjacent node.
- ❖ The adjacent node will verify that all the information provided by the successfully mined node is correct before creating its block and relaying the same information to other adjacent nodes.

Summary of Transaction Immutability Through Blockchain (contd)

- ❖ In the event that information from the sending node is incorrect (transactions invalid or double spending attempted etc) the receiving node will reject and will not create the block and will not relay the information to other adjacent nodes.
- ❖ Thus immutability is assured through block creation (linking earlier blocks) and distributed databases in blocks in adjacent nodes.
- ❖ The system assures trust without relying on a single party.
- ❖ As there are over 6000 nodes, it is unlikely that immutability will be compromised.
- ❖ This is the core strength and attractiveness of the Blockchain (with Distributed Ledger) that caught the attention of many observers.

Other Blockchains

- ❖ There are other Blockchains apart from those in the Bitcoin system and there are also variations in the process to create blocks in the other Blockchain solutions.
- ❖ Bitcoin's transaction layer handles cryptocurrency transfers.
- ❖ The transaction layer is used by other Blockchain solutions for uses other than cryptocurrency processing eg identity, property titles, logistics etc.
- ❖ The common denominator with all Blockchain solutions with Distributed Ledger is that the Blockchain provides an inherent trust mechanism and immutability of data without intervention of current trusted parties like banks.

Problems Addressed Through Blockchain

- ❖ Double spending will be prevented as the nodes will reject it if immediately communicated to them.
- ❖ Due to the aggregation of transactions by different miners, two new blocks can be formed following one earlier block. This is called a fork. Each fork can 'grow' at different pace and one will be longer than the other. The shorter fork(s) will then cease to exist and all transactions will follow the longer fork. This is a self correcting feature as part of governance.
- ❖ The “Byzantine General's” problem and “Sybil Attack” will be avoided or inherently addressed.
- ❖ No one miner can supersede the majority unless he has exceptionally large computing power (which is unlikely).

INTRODUCTION TO BLOCKCHAIN AND ITS DISRUPTIVE POTENTIAL

**BLOCKCHAIN TYPES, DEFINITIONS AND
TECHNOLOGY ERAS**

Types of Blockchains

Comparison among public-type, consortium-type, and private-type mechanisms

Public	Consortium	Private
<ul style="list-style-type: none">■ Participation in a network (building a consensus and conducting mining) is open to anyone.■ Methods of building a consensus are important in order to eliminate malicious participants.	<ul style="list-style-type: none">■ A blockchain is used while building a consensus only among members who can be trusted with each other to some extent, such as members of a specific company group.■ Building a consensus is easier as participants are all identified.	<ul style="list-style-type: none">■ A blockchain is used only within a specific organization.■ Building a consensus is quite easy as the mechanism is open only to the relevant organization.

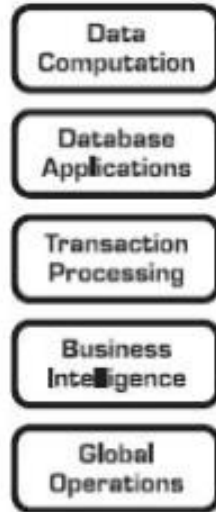
Blockchain Definitions (Several..)

- ❖ A blockchain is the public ledger of all bitcoin transactions that have ever been executed. (Swan)
- ❖ A blockchain is a type of database that takes a number of records and puts them in a block [rather like collating them onto a single sheet of paper] (UK Government Office for Science)
- ❖ A blockchain is a sequence of electronic files in which entity-linked transaction data is gathered and condensed. (Takashi)
- ❖ A blockchain is *“a technology that allows people who don’t know each other to trust a shared record of events”*. (Bank of England) This shared record, or ledger, is distributed to all participants in a network who use their computers to validate transactions and thus remove the need for a third party to intermediate. (Deloitte added)

Note : *There is no common definition of blockchain but each mentions the core elements approaching from different angles.*

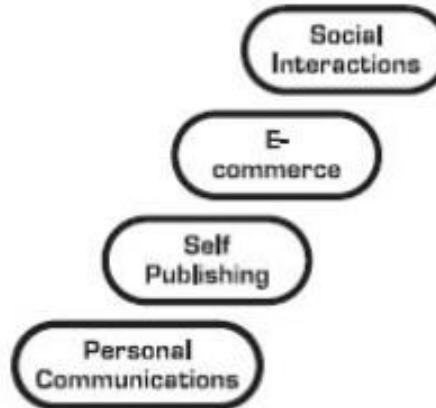
DEFINING TECHNOLOGY ERAS

IT Supremacy

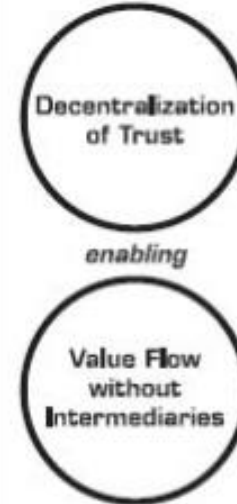


1994

Internet Years



Blockchain
Promise



2015

Decentralized Trust Using Blockchains – Seven Principles

1. It would be inaccurate to label Blockchains as a tool for a disintermediation of trust. In reality they only enable re-intermediation of trust.
2. Blockchains enable a degree of trust unbundling. The Blockchain challenges the role of existing trust players and reassigns some of their responsibilities, sometimes weakening their authority.
3. The Blockchain does not eliminate trust. It shifts it. It moves it around.
4. Trust is always needed. What changes with the Blockchain is how trust is delivered and how it is earned. Whoever earns the trust earns the relationship and that includes trusting a Blockchain.
5. The Blockchain decentralizes trust and makes way to multiple, singularly harmless, but collectively powerful entities that authenticate it.
6. The Blockchain disrupts existing economics of trust because the costs of delivering that trusts are now distributed.
7. Whereas central trust distanced us, distributed trust brings us together.

INTRODUCTION TO BLOCKCHAIN AND ITS DISRUPTIVE POTENTIAL

COUNTRY INITIATIVES, PLANS AND WHITE PAPERS

Blockchain Initiatives in Some Countries

- UK** : [Distributed Ledger Technology, Beyond Blockchain \(UK Govt Science Advisor\)](#) – Dec 2015
- Dubai** : [Dubai Claiming Position at Forefront of Blockchain Technology](#) – Aug 2016
- : [Dubai Wants All Government Documents on Blockchain by 2020](#) - Oct 2016
- Estonia** : [Blockchain-Enabled Cloud: Estonian Government selects Ericsson](#) Aug 2016
- Belarus** : [Researchers Propose Using Blockchain In E-Governance Of Belarus](#) – Oct 2016
- China** : [The Chinese Government Publishes an Official Blockchain Whitepaper](#) – Oct 2016
- : [Blockchain to Drive Wanxiang's \\$30 Billion Smart Cities Initiative](#) - Sep 2016
- Singapore** : [Singapore's Central Bank Pairs Up With R3 to Create Blockchain R&D Center](#) – Nov 2016
- : [IBM is Opening a Blockchain R&D Innovation Centre in Singapore](#) Jul 2016
- India** : [Indian IT Consultancy TCS is Developing over "100" Blockchain Projects](#) – Oct 2016
- Russia** : [Russian Central Bank Sends First Distributed Ledger Transactions](#) – Oct 2016
- Thailand** : [Thailand's KBank and IBM team on blockchain project](#) – Nov 2016
- Indonesia** : [This Emerging Tech Company Has Put Asia's Tuna On The Blockchain](#) – Sep 2016

Note: Countries in blue letters have published Blockchain position/strategic papers or plans at government or national level.

World Government Summit Report

– Feb 2017

This report hopes to bring the World Government Summit a fresh perspective on the current state of Blockchain technology. The report explores how the blockchain will drive positive changes in nearly every area of civic life over the next ten years. Both national and municipal governments will realise these benefits as they adapt and adopt these technologies to meet diverse requirements, smoothly integrating into the technological fabric which supports and serves their citizens.

The global economy may also realise real benefits as the reduced transaction costs and increased security provided by the blockchain foster innovation in the global systems of trade which support us all. Security and reliability are core requirements of future computing systems. The blockchain is a bold new innovation that will bring this reliability and trust into every walk of life.



UK Government Chief Scientific Advisor Report on Blockchain



Foreword

The progress of mankind is marked by the rise of new technologies and the human ingenuity they unlock.

In distributed ledger technology, we may be witnessing one of those potential explosions of creative potential that catalyse exceptional levels of innovation. The technology could prove to have the capacity to deliver a new kind of trust to a wide range of services. As we have seen open data revolutionise the citizen's relationship with the state, so may the visibility in these technologies reform our financial markets, supply chains, consumer and business-to-business services, and publicly-held registers.

We know there will be challenges as Distributed Ledgers mature and disrupt how we think about and store data. The UK is in a unique position to explore those challenges and help maximise the benefits to our public services and our economy. We already have world-class digital capability, innovative financial services, a strong research community and growing private sector expertise. It is vital that our key assets – including the Alan Turing Institute, Open Data Institute and the Digital Catapult – work together with the private sector and with international partners to unlock the full potential of this technology.

We are both, therefore, delighted to be jointly leading efforts in this area, and look forward to working with other departments on seizing the opportunity as well as understanding how its use can be implemented for the benefit of UK citizens and the economy.



Matthew Hancock
THE RT HON MATTHEW HANCOCK MP
Minister for the Cabinet Office
and Paymaster General

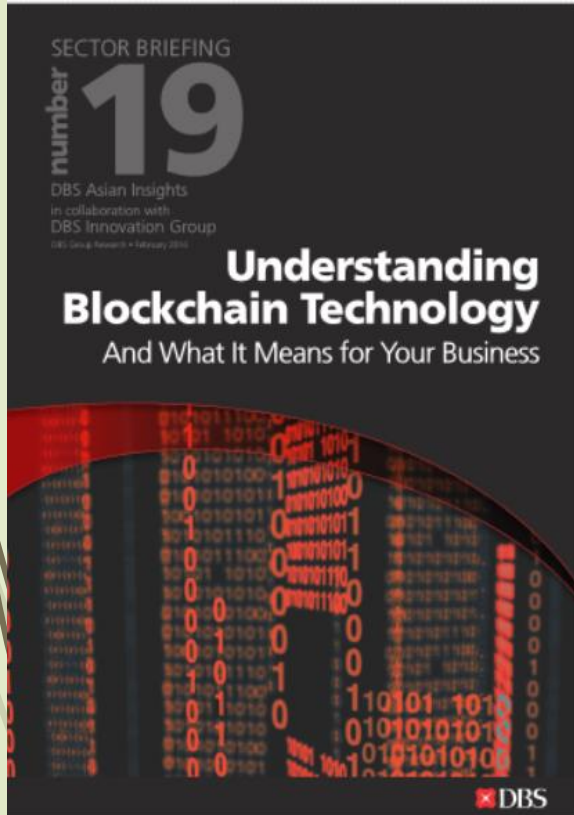


Ed Vaizey
THE RT HON ED VAIZEY MP
Minister of State for Culture
and The Digital Economy

Two UK
Ministers
jointly leading
Blockchain
efforts



Blockchain Helps Facilitate Intra Asia Trade and Capital Flows



*"We believe that blockchains have the greatest **potential to increase productivity in Asia if applied regionally**, as opposed to constrained within a country or entity."*

Before blockchains, we needed to trust entities. With blockchains, trust is assured by mathematics and systems instead. In a region where trust in entities, including companies and governments, is low, blockchains have the biggest potential for impact.

While attempts have been made to increase trade within the region, one of the biggest drags to success is low levels of trust in both businesses and political regimes. In Asia, this lack of trust has led to maintaining supply chains with known entities, where changes to the status quo are limited due to the risk of using new suppliers. New business relationships are slow to establish and often based on family ties and introductions by mutual trusted parties. By establishing digital credibility on an open system that is known to be fair and not under the influence of any politician, perhaps this can provide the lubrication that businesses need to open up."

Understanding Blockchain Technology - DBS Singapore
February 2016

China Blockchain Technology and Application Development White Paper

中国区块链技术和应用发展白皮书

(2016)

指导单位：工业和信息化部信息化和软件服务业司
编写单位：中国区块链技术和产业发展论坛

2016年10月18日发布

“The paper summarizes the Blockchain development status and trends, analysis of the core technologies and typical application scenarios, and puts forward China’s Blockchain technology roadmap and standardization roadmap and other related recommendations. ... It is hoped that all sectors work together to actively grasp the Blockchain development and trends and the laws and regulations alignment, to create a favourable environment for development and to promote China’s Blockchain technology and industrial development.”

**China Ministry of Industry and Information Technology
October 2016**



Building trust in government

Exploring the potential of blockchains

IBM Institute for Business Value
survey conducted by
The Economist Intelligence Unit

IBM Survey of 200 Government Leaders from 16 Countries



14% of government institutions

– the Trailblazers – expect to have blockchains in production and at scale by 2017.



7 in 10 government executives

expect blockchain will deliver the greatest cost, time and risk reduction benefits in regulatory compliance.



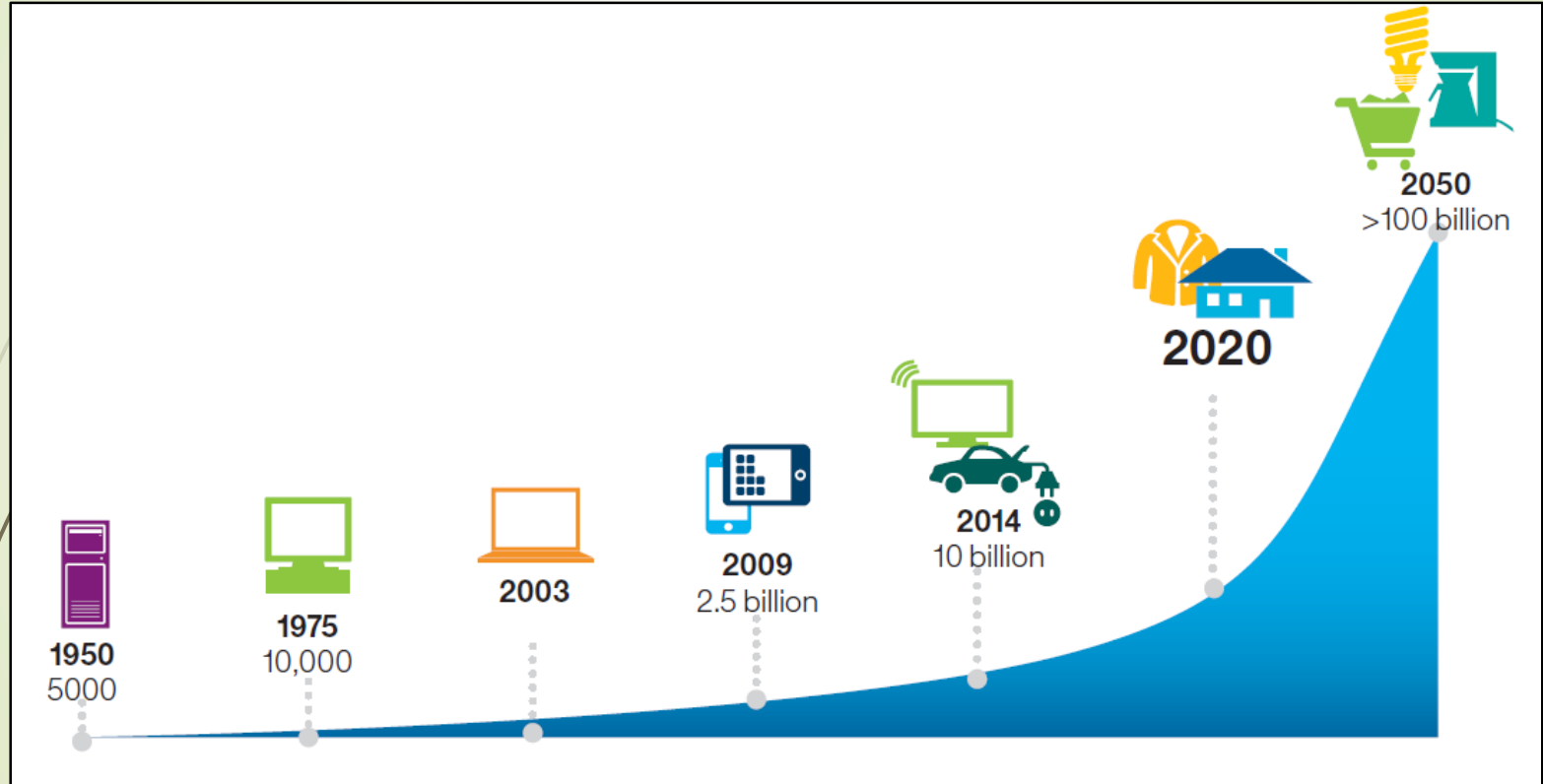
9 in 10 government executives

plan to make blockchain investments in financial transaction, asset management, contract management and regulatory compliance by 2018.

INTRODUCTION TO BLOCKCHAIN AND ITS DISRUPTIVE POTENTIAL

USE CASE - INTERNET OF THINGS (IoT)

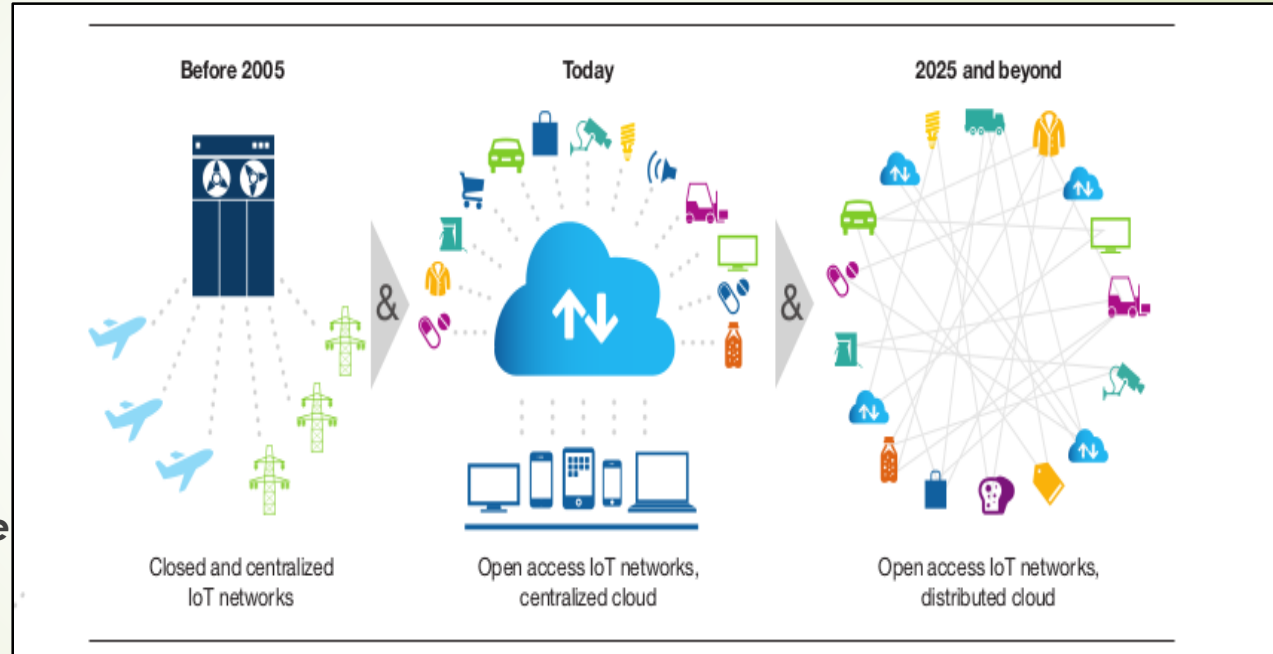
Internet of Things Devices Explosion



Source : Device Democracy – Saving the future of IoT (IBM)

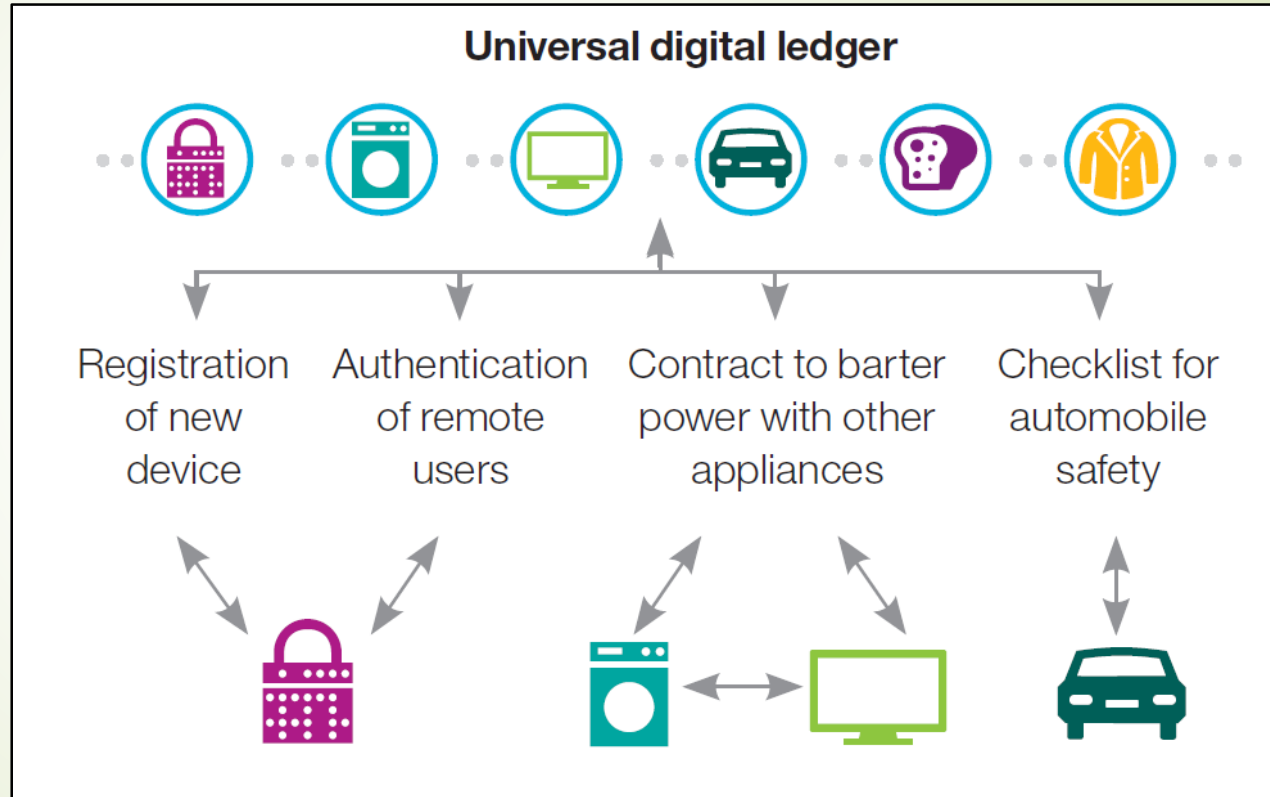
Blockchain and Internet of Things (IoT)

*'The greatest challenge, however, is not in simply building a decentralized IoT, but one that can scale universally while maintaining private, secure and trustless transactions. In other words, the IoT represents a case of billions of players, not all of which can be trusted – some even malicious – with a need for some form of validation and consensus. **And for this, the "blockchain" offers a very elegant solution.***



Blockchain and Internet of Things (IoT)

'In our vision of a decentralized IoT, the blockchain is the framework facilitating transaction processing and coordination among interacting devices. Each manages its own roles and behavior, resulting in an "Internet of Decentralized, Autonomous Things" – and thus the democratization of the digital world.'



IBM and Maersk Ready Blockchain Technology

"The technology will be made available to the shipping and logistics industry to help manage the paper trail of tens of millions of shipping containers across the world by digitizing the supply chain process from end-to-end.

It is expected to enhance transparency and facilitate secure sharing of information among trading partners. It is designed to help reduce fraud and errors, reduce the time products spend in the transit and shipping process, improve inventory management and ultimately reduce waste and cost.

When adopted at scale, the solution has the potential to save the industry billions of dollars, says IBM.

Maersk found in 2014 that just a simple shipment of refrigerated goods from East Africa to Europe can go through nearly 30 people and organizations, including more than 200 different interactions and communications among them.

The costs associated with trade documentation processing and administration are estimated to be up to one-fifth the actual physical transportation costs.

IBM and Maersk intend to work with a network of shippers, freight forwarders, ocean carriers, ports and customs authorities to build the new global trade digitization solution, which is expected to go into production later this year.

Ramesh Gopinath, a vice president at IBM told the International Business Times: "This is a solution for industry, not just Maersk. Customs and other carriers will come on and they will all be running their own blockchain nodes. That will happen as part of bringing this into production later this year."

Blockchain and IoT Possible Use Cases – Motor Insurance

“It can be fairly disruptive in the insurance space where autonomously hosted contracts can be negotiated between parties.

For example, a contract can be established between an individual and an insurance provider, where the individual agrees to drive safely. The contract itself is stored in a shared ledger (blockchain) with an initial seed value (for example Bitcoin). Subsequently the value can increase or decrease based upon the actual driving behaviour (the shared ledger is updated via telematics without any user intervention).

In essence, blockchain technologies drive us towards an on-demand (smart) contract model, where the benefit or loss to an individual is based on an individual’s actual behaviour. This simple model eliminates the bureaucratic process of creating a policy and subsequently processing the claim. In addition, since blockchains are peer-to-peer (on the Internet) there is nothing that needs to be stored or processed by the insurance company.”

Source: <http://blogs.lexisnexis.com/insurance-insights/2016/09/dispelling-some-myths-about-blockchain/>

Blockchain and IoT Possible Use Cases – Health Insurance

“Another great example would be a healthcare one. The agreement between a patient and an insurance provider could be based on the fact that a patient would walk or run two miles a day and does not smoke, and so on. To start with a seed value is established. As the individual tries to conform to the agreement (automatically updated by the tracking wearable) the value of the contract could either increase or decrease.

Undoubtedly blockchain, by whatever name or flavour it may become adopted, could play some part in the current transformation in the insurance industry. Ultimately blockchain forms a single point of truth. Digital transformation is about continually learning and adapting.”

Blockchain and Internet of Things (IoT) – Some News

- ❖ New Blockchain registry for Internet of Things using Bluetooth and NFC – Aug 2016
- ❖ IBM Invests \$200 Million in Watson IoT Blockchain Development Oct 2016
- ❖ How can blockchains improve the Internet of Things? – Oct 2016
- ❖ IBM Invests \$200M Into Blockchain and IoT Research at German Headquarters Oct 2016
- ❖ How blockchain can change the future of IoT Nov 2016
- ❖ How Blockchain Startups Will Solve The Identity Crisis For The Internet Of Things Apr 2017

INTRODUCTION TO BLOCKCHAIN AND ITS DISRUPTIVE POTENTIAL

USE CASE - SMART CITIES

Blockchain, Internet of Things and Smart Cities













One of the ways **blockchains** supports smart cities is through the **Internet of Things (IoT)**. The IoT embeds sensors into the infrastructures of environments where people live. Such sensors can be used for data-driven systems including for transport, law enforcement, and energy use, to increase both efficiency and quality of life for citizens.

An example of this sensor model is a **mobile application** that would display available parking spots in an area. In a smart city, a driver would pay a parking meter once and through the use of a **smart contract**, the meter would **auto-refill** by deducting funds from the driver's bank account, without the need of a third-party intermediary.

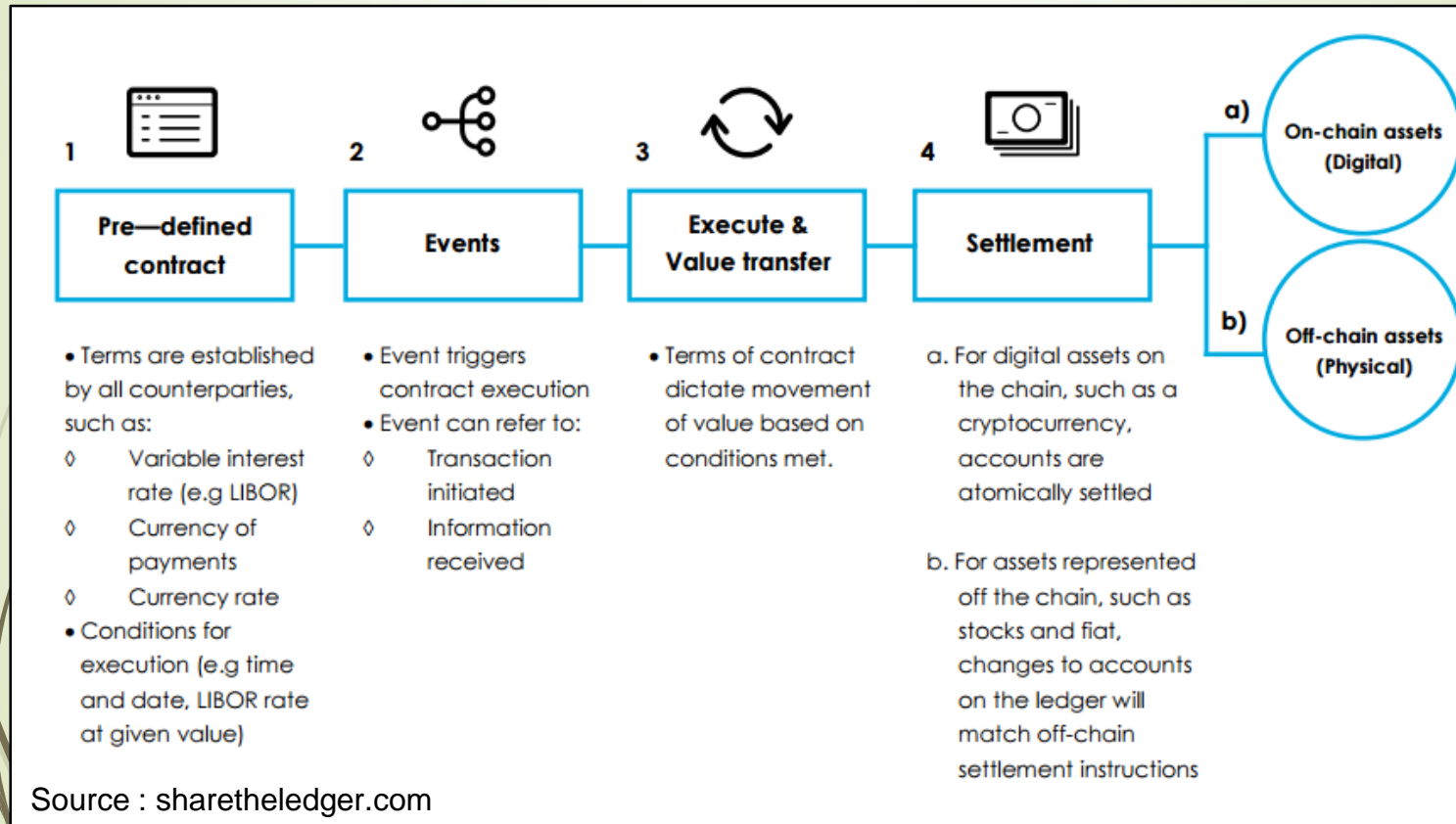
INTRODUCTION TO BLOCKCHAIN AND ITS DISRUPTIVE POTENTIAL

USE CASE - SMART CONTRACTS

Smart Contracts vs Traditional Contracts

<i>Traditional contracts</i>	<i>Smart contracts</i>
 1-3 Days	 Minutes
 Manual remittance	 Automatic remittance
 Escrow necessary	 Escrow may not be necessary
 Expensive	 Fraction of the cost
 Physical presence (wet signature)	 Virtual presence (digital signature)
 Lawyers necessary	 Lawyers may not be necessary

Smart Contracts – Possible Sequence



INTRODUCTION TO BLOCKCHAIN AND ITS DISRUPTIVE POTENTIAL

SOME ELEMENTS COMMON TO ALL BLOCKCHAIN

Some Elements Common to Most Blockchains

- ❖ A blockchain is digitally distributed across a number of computers in almost real-time: the blockchain is decentralised, and a copy of the entire record is available to all users and participants of a peer-to-peer network. This eliminates the need for central authorities, such as banks, as well as trusted intermediaries, such as brokerage firms.
- ❖ A blockchain uses many participants in the network to reach consensus: the participants use their computers to authenticate and verify each new block – for example, to ensure that the same transaction does not occur more than once. New blocks are only adopted by the network once a majority of its participants agree that they are valid.

Some Elements Common to Most Blockchains (contd.)

- ❖ A blockchain uses cryptography and digital signatures to prove identity: transactions can be traced back to cryptographic identities, which are theoretically anonymous, but can be tied back to real-life identities with some reverse engineering.
- ❖ A blockchain has mechanisms to make it hard (but not impossible) to change historical records: even though all data can be read and new data can be written, data that exists earlier in a blockchain cannot in theory be altered except where the rules embedded within the protocol allow such changes – for instance, by requiring more than 50 per cent of the network to agree on a change.

Source : Deloitte. Blockchain-Enigma. Paradox. Opportunity.

Some Elements Common to Most Blockchains (contd.)

- ❖ A blockchain is time-stamped: transactions on the blockchain are time-stamped, making it useful for tracking and verifying information.
- ❖ A blockchain is programmable: instructions embedded within blocks, such as “if” this “then” do that “else” do this, allow transactions or other actions to be carried out only if certain conditions are met, and can be accompanied by additional digital data.

Source : Deloitte. Blockchain-Enigma. Paradox. Opportunity.

ISO TECHNICAL COMMITTEE ON BLOCKCHAIN AND DISTRIBUTED LEDGER TECHNOLOGIES

ISO/TC 307

ISO – International Organization for Standardization

- **ISO is an independent, non-governmental international organization with a membership of 162 national standards bodies.**
- **Through its members, it brings together experts to share knowledge and develop voluntary, consensus-based, market relevant International Standards that support innovation and provide solutions to global challenges.**
- **ISO creates documents that provide requirements, specifications, guidelines or characteristics that can be used consistently to ensure that materials, products, processes and services are fit for their purpose.**
- **ISO has published 21582 International Standards and related documents, covering almost every industry, from technology, to food safety, to agriculture and healthcare. ISO International Standards impact everyone, everywhere.**

ISO/TC 307 Member Countries

Participating Countries (18)

Australia (SA) - Secretariat
Austria (ASI)
Canada (SCC)
China (SAC)
Denmark (DS)
Finland (SFS)
France (AFNOR)
Germany (DIN)
Ireland (NSAI)
Italy (UNI)
Japan (JISC)
Korea, Republic of (KATS)
Malaysia (DSM – TC/G/15)
Netherlands (NEN)
Russian Federation (GOST R)
Spain (UNE)
United Kingdom (BSI)
United States (ANSI)

Observing Countries (16)

Argentina (IRAM)
Belgium (NBN)
Czech Republic (UNMZ)
Hong Kong (ITCHKSAR) (*Correspondent member*)
Indonesia (BSN)
Iran, Islamic Republic of (ISIRI)
Israel (SII)
Luxembourg (ILNAS)
Netherlands (NEN)
Norway (SN)
Singapore (SPRING SG)
Slovakia (SOSMT)
South Africa (SABS)
Sweden (SIS)
Switzerland (SNV)
Thailand (TISI)

ISO/TC 307 Meeting 3-5 April 2017 in Sydney, Australia

Resolutions – Liaisons with Other Technical Committees

- ISO/IEC JTC 1 *Information Technology*
- ISO/IEC JTC 1/SC 22 *Programming languages, their environments and system software interfaces*
- ISO/IEC JTC 1/SC 27 *IT Security Techniques*
- ISO/IEC JTC 1/SC 32 *Data management and interchange*
- ISO/IEC JTC 1/SC 37 *Biometrics*
- ISO/IEC JTC 1/SC 38 *Cloud Computing and Distributed Platforms*
- ISO/IEC JTC 1/SC 40 *IT Service Management and IT Governance*
- **ISO/IEC JTC 1/SC 41 *Internet of Things and related technologies***
- ISO/TC 46 *Information and documentation*
- ISO/TC 68 *Financial services*
- ISO/TC 215 *Health Informatics*
- ISO/TC 262 *Risk management*
- ISO/TC 292 *Security and resilience*
- ISO/PC 295 *Audit data collection*
- ISO/PC 308 *Chain of custody*
- ISO/TC 309 *Governance of Organisations*

Member Organisations of Malaysian Standards Committee on Blockchain and Distributed Ledger Technologies

(TC/G/15 – National Mirror Committee to ISO/TC 307)

- Accountant General's Department of Malaysia
- Advanced Informatics School, Universiti Teknologi Malaysia
- Association Of The Computer And Multimedia Industry Of Malaysia (PIKOM)
- Bursa Malaysia
- Central Bank of Malaysia (BNM)
- Cybersecurity Malaysia
- Department of Personal Data Protection
- Federation of Malaysian Consumers Association (FOMCA)
- Fintech Association of Malaysia
- National Security Council (MKN-JPM)
- Malaysia Digital Economy Corporation (MDEC)
- Malaysia Institute of Accountants
- Malaysian Administrative, Modernisation and Management Planning Unit (MAMPU-JPM)
- Malaysian Communications and Multimedia Commission (MCMC)
- Malaysian Electronic Payment System Sdn Bhd (MEPS)
- Malaysian Industry-Government Group for High Technology (MIGHT-JPM)
- Malaysian Software Testing Board (MSTB)
- MIMOS Berhad
- Ministry of International Trade and Industry (MITI)
- Securities Commission
- The Association of Banks in Malaysia (ABM)
- TM Applied Business Sdn Bhd

INTRODUCTION TO BLOCKCHAIN AND ITS DISRUPTIVE POTENTIAL

SUMMARY

Summary

- ❖ Bitcoin, a cryptocurrency, is based on Blockchain technology. Blockchain technology is applicable to many other areas of finance, commerce, IoT and Smart Cities apart from cryptocurrency.
- ❖ Blockchain is a disruptive and emerging trend which will have far wider impact than the Internet and World Wide Web, covering all aspects of society (and not confined to finance/banking sector).
- ❖ Several countries are in various stages of study, policy development and implementation of Blockchain
- ❖ Blockchain technology eliminates the need for a central trusted party to “facilitate” transactions (financial, contracts, ownership, identities, **IoT initiated messages and actions** etc).
- ❖ G20 which covers 80% of Global GDP, 75% of world trade and two thirds of the world population has made a position with regards to Blockchain implementation for the Global Economy. All other economies will necessarily follow what the G20 countries are doing in order to continue or enhance trade and economic relations.

THANK YOU

Abdul Fattah Yatim MIEM

(0193206636, fattahyatim@gmail.com)

Useful Links

Bitcoin Information

- <https://blockchain.info/>
- <https://bitcoinmagazine.com/>
- <http://insidebitcoins.com/>
- <https://www.walletexplorer.com/>
- <https://www.blocktrail.com/BTC#>! Explorer
- <https://bitinfocharts.com/bitcoin/explorer/>
- <https://live.blockcypher.com/btc/>
- https://bitcoinchain.com/block_explorer Hash
- <http://explorer.bitcoin.xyz/> Latest transactions

Wallets

- <https://www.buybitcoinworldwide.com/wallets/#hot-wallets>

News

- <http://www.opengovasia.com/articles/7274-blockchain-and-the-public-sector---developments-in-2016>
- <http://Govinsider.asia/search/Blockchain>
- www.Coindesk.com
- <https://www.cryptocoinsnews.com/blockchain-news/>
- <https://cointelegraph.com/>
- <https://coinidol.com/blockchain/>
- <https://coincenter.org/>
- <https://btcmanager.com/news/>
- <http://www.the-blockchain.com/>
- <http://coinjournal.net/>

Thoughts on Blockchain technology

- <https://bitsonblocks.net/>
- <http://blockgeeks.com>
- <http://www.decentralstation.com/>

Hash

- <https://quickhash.com>
- <http://www.xorbin.com/tools/sha256-hash-calculator>