



Blockchain – Operator Opportunities

Version 1.0

July 2018



About the GSMA

The GSMA represents the interests of mobile operators worldwide, uniting more than 750 operators with over 350 companies in the broader mobile ecosystem, including handset and device makers, software companies, equipment providers and internet companies, as well as organisations in adjacent industry sectors. The GSMA also produces the industry-leading MWC events held annually in Barcelona, Los Angeles and Shanghai, as well as the Mobile 360 Series of regional conferences.

For more information, please visit the GSMA corporate website at www.gsma.com.

Follow the GSMA on Twitter: [@GSMA](https://twitter.com/GSMA).

About the GSMA Internet Group

The GSMA Internet Group (IG) is the key working group which researches, analyses and measures the potential opportunities and impacts of new web and internet technologies on mobile operator networks and platforms. We maintain the most up-to-date knowledge base of new internet and web innovations through intelligence gathering of available global research and active participation in key Standards organisations.

www.gsma.com/workinggroups

Authors:

Peter Ajn Vanleeuwen, KPN

Douwe van de Ruit, KPN

Contributors:

Dan Druta, AT&T

Axel Nennker, Deutsche Telecom

Shamit Bhat, GSMA

Rinze Cats, KPN

Kaissar Jabr, Monty Holding

Table of Contents

Blockchain – Operator Opportunities	1
Version 1.0	1
1 Introduction	6
1.1 Overview	6
1.2 Scope.....	6
1.3 Definitions.....	7
1.4 Abbreviations.....	8
1.5 References.....	8
2 Blockchain explained	9
2.1 Blockchain background.....	9
2.2 Blockchain characteristics	9
2.2.1 Distributed Database.....	10
2.2.2 Distributed Ledgers	10
2.2.3 Blockchain.....	10
2.3 Blockchain progress.....	11
2.3.1 Fundamental functional properties.....	12
2.4 Blockchain technical explanation.....	13
2.4.1 The Blockchain ‘protocol’.....	13
2.4.2 Blockchain ledger infrastructure.....	13
2.4.3 Transactions.....	15
2.5 Cryptography & Hashing.....	15
2.5.1 Consensus	15
2.5.2 Smart Contracts.....	16
3 The promise of blockchain technology	17
3.1 Cryptocurrency and blockchain	17
3.2 Blockchain applications in other industries.....	18
3.3 The blockchain ecosystem.....	19
4 Operator Business Opportunities	20
4.1 5G Technology and connectivity.....	20
4.2 IOT Connectivity	21
4.3 Fraud prevention.....	21
4.4 Wholesale roaming & interconnect, billing and charging for Mobile Operators.....	22

4.5	Charging for Hotspot and Mobile Operators	22
4.6	Re-selling fixed-line access through Wi-Fi access	23
4.7	Distributed ledger & blockchain network hosting	23
4.8	Supply Chain Management and Purchase to Pay processes	23
4.9	Self-sovereign Identity & Mobile Connect	24
4.10	Blockchain consumer services	25
4.11	IOT	25
4.12	Content distribution	25
4.13	Crypto-Wallets	25
4.14	Smart cities	26
4.15	Advertising	26
5	Business rationale for investing in blockchain	27
5.1	Blockchain applicability	27
5.1.1	<i>Multiple entities are involved (organisations, departments, consumers)</i>	27
5.1.2	<i>Blockchain (sometimes partly) replaces central authority or creates trust in a previously trust-less situation</i>	27
5.1.3	<i>Auditability of processes is important</i>	27
5.1.4	<i>Information involved needs to be reliable and represents a certain value</i>	27
5.2	Strategic drivers for blockchain adoption & adaptation	28
5.2.1	<i>Timing</i>	28
5.2.2	<i>Protect current business</i>	28
5.2.3	<i>Develop new business</i>	28
5.2.4	<i>Improve core operations</i>	28
5.2.5	<i>Retain innovative edge</i>	28
6	Regulatory and Compliance Review	29
6.1	Regulation	29
6.2	Compliance/ Legal	29
6.3	Privacy and Data Protection	29
6.4	Jurisdiction for Smart Contracts	29
6.5	Blockchain auditability	30
7	Blockchain myths and challenges	30
7.1	Myths	30
7.1.1	<i>Blockchain removes the need for trust</i>	30
7.1.2	<i>Blockchains cannot be hacked</i>	30
7.1.3	<i>Every transaction in blockchain represents the truth</i>	31



7.1.4 *A blockchain is immutable* 31

7.2 Challenges 31

7.2.1 *Blockchain technology is not yet mature* 31

7.2.2 *Scalability/performance* 31

7.2.3 *Regulators respond late or insufficient* 31

7.2.4 *Control, security, and privacy* 32

7.2.5 *Integration with existing systems can be complex & expensive* 32

7.2.6 *User adoption* 32

7.2.7 *Cost & Benefits* 32

Annex A Blockchain Types and Cryptocurrency Brands **33**

A.1 Ethereum 33

A.2 Bigchain DB 34

A.3 Hyperledger 34

1 Introduction

1.1 Overview

Blockchain is a distributed ledger technology that provides a way to record and share information and value between participants of a network. Within this network, each member gets a copy of the ledger, and members validate updates collectively. The information could represent contracts, identities, transactions, and any assets that can be represented digitally. Blockchain entries are permanent, transparent, and traceable, which makes it possible for participants to view transaction historical data with a guarantee that the entries are valid and have not been modified. The distributed ledger takes the form of a series of linked blocks of data, hence the name blockchain.

Top of mind innovations for operators include: Clearing & settlement of roaming and other inter-operator services, content aggregation & delivery, wallet services, mobile money, P2P Networking & LTE direct, LTE based personal hotspot, decentralised compute services, decentralised storage, billing, personal data storage, self-sovereign identity, IOT & supply-chain management, OSS & BSS, tokenisation and trading of digital assets and Support of processing (up- and download) of transactions at protocol level.

The Blockchain protocol manages how new entries are initiated, validated, recorded and shared. Blockchain enforces policies and procedures on handling and recording the information.

Blockchain allows transactions to be securely stored and verified without any centralised authority. Instead, the data is validated by the network. Although it was originally designed for digital currency transactions, it provides a mechanism to apply decentralised consensus to a wide variety of applications. Any service which requires a method to systematically record an event (such as ownership) could potentially benefit from blockchain.

Blockchain is considered a disruptive technology because it has the potential to transform business processes across all industries: it removes the need for intermediaries and reconciliation processes because it guarantees the validity of stored data (transactions, smart contracts etc.) using shared infrastructure. When created, this data is recognised as valid by all parties, and cannot be modified afterwards without a majority vote.

1.2 Scope

The goal of this document is to review and understand the technology of blockchain and describe the possible impact this might have on the operator industry.

Blockchain could drive operator strategy to remain a relevant strategic partner for corporate and mid-market clients and build a trustworthy “one stop shop” service offering. Operators risk losing existing business in areas where blockchain might disrupt. It is therefore in our interest to research and invest in blockchain to detect opportunities and disruptions early.

Blockchain investments should support operator’s overarching goal to develop new revenue streams (external use cases), cut costs and improve control (internal use cases).

This document also describes Distributed Ledger Technology (DLT), analyses impacts DLT will have on operator strategy and explores business opportunities arising of its use.

Blockchain technology finds its roots in the world of cryptocurrencies like Bitcoin & Ether. Cryptocurrencies will be mentioned in this document but will not be compared or analysed.

1.3 Definitions

Term	Description
Auditable	Blockchain technology enables auditing the entire gamut of transactions carried out within a period under observation, thereby foregoing the need for sample based substantiation. This extensive coverage will make impacted processes more auditable.
Blockchain	Blockchain is a distributed ledger that records transactions in a verifiable and permanent way using a chain of cryptographically linked 'blocks' containing batched transactions; generally all data is broadcast to all participants in the network.
Distributed	All workloads are processed by nodes in the network.
Distributed ledger	Distributed database that assumes the possible presence of malicious users (nodes).
Decentralised	There is no central authority governing the processes.
Hash function	A one way function that takes arbitrary data as input and creates a hash string as output. It's infeasible to derive the input data from the hash, but it's easy to verify the hash if the input data is known.
Immutable	Once a valid transaction is included into a block, and the network has reached consensus about the new state of the blockchain, neither the transaction nor the block can be altered. Immutability is ensured by the hash function, binding successive blocks together, and by the consensus algorithm.
Off-chain	Process or transaction that is external to the distributed ledger.
On-chain	Process or transaction that takes place directly on the distributed ledger network.
Permissioned	Only selected parties can make changes to the distributed ledger.
Permission-less	Anyone can in theory, participate in the consensus process (in practice, however, often limited by resource requirements such as owning suitable hardware or cryptocurrency).
Smart Contracts	Blockchain technology enables Smart Contracts used for automated execution of pre-agreed contractual terms without the need of physical intermediaries or third parties.
Tamper-Proof	Resistance to tampering (intentional malfunction or sabotage) by either the normal users of a product, package, or system or others with access to it.
Tokenisation	Refers to the process of digitally representing an existing, off-chain asset on a distributed ledger.
Transparent	Each blockchain node or everyone with access to a node, can view all the blocks and transactions on the blockchain.



Trust-less	Blockchain is byzantine fault tolerant. Trust in honest majority to reject illegitimate transactions or blocks initiated by a malefactor replaces the trust in individual parties. This property also enables value transfer on blockchain (through elimination of potential double spending).
------------	--

1.4 Abbreviations

Term	Description
CDR	Call Data Record
CSP	Communications Service Provider
DAG	Directed Acyclic Graph
DID	Decentralised IDentity
DLT	Distributed Ledger Technology
EEA	Enterprise Ethereum Alliance
ETH	Ethereum Coin
KYC	Know Your Customer
MNO	Mobile Network Operator
POS	Point of Sale
W3C	World Wide Web Consortium

1.5 References

Ref	Title
[1]	Bitcoin: A Peer-to-Peer Electronic Cash System – Satoshi Nakamoto
[2]	How to timestamp a digital document - Haber & Stornetta
[3]	The risks and rewards of blockchain technology – Katherine Heires
[4]	The truth about blockchain - Iansiti & Lakhani
[5]	Why business schools need to teach about blockchain - Bheemaiah
[6]	IOTA - IOTA actually isn't a blockchain solution but instead uses a distributed ledger technology called a DAG or Directed Acyclic Graph
[7]	Avoiding the pointless blockchain project
[8]	When do you need blockchain – decision models
[9]	Zooko Triangle
[10]	At the time of writing, the W3C is working on a specification for digital identities (DID) , currently in version 0.9.

2 Blockchain explained

2.1 Blockchain background

The idea of a chain of blocks connected by a hash function was formulated by Haber & Stornetta (1991) [2] more than 25 years ago, but there was no production-ready application of this technology until 2008, when a person or group of people with the pseudonym Satoshi Nakamoto conceptualised blockchain in the whitepaper “Bitcoin: A Peer-to-Peer Electronic Cash System” (Nakamoto, 2008) [1]. Bitcoin is an example of the first generation blockchain.

While blockchain is placed by Gartner (2016) at the Peak of Inflated Expectations with the Plateau of Productivity expected to be reached by 2021 - 2026, it already deserves attention from tech experts and business executives as a technology with “disruptive,” “transformative” and even “revolutionary” power (Heires, 2016) [3].

Blockchain is commonly compared with another disruptive technology: the internet (TCP/IP). Two examples are given below:

- “The parallels between blockchain and TCP/IP are clear. Just as e-mail enabled bilateral messaging, Bitcoin enables bilateral financial transactions.” - Iansiti & Lakhani (2017) [4].
- “Today, the Blockchain protocol is following a similar path of evolution with one major difference. Just as TCP/IP and HTTP are protocols of communication, the Blockchain is a protocol of value exchange” - (Bheemaiah, 2015) [5].

2.2 Blockchain characteristics

Blockchain is a decentralised distributed ledger technology (DLT) which is immutable and enables asset value storage, exchange and business rules based autonomous transaction processing.

Blockchain may also be referred to as a distributed database:

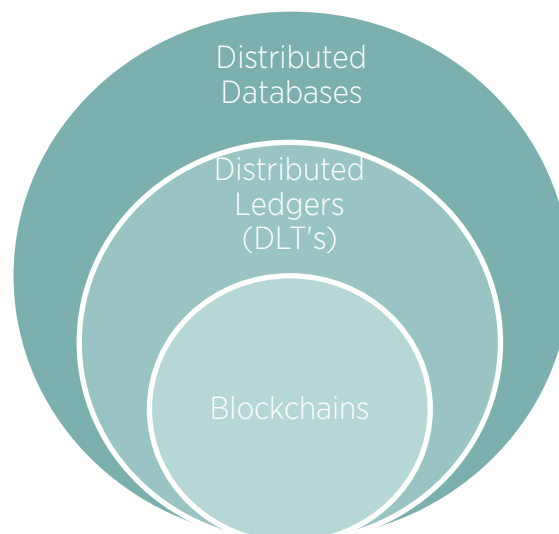


FIGURE 1: BLOCKCHAIN AS A DECENTRALISED DATABASE

2.2.1 Distributed Database

A distributed database has no central master database node that acts as the authoritative source. Rather the nodes are replicated through the network and collaborate to maintain a consistent state of records on all nodes. A distributed database scenario requires a mutual trust between database-node owners. This means that distributed databases are generally operated by a single entity that maintains strict access control of the network, residing in a trusted environment. The assumption here is that all nodes are honest.

2.2.2 Distributed Ledgers

Distributed Ledgers are a subset of distributed databases that use a different assumption about the relation between nodes/node owners. Their design is based on an adversarial threat model that mitigates the presence of malicious (i.e., dishonest) nodes in the network. They are designed to be Byzantine fault-tolerant, meaning that the database should be able to synchronise and run even if a certain number of nodes are acting maliciously. As opposed to traditional distributed databases, individual nodes do not trust their peer nodes by default and thus need to be able to verify and validate transactions that update the actual state of records.

2.2.3 Blockchain

Blockchain takes the approach of Distributed Ledgers, while *adding* characteristics that make them unique. In the Enterprise blockchain industry there is no single definition of a blockchain. However, the following key blockchain characteristics are generally applicable:

1. **Cryptography:** a wide variety of cryptographic functions are used including hashing algorithms
2. **Peer to peer:** consist of a peer to peer discovery and synchronisation mechanism
3. **Consensus:** algorithms that determine the sequence and validity of transactions
4. **Ledger:** list of transactions that are bundled together in cryptographically linked blocks
5. **Validity rules:** ruleset of the network that determine what transactions are considered valid and how the ledger gets updated, etc.
6. **Crypto economics:** a combination of cryptography and economics (game theory) that makes sure all actors in a decentralised system are incentivised to remain honest.

2.3 Blockchain progress

Blockchain 1.0 (for example Bitcoin) is a single-purpose blockchain that serves as an accounting system, ergo, a ledger for registering cryptocurrency transactions in a tamperproof way.

Blockchain 2.0 (for example Ethereum) is designed to be multi-purpose. Ethereum is a decentralised platform focused on running smart contracts: applications that run exactly as programmed without any possibility of downtime, censorship, fraud or third party interference. These smart contracts are computer protocols that facilitate, verify, or enforce the negotiation or performance of some sort of agreement (for example a legal contract emulating the logic of contractual clauses or a financial contract specifying responsibilities of the counterparts and automate flows of value).

With blockchain, rather than drafting a costly, lengthy contract employing attorneys, banks or notaries, contracts might be created with a few lines of code, perhaps constructed automatically by wiring together a handful of human readable clauses. This allows for a system where transactions are provable compliant and easily auditable.

Smart contract based applications are run on a powerful shared global infrastructure that facilitates value transfers and represents the ownership of assets. This enables developers to create markets, store registries of debts or promises, move funds in accordance with instructions given long in the past (like a will or a futures contract) and many other things that have not been invented yet, all without a middle man or counterparty risk. Because smart contracts and data are shared, developers can oftentimes leverage existing smart contract solutions as building blocks for their own applications.

Ethereum was first bootstrapped during August 2014 by fans all around the world. It is developed by the Ethereum Foundation, a Swiss non-profit, with contributions from great minds across the globe, gathering 20 million USD in less than four weeks.

There are four core technological building blocks that are coordinated to enable the Ethereum decentralised platform to operate:

1. Cryptographic Tokens and Addresses: a mathematically secure unique voucher system that can act as numeraire and be used to pay for goods, services or assets, and represents a mathematically secure, pseudonymous identity;
2. Peer-to-Peer Networking: individual users connect their computers together forming a network to exchange data without a central server (both Bitcoin and Ethereum run on P2P networks);
3. Consensus Formation Algorithm: permits blockchain users to reach consensus about the current state of the blockchain. As an example, the Bitcoin blockchain reaches consensus on a global state every 10 minutes on average, whereas the Ethereum blockchain reaches consensus approximately every 15 seconds.
4. Turing Complete Virtual Machine: this software can run any computer program, being powerful enough to implement any program defined in any similarly computationally complete system (as opposed to Bitcoin, which has a virtual machine but can only run a much simpler class of programs);

In general, blockchain types differ from various permission models as illustrated below:

		Read	Write	Commit	Example
Open	<i>Public permission-less</i>	Open to anyone	Anyone	Anyone	Bitcoin, Ethereum
	<i>Public permissioned</i>	Open to anyone	Authorised Participants	All or subset of authorised participants	Ripple, Sovrin
Closed	<i>Consortium</i>	Restricted to an authorised set of participants	Authorised participants	All or subset of authorised participants	Multiple banks operating a shared ledger
	<i>Private permissioned ('enterprise')</i>	Fully private or restricted to a limited set of authorised nodes	Network operator only	Network operator only	Internal bank ledger shared between parent company and subsidiaries

FIGURE 2: TYPES OF BLOCKCHAIN

Blockchain types (fabrics) differ to a great extent and it is up to the enterprise to evaluate which solution stack best meets the organisation's needs.

2.3.1 Fundamental functional properties

The following list categorises the fundamentals of blockchain Technology.

1. Distributed / Decentralised – there is no central authority governing and maintaining the blockchain. Each full node owns a copy of the entire chain, and data is shared through a peer-to-peer network;
2. Immutable / Unalterable / Permanent – once a valid transaction is included into a block and the network has reached consensus about the new state of the blockchain, neither the transaction, nor the block can be altered. Immutability is ensured by the hash function, binding successive blocks together, and by the consensus algorithm;
3. Trust-less / Credible / Tamper-Proof – blockchain is byzantine fault tolerant. Trust in the honest majority that will reject illegitimate transactions or blocks

- initiated by a malicious or erroneous party replaces the trust needed between individual parties. This property also enables value transfer on blockchain (through elimination of potential double spending);
4. Transparent / Auditable – each blockchain node has insight into all the blocks and transactions on the blockchain. Therefore, everything transmitted to the chain is available for everyone to see.

Another concept related to transaction processing is the consensus algorithm. A non-exhaustive list of algorithms include: Proof of Work, Proof of Stake, Dedicated Proof of Stake, Proof of Authority, Proof of Elapsed Time, and Practical Byzantine Fault Tolerance. Choice of consensus approach impacts on performance of the blockchain, energy / cost efficiency, and security.

The next and final concept to take into consideration is the presence of a native

cryptocurrency. A currency could be used for mutual payment and settlement, and, particularly in the public setting, for

participation incentivising and misuse prevention (rooted in the Game theory).

2.4 Blockchain technical explanation

For better understanding of this document, reading the technical explanations detailed in this chapter is recommended.

2.4.1 The Blockchain 'protocol'

A blockchain ledger is a chain of blocks where the blocks have a transaction data-structure. The blocks are 'chained' together in a sequential way, which adds the support for a time element to the blockchain. Ordering and sequencing of new transactions is performed

every time a validated block, containing new transactions, is added to the blockchain.

Before adding a block to the blockchain, a cryptographic function adds a digital signature to the block, making it immutable and irreversibly linked to the previous block in the chain, as illustrated below.

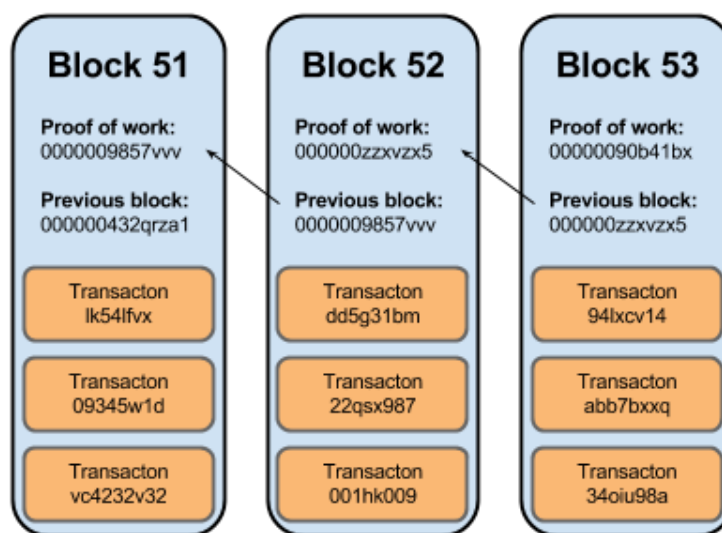


FIGURE 3: CHAINING OF BLOCKS

2.4.2 Blockchain ledger infrastructure

The blockchain is a digital ledger which runs on a distributed network of computers that maintain all operations of the blockchain protocol using P2P technology. All network nodes interconnect in a mesh network with a "flat" topology. No centralised service or hierarchy exists in the network concerning the core processes of the blockchain protocol. In the Bitcoin protocol a network node may host four core functions:

1. Routing Node - All nodes support the Routing function to validate and propagate transactions and blocks. Routing nodes also take care of discovery and maintaining connections to peers.
2. Wallet - The wallet function is used to generate key pairs and public addresses, which are used to send crypto currency or transactions to and from trusted nodes.

3. Miner - The miners compete to create new blocks by solving proof-of-work algorithms.
4. Full Blockchain Node - A full node maintains a complete and up-to-date copy of the blockchain. Full nodes can verify any transaction autonomously and authoritatively without external reference.

There are some extended functions in the Bitcoin protocol, which include the support of specialised protocols for enabling mining pools and lightweight wallet clients. In the extended protocol the following functions are identified:

1. Lightweight Wallet using SPV (simplified payment verification) - A lightweight wallet combines a Routing Node and Wallet to enable payments without the need of running a Full Blockchain Node.
2. Pool Protocol Servers - In mining pools gateway routers connect the Bitcoin P2P network to nodes running other protocols such as pool mining or Stratum nodes.
3. Pool Miners - A mining node in a pool does not hold a copy of the blockchain and contain a Stratum protocol Node or a Pool mining protocol Node.

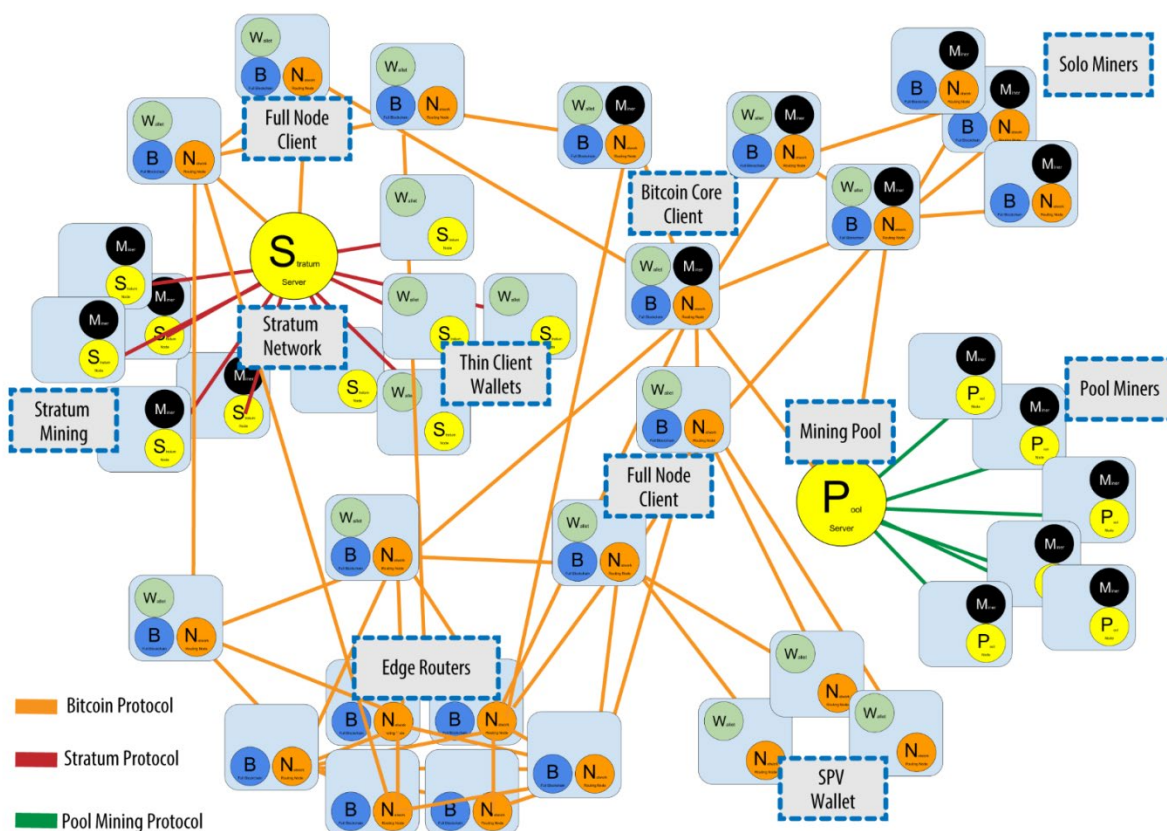


FIGURE 4: EXTENDED BITCOIN NETWORK SHOWING VARIOUS NODE TYPES, GATEWAYS AND PROTOCOLS. (SOURCE: BOOK "O'REILLY, BITCOIN & THE BLOCKCHAIN")

2.4.3 Transactions

Transactions must be signed to prove that the sender owns the referenced wallets containing unspent Bitcoin. To prevent double-spending, a transaction always references previous transaction outputs as new transaction inputs and dedicates all input values to new outputs. In this way transactions as compared to blocks

can be 'chained' as well. With this method only unspent inputs can be used to compose a balance corresponding with a public address (wallet). This illustrates the clear distinction between cryptocurrencies and the blockchain itself: where the blockchain provides a mechanism to safely record and secure a transaction history, **recorded transaction history**.

2.5 Cryptography & Hashing

Blockchain technology uses asymmetric cryptography using private and public keys to sign and validate transactions. Only the owner of a private key can sign transactions and this signature is then validated by using the associated public key.

Hash functions map data of arbitrary size to data of fixed size. The values returned by a hash function are called hash values, hash codes, or simply hashes. If any part of the data contained within a hash code is changed, then so will the hash code. Hash codes can be validated by everyone who knows the public key corresponding to the private key that was used to create the hash code. Therefore, hash codes can be used to spot changes in data (e.g. a document or program). It is used in blockchain technology to connect blocks by including a hash value of the previous block to the current block. This provides the immutability property of blockchains: any change to the contents of a block invalidates the hash of the next block, which in turn invalidates the hash of the next block, and so on.

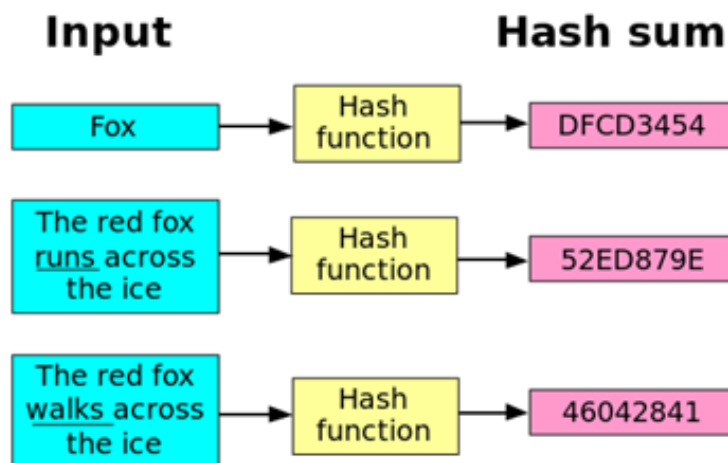


FIGURE 5: HASH FUNCTION

2.5.1 Consensus

At the infrastructure level, computers in the network will maintain a synchronised copy of the blockchain by running blockchain client

software. By installing this software the computer becomes a node in the network. The main goal of a blockchain node is to maintain consensus (or economic strength) in the network and thereby the actual state of

the blockchain as a single source of truth. The network rejects transactions and blocks, which violate the consensus rules. As examples, these are the consensus rules for Bitcoin:

- Blocks may only create a certain number of coins;
- Transactions must have correct signatures for the Bitcoins being spent;
- Transactions/blocks must be in the correct data format;
- The transaction output within a single blockchain cannot be double spent.

2.5.2 Smart Contracts

Smart contracts are a feature of Blockchain 2.0, as described in section 2.3: *Blockchain Progress*. Ethereum is the first and by far the most mature platform available, even though many new players have entered the market since its inception (for example Neo, Cardano, Nem, EOS).

Smart Contracts are small software programs that run on top of the blockchain. They are immutable as well, which makes them very well suited to capture the rules of a transactional system and guarantee its behaviour. Smart Contracts grant the ability to disintermediate in a trust-less way, allowing us to automate a broad range of business processes between cooperating and competing businesses.

Just like transactions are executed by every node in the network to collectively verify them, so are smart contracts. This guarantees valid execution of the code, but also introduces some limitations in terms of scale and size. Smart Contracts also share the immutability aspect of the data, meaning the Smart Contract cannot be changed after it is deployed on the blockchain. To rephrase this: a Smart Contract deployed at a certain address cannot be altered and will behave in the same way forever. If the underlying terms of the contract change, a new Smart Contract has to be published.



3 The promise of blockchain technology

Before operator specific opportunities and potential disruptions are addressed, a review of the implementations and general use cases that are currently known or under development is required. There are three identified general areas of disruption:

1. Efficiencies: those enabled by the disintermediation of “trusted” 3rd parties
2. New Business Models: enabled primarily from crypto-economics applications, but also by data protected by a cryptographic identity. For example tokenising customer’s digital footprint and enabling data marketplaces.
3. Customer engagement: Bounty models, and cryptographic assets related to a brand, would create a new kind of customer where they would be providers and investors at the same time

3.1 Cryptocurrency and blockchain

Both blockchain technology and cryptocurrency have enough merit to cause a serious disruption in the way day-to-day business is conducted. It is good to differentiate between and clearly define the two.

An easy way to do this is by looking at a traditional application using a database. The database can serve as a means of storage and data categorisation for a large number of applications. This is the same for blockchains, where the ledger can store any type of transaction. In the case of cryptocurrency, the ledger is used to record financial transactions between peers, making it equivalent, or at least very similar, to money.

The realisation that a cryptocurrency is only one of the actual applications that can greatly benefit from blockchain technology is what is driving the current rapid development of the blockchain ecosystem.

Therefore, there is blockchain driving innovation and reinventing business processes across industries, and a digital peer-to-peer currency as a blockchain killer-app to bring a wave of disruption. Both work on different timelines and to illustrate this, a review of the banking sector would be useful.

Financial institutions like banks were the first to realise the disruptive nature of cryptocurrencies. A blockchain backed financial transaction system that would exclude banks from partaking in a large number of transactions can indeed be disruptive, however this will not be implemented in the near future as a function in a day-to-day payment system.

Blockchain solutions however are being implemented *today*. The same financial institutions that may get disrupted by blockchain powered peer-to-peer payment systems are working on blockchain solutions to improve expensive processes involving regulation, compliance, risk management, clearing & settlement and cost reduction through efficiency.

3.2 Blockchain applications in other industries

Blockchain technology is embraced by the financial industry and now many other industries are starting to benefit from it. A wide range of applications across multiple fields are being developed, including traditional industries such as energy markets, healthcare and even public sectors. It is widely accepted amongst a large community that blockchain technology will change the way people interact, prove their Identity and do business together. It will have social and economic impact all around the world. Using a blockchain may help to:

1. Reduce the need for trust between stakeholders
2. Build a secure value exchange system
3. Streamline business processes across multiple entities
4. Increase record transparency and ease of auditability

For the Telecom sector, innovative solutions are starting to surface, mainly in the Internet of Things business. Within IOT systems, blockchain technology can provide a way to track the unique history of individual devices or device networks and enable secure, traceable and autonomous transactions using ledger technology. IOT tailored ledgers are coming, supporting instant transactions over resource limited devices and networks. These ledgers allow IOT devices to sell data using micro-transactions and enable pay per use models for a large group of IOT based services.

In a more general sense, the following is a list of notable innovation topics relating to Blockchain across a variety of industries

- P2P payments & Lending
- Currency Exchange & International Money Transfer
- Proof of authorship & ownership
- Energy distribution
- Know Your Customer & Identification (Self-Sovereign identity)
- Data storage
- Proof of authenticity for luxury goods
- Origin of components auditing
- Voting Systems
- Governance
- Prediction markets (forecasting)
- Advertising
- Loyalty
- Healthcare

In the near future, changes will occur in the way operators handle their roaming, billing, payments, data distribution and enhanced network capabilities using blockchain. It is necessary for the industry to watch the development carefully to leverage this as an innovation opportunity rather than a new wave of disruption.

3.3 The blockchain ecosystem

It is difficult to predict the extent of blockchain's impact on various industries, but it's currently hard to imagine an area that will not be impacted by blockchain technology. It is however good to remember that actual realised successes are still limited and the technology still has to be proven.

Second generation blockchain technologies have shifted from the singleton payments feature that Bitcoin introduced to the world, to providing either:

- A more focused solution, like IOTA[6], who are building an entire ecosystem for bringing real time transaction capability to the world of IOT, or
- A Smart Contract platform solution like Ethereum, enabling other developers to build applications in a public or private collaboration setting.

Ethereum in particular is advancing quickly, uniting a large number of influential companies in the Enterprise Ethereum Alliance (EEA), set to create a more adaptable version of Ethereum that allows different organisations to tailor the blockchain parameters to their needs. The EEA is currently forming sector specific workgroups to make sure their solutions can meet sector regulations. No Telco working group has been formed at the time of writing.

Looking further, the public interest to invest in blockchain solutions is growing at an increasing pace. Furthermore, the pace of innovation is growing rapidly, as well as the size of the developer community.



4 Operator Business Opportunities

Considering the development of blockchain initiatives and the business opportunities it creates, there are strong indications that mobile network operators may benefit from these developments.

Blockchain has the potential to be for value what the Internet has been for information. In addition to the many use cases being explored for industries such as finance, healthcare, and government, there are plausible applications of blockchain technology for an operator, both within its current and future portfolio.

The business opportunities that blockchain creates for the operator business are diverse and extensive. Further study on the blockchain technology and its use for operators is necessary, especially in the way operators work at the network level.

In this chapter, we explore a number of current and future developments in the mobile operator sector where blockchain or distributed ledger technology can be applied to improve business processes, to reduce costs, and to enable new business opportunities.


Please note that the following ideas are, in general, looking to improve existing solutions. There is an entirely distinct category of solutions that can be implemented across operator networks and mobile devices that are out-of-scope for this initial opportunity write-up. There are exciting opportunities that will arise in a sharing economy, where

- everyone is a *consumer* as well as a *service provider* (*aka prosumer*),
- subscriptions may very well be replaced by *pay-per-use* models
- the mobile device is used to conduct frictionless peer-to-peer micropayments with persons, organisations and autonomous IOT devices
- companies and partnerships between companies are formed as autonomous decentralised organisations
- transactions and exchange of value become an inherent capability of the networks users interact on

4.1 5G Technology and connectivity

5G technology implementation can potentially benefit from DLT to streamline processes. To realise the 5G promise of ubiquitous access across various networks, CSPs will need to handle heterogeneous access nodes and diverse access mechanisms. Selecting the fastest access node for every user or machine will be a central challenge in the future. Blockchain can be used for guaranteeing/incentivising a mere number of nodes/servers to support faster path selection.

The access networks in a given area can be networked via a blockchain where each access point (Wi-Fi router, SP cell tower, etc.) can serve as a node in the network, monitoring the devices. Rules and agreements between the various access providing networks can be coded into autonomous smart contracts. These contracts can be dynamic in nature wherein any time a policy needs to be changed, only the contract code needs to be changed.



When a device broadcasts its identity, it is accepted into the network by the corresponding CSP cell. Once the device broadcasts its location, the access node that can best provide service to the device is called upon to do so. This also allows for seamless rating and charging of all services between the various access nodes. If, for example, a WLAN from an office or a home network has provided access to a device, then the CSP can conceivably give a reduction in the bill amount appropriately for the invoice of the accommodating company or home.

4.2 IOT Connectivity

DLT can support secure and error-free peer-to-peer connectivity for thousands of IoT devices with cost-efficient, self-managed networks. While this relies on other technologies such as Generic Bootstrapping Architecture (GBA), Crypto graphics chips and networks for data insourcing, blockchain can provide support through its immutability capabilities. A blockchain system by itself has no way to verify data from outside sources. To mitigate this, decentralised oracle networks function as a bridge or source of truth by reaching consensus about the correctness of data before relaying it to the blockchain. For example, machines within a manufacturing plant will be able to communicate and authenticate themselves via the blockchain to steer production processes. Active manual intervention by the workforce will for example only be needed if individual machines require service on the basis of predictive maintenance indicators. In addition, the risk of a production shut-down due to corrupted or hacked machines could be limited, thanks to the distributed and consensus-based authentication of data in the blockchain network. Other DLT technologies like DAG tangle (used by IOTA) [6] can provide the same benefits as the sensors themselves can operate as nodes in the DAG without the need for an intermediary IOT or data management platform.

These self-managed networks can operate on a global scale as long as device, blockchain and communication protocols are standardised. While localised networks in for instance a manufacturing line can provide great benefits, self-organised global supply chains powered by IOT can help streamline processes that require a lot of paperwork and governance. This would shift the focus from centralised IOT platforms (in technology and governance) to self-governed mesh networks. For instance, a shipping container moving between logistics partners without any manual paperwork, while leaving a tamper prove audit trail of conditions and pass-over registration.

Benefits are: self-managed, peer-to-peer networks taking over regional routing, high security levels for IoT devices within public blockchain networks and low-cost setup options for SME purposes.

4.3 Fraud prevention

Fraud detection and prevention continue to be topics of relevance for most CSPs, as a result of fraud costs in the industry of over USD 38 billion annually. The telecom industry has not yet found a way to effectively and sustainably prevent fraud. In a general sense, working together to combat inter-operator fraud is a good way to start. Blockchain could for instance be used to govern access to fraud detection information shared between operators. In a broader sense, fraud can start at the POS by different means of cheating the operator KYC system. Especially if different compliance rules are being deployed by various operators in different countries.

Blockchain is looking to 'externalise' KYC processes and introduce a new era of Identity management. Operators can benefit to leverage this and combat KYC fraud.

Another angle is fraud caused by delays in sharing CDR's between operators. As blockchain works in real-time, using a shared administration of network activity could help identity plausible fraudulent connections faster. Smart contracts could be deployed to actively enforce network usage compliance rules and help us resolve inter operator disputes easier.

4.4 Wholesale roaming & interconnect, billing and charging for Mobile Operators

One additional major usage for blockchain is in the wholesale roaming and interconnect billing. By allowing our customers to roam/ interconnect on each other's networks, we provide a valuable, indispensable service, but this also requires a lot of interaction between operators. The current system of storing CDRs and clearing and settling these records is a costly process. Even post this immense effort in supporting the reconciliation process, there is always mistrust on abusing the tolerance margin. Low wholesale margins can be eroded by rounding or tolerance abuse.

Banking industry is the first sector to truly start reinventing clearing and settlement processes based on blockchain technology, and considering our clearing & settlement process is modelled around similar principles it's worth investigating the possibility of disintermediating this process through blockchain technology.

In this scenario, smart contracts can be used to enforce roaming partner agreements in real time, using cryptocurrencies or tokens to settle between operators over a private blockchain. On-chain governance can be achieved by managing the contracts together, requiring all parties to agree on contract revisions. Secondly, since CDR's are digital, they can consider them as blockchain items where both roaming and interconnect parties, along with their third party vendors and compliance agencies for example regulators can be made privy to the ledger. API's would be communicating and building the blockchain with every CDR in seamless and immediate reconciliation in a trustworthy atmosphere. This initiative can be sandboxed in internal transactions between a GSM operator and its ISP customers, MVNO dependencies or other third party allies. Then after a successful proof of concept, this solution can be applied to interconnect for voice and SMS, before getting recognised for international carrier business and services, and ultimately wholesale roaming based on a roadmap designed by GSMA.

4.5 Charging for Hotspot and Mobile Operators

Currently global access to hotspots is limited for an operator's customers. Intermediaries, who mediate between the subscriber and the hotspot provider, charge for their services. **FON** is an example of such a service.

Access control via blockchain, smart contracts and/or access-coins could remove intermediaries and allow hot spot users to interact directly with the access points, paying (if needed) for the bandwidth they are using in real-time. No prior customer-service provider relationship is even necessary as the required access tokens are purchased to access different hot spots and award hot spot owners.

4.6 Re-selling fixed-line access through Wi-Fi access

In this scenario, the fixed-line operator (ISP) allows end customers to sell Wi-Fi (or maybe even 4g/5g) access to other end customers, thus reselling their own bandwidth/connectivity. This ISP offering may or may not include offerings to access hot spots worldwide.

In a more general sense, homeowners could start participating in the Sharing Economy for digital services, sharing their access energy, computing power, storage and bandwidth to anyone willing to pay. To implement such a system, secure access and easy setup are required. This can be accomplished in many ways, like leveraging existing devices (modem, set-top box), installation mechanic services and customer service infrastructure.

4.7 Distributed ledger & blockchain network hosting

Distributed Ledger and/or Blockchain network operators are responsible for configuring the network and granting access to network participants. In general, they specify the use case(s) that the network is serving, and are often involved in managing the network in terms of software upgrades, arbitration services, etc. A network can be operated by a single entity or a federation of multiple, separate entities.

There are two different types of network operators: some are using a (mostly internally deployed) distributed ledger network as a core infrastructure component to deliver their value proposition, while others are positioning their network as a shared enterprise infrastructure. For the former, DLT is a means to an end, whereas for the latter, the provisioning of a DLT network is their core activity.

Network participants directly interact with the distributed ledger by running a node. They can perform certain actions depending on their permissions. Network participants can range from individuals, non-profit organisations and corporations to government agencies.

4.8 Supply Chain Management and Purchase to Pay processes

Simplified transactions facilitated by blockchain will become the basis for smart contracts, with the promise to automate complex processes while making them legally binding and self-enforcing at the same time.

Smart Contracts, cooperation in mining and Telecom operators becoming blockchain hubs will allow them to replicate this technology on their own financial management:

Consider the blockchain startup Ripple which settles an international money transfer between two banks in 20 seconds. Traditionally, this process took two to six working days. This transformative technology won't find instant global adoption due to many unsolved challenges. However, it is expected that around 10 percent of global GDP might be stored in blockchain before 2030.

Smart contracts can be used to pay for asset delivery. Warehouse to warehouse, spare parts, services, settlements, space segment, fiber capacity, bandwidth usage, consortia deals, fleets and other assets.

Disintermediation and data integrity are the DNA of blockchain and sought after for a healthy relation between telecom operators and vendors & partners.

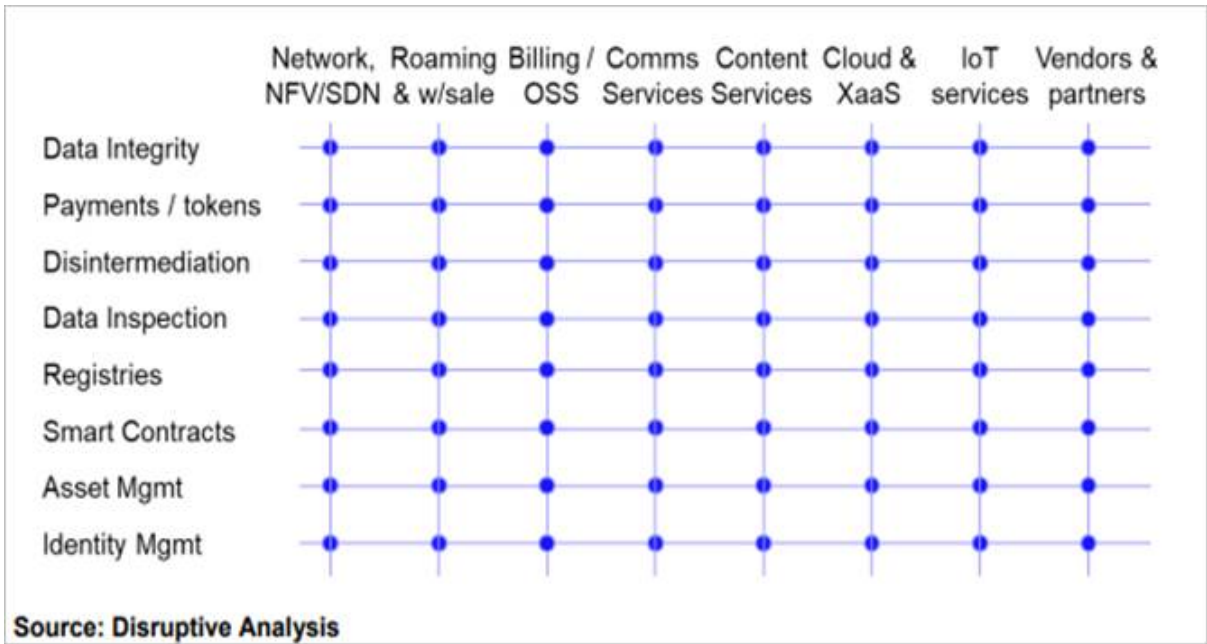


FIGURE 6: DEAN BUBLEY, BLOCKCHAIN AND THE TELECOMS INDUSTRY: WHAT'S HAPPENING? PUBLISHED ON MAY 19, 2017: BLOCKCHAIN / TELECOM OPERATORS INTERSECTIONS

4.9 Self-sovereign Identity & Mobile Connect

A self-sovereign Identity is a digital identity where the user is on full control of their own data. There are two opportunity streams related to self-sovereign identities:

1. Strengthen Mobile Connect implementation, governance and cooperation by using blockchain and self-sovereign identities to bridge the gap between 'real' and digital identities. On the flipside, the emergence of Decentralised IDentity (DID) platforms have the potential to leapfrog Mobile Connect as an Identity system. Zooko's triangle[9] describes three desirable properties for identity handles in networked systems. Secure, decentralised and human meaningful. Blockchain in general and the W3C DID specification[10] specifically address the first two of these properties. The usability of phone numbers through mobile connect for authentication could augment DID and bring human-meaningfulness to blockchain identities.
2. Providing services for customers to help them manage blockchain access and identity, like blockchain API endpoints, Identity or key recovery services or authorisation endpoints for DID interaction.

Mobile Connect provides a great opportunity for operators to facilitate identity, authentication and authorisation processes for service providers. Implementations of Mobile Connect in different countries have shown that while being successful, there's room to improve the governance and cooperation between operators and vendors, mainly due to complex contract structures. This would introduce a fifth mobile connect governance model that leverages blockchain & smart contracts to address existing issues across all four other models currently in use.

Blockchain could potentially provide a new approach to implementing a contracting system for service providers across operators and by doing so eliminate a lot of the process and legal hurdles that are currently identified.

Many other services can be built on top of such a system, like the ability to leverage existing KYC processes, introducing new business models for digital identity management or consent management services for data stored by third parties.

As a payment and token system, it can also be worthwhile to employ a token for inter-operator user verification across each operator's vendor network. This will simplify the use of each other's authentication end-points and related charges can be facilitated from MNO data centres. In a production setting, it would make much more sense to spread nodes across multiple independent enterprises to create a decentralised blockchain operating system. This could be an interesting opportunity and a national as well as global scale.

4.10 Blockchain consumer services

Blockchain is still an incomprehensible technology for most. To become an important operating layer in society, more work needs to be done to make blockchain services fully integrated and easily accessible. Through devices, stores, set-top boxes, business integration services and a role as trusted party in general; MNO's are well positioned to leverage their infrastructure to engage and involve consumers with an all-new suite of services.

4.11 IOT

IOT is already a big industry for Telcos. Secured mesh networking is an interesting opportunity and so are IOT based quality control, self-governing data sensors and transport layer independent IOT networks. Many start-ups are focussing on providing secure crypto chips for IOT devices creating very interesting IOT platforms.

IOT can also be used for automatic tracking for quality and conditional parameters during transports, switching of ownership and provenance use cases. Another interesting concept is that of the circular economy, where we start tracking not only the origins of products but also what happens after we discard them.

4.12 Content distribution

Delivering content directly from content providers (e.g. Disney) straight to CSP customer devices, removing intermediaries from the process.

4.13 Crypto-Wallets

Crypto-wallets are not yet mainstream due to complex user experience, especially in the case of hardware wallets. MNOs could play a role developing secure and trusted crypto-wallets with secure back-up and recovery functions, which is a big gap that exists today.



4.14 Smart cities

Smart cities require IOT and new governance solutions. Blockchain technology used as a basic building block will make resulting products & services not only secure and transparent, but also provides an Identity and payments layer to benefit from. Besides providing general transaction capabilities, a new *smart citizen* concept can be adopted where desired behaviour is stimulated through crypto-economic incentives.

4.15 Advertising

Comcast has started work on a blockchain based insights platform to improve customer profiling across companies and channels. Through user consent registered on the blockchain, advanced data sharing models and targeted advertising models can become a reality.

5 Business rationale for investing in blockchain

5.1 Blockchain applicability

Blockchain, while using technology, cryptography and research that was developed over the past few decades, is still an immature technology. It is seen by many as a, 'cure for all'. It is critical to choose applications for which blockchain is the right technical solution with proper timing. To be able to decide whether or not a certain use case is viable for business there are multiple principles to validate.

The section highlights a non-exhaustive list of principles to follow for viability assessment. The commentary draws heavily from below blog posts:

- **Avoiding the pointless blockchain project [7]**
- **When do you need blockchain – decision models [8]**

5.1.1 Multiple entities are involved (organisations, departments, consumers)

- Multiple entities regularly exchange information/assets
- Several entities need a synchronised data position
- Entities have only basic level of trust

5.1.2 Blockchain (sometimes partly) replaces central authority or creates trust in a previously trust-less situation

- An intermediate party creates trust among otherwise trust-less competing/collaborating entities
- Currently, no transactions are possible due to lack of trust between parties

5.1.3 Auditability of processes is important

- Entities need to verify authenticity, origin or quality of data
- Entities need to verify data integrity
- Entities need to be able to rely on immutability of data

5.1.4 Information involved needs to be reliable and represents a certain value

- Data involved represents high tangible or intangible value
- Information involved facilitates high value transactions

5.2 Strategic drivers for blockchain adoption & adaptation

The following is a list of strategic considerations when deciding to start implementing blockchain technology. The areas to consider may vary from company to company and implementation to implementation.

5.2.1 Timing

Initiatives should take a maximum of five years on average to reach relevant revenues to mitigate commercial product development risks and opportunity costs. Payback periods should be divided in short-, mid- and long-term categories to align with the evolutionary state of the blockchain technology. Evaluating the actual state and planning new Go-to markets accordingly should be done at least every quarter.

Note: These figures are estimates and, may vary depending on scale and complexity of implementation.

5.2.2 Protect current business

- Protect the position as connectivity provider. Blockchain may become a foundational technology underlying connectivity solutions from mobile networks to IoT.
- Blockchain positions operators as a one stop shop for future digital service offerings.

5.2.3 Develop new business

- Revenues on core network activities declining

- MNOs looking for new revenue sources to fill the gap
- Blockchain offers exciting new fields with many growth opportunities
- Ease new market entry by broadening the landscape of emerging technologies whereby market shares of existing markets are getting reshuffled
- Initiatives that can help MNO's attain a strategic position in the value chain, strengthening its other applications

5.2.4 Improve core operations

- Cut costs and improve operational control on KPN core networks and other activities through blockchain's ability to offer high grade security and process control
- Reduce complexity in a MNO's operational core. The difficulty of realising and operating the solution is an indicator for investments and operational costs.

5.2.5 Retain innovative edge

- A MNO needs to remain the cutting edge provider of IT to attract and retain top talent
- Blockchain is a promising new tech area and MNO's should not "miss the boat"

6 Regulatory and Compliance Review

Blockchain, as a technology, has the potential to become an integral part of the operation of many enterprises, offering scalability, security and computing power at a lower cost. But, there are a number of issues that need to be carefully considered in order to realise the potential benefits. Some of the expected issues are discussed below.

6.1 Regulation

Depending on the uses of blockchain, and as blockchain is utilised or considered as appropriate for enabling specific service offerings, it is likely to receive more regulatory attention. For example, in Q4 2017/ Q1 2018, the level of interest from governments and financial regulators increased in bitcoin and other cryptocurrencies underpinned by blockchain technology. Also, another use case is where blockchain technology is used as a, or in a similar manner to a distributed database system, then adherence to data privacy and financial regulations is likely. It is possible that issues ranging from (but not limited to) quality of service, cross border data transfers, illegal content, lawful access etc. will need to be examined on a case by case basis.

6.2 Compliance/ Legal

The technology provides an opportunity to conduct real time compliance checks, and ensure all operations are transparent and bound by the contractual legal terms at all times. Any exceptions could be identified allowing for corrective course of action. However, this will also depend on technical requirements and the types of operational and support systems utilised. Different countries might end up operating under different regulatory and legal frameworks- this, in-turn, will require review of each use case.

6.3 Privacy and Data Protection

Blockchain is based on a certain level of pseudonymity - there is no concept of a real world identity in the blockchain itself: these exist only in the ecosystem, for example exchanges or wallets that require KYC processes. What can be derived from the public, open to everyone, blockchain data, is the set of services and data related to a digital identity. In addition to use of pseudonymised data, certain use cases of blockchain may involve personal data identifying individuals. Therefore each use case will have to be examined to understand how data protection legislation can be complied with and privacy protection can be built into the use case.

6.4 Jurisdiction for Smart Contracts

Smart contracts are self-executing programs that will execute itself upon specified criteria and eliminate the need for intermediary partners to confirm a transaction. These smart contracts lead to various new opportunities but may also raises legal questions in relation to applicable law and jurisdiction.

Blockchain has the ability to cross jurisdictional boundaries as the nodes on (public) a Blockchain can be located anywhere in the world. This can pose a number of complex jurisdictional issues which will

require careful consideration in relation to the relevant contractual relationships that underpin the use of blockchain.

6.5 Blockchain auditability

Auditing services could benefit from the immutable aspects of blockchain data to simplify their processes. These processes are likely to be subject to the same laws.

7 Blockchain myths and challenges

The use of blockchain technology, in some cases, provides advantages over other technologies when processing transactions where assets or identity are involved. Even though Blockchain technology has the potential to bring a paradigm shift in the way people operate their businesses, a detailed study must be conducted prior to choosing it for enabling any service offerings. This section counters common myths and challenges faced.

7.1 Myths

7.1.1 Blockchain removes the need for trust

Blockchain in many cases makes the need for strong trust relationships obsolete, but does not completely remove the need for trust. In the simplest form, trust in cryptography replaces the traditional trust factor. Furthermore, blockchain can function as a decentralised trust root, removing the need for trust in centralised authorities.

An important consideration when it comes to trust is that blockchain provides a way to predefine the rules of engagement in a verifiable and immutable fashion, restricting the need to trust each other, while delegating operations to self-governing system.

In case of a permissioned or a private blockchain, a gatekeeper is required for enabling secure access. The cryptographic authenticator or a gatekeeper still represents a traditional trust relationship.

To convince business partners and consumers to start trusting a piece of technology they do

not fully understand is problematic, but Telecom operators are well positioned to make blockchain applications accessible to the masses.

7.1.2 Blockchains cannot be hacked

Most hacks talked about represent badly secured exchanges, badly written software and/or smart contracts, or personal social engineering attacks. In addition, lack of actual understanding of blockchain technology combined with an influx of non-tech savvy users is a feeding ground for social hackers. Hardware wallets in form of a pluggable memory drive can protect users in this regard, but custodian services to help people guard and recover their accounts will be required. Management of actual money could very well shift to management of user's identities and a lot more needs to be done in this area.

Even with all the above challenges, the statement 'Blockchain technology cannot be hacked' holds true as cryptography used in blockchain technology has held up so far. To date, neither Bitcoin nor Ethereum have been

subject to *any* successful hack. New technologies like quantum computing might disrupt this, but blockchain security will have to adapt and rise to these new challenges.

7.1.3 Every transaction in blockchain represents the truth

The system itself does not control the input or output and simply executes a given transaction. Blockchain based IOT transaction systems for instance depend on the trust in data for example the integrity of the IOT sensor. Therefore, the input data must be accurate to assure the integrity or correctness of data in the Blockchain.

The governance of truth as ascribed to blockchain technology is in-fact related to its properties of transparency and cryptographic signing. This applies purely to transactions processed entirely within the blockchain itself.

7.2 Challenges

7.2.1 Blockchain technology is not yet mature

Resolving challenges such as transaction processing speed, the verification process, development ecosystem, data limits and personal key management will be crucial in making blockchain widely applicable. As the technology matures, a migration path from private blockchain environments (permissioned chains) to public blockchain is required as companies' shift their attention from private to public solutions. This however may not be the case in all uses cases for instance wholesale roaming settlement operations will remain a permissioned private blockchain environment.

A lot of work will happen in the space of verifying external inputs, as demand will grow for building interfaces between different blockchains. For example: Oracle is developing systems to 'govern the truth', allowing outside data points to be taken for truth within the blockchain system.

7.1.4 A blockchain is immutable

Blockchain relies on a crypto economic system based on cryptography and game theory which prevents attacks by making them economically unfeasible.

The technology is not 100% immutable, but the cost of engaging in an attack is much higher than the gains derived out of a successful attack. Therefore, during normal operations Blockchain is immutable. It is however susceptible to 51% (or a quorum agreed to commit a transaction) attacks, meaning that history can be rewritten if the majority of the network agrees to do so.

7.2.2 Scalability/performance

Existing networks have too little transaction processing power for executing high volumes of transactions. Many developments are underway to resolve this (difficult problem) in an attempt to reach Visa scale transaction processing capabilities.

7.2.3 Regulators respond late or insufficient

All traditional currencies used in the world today, are created and regulated by national governments or similar central authorities. Blockchain based implementations using these crypto currencies for asset value exchange may face a hurdle in wide spread adoption if major financial institutions or government regulation remain unclear.

7.2.4 Control, security, and privacy

While solutions exist, including private blockchains and strong encryption, there are still cyber security concerns that need to be addressed before the general public will entrust their personal data to a blockchain solution. Quantum computing for instance is advancing rapidly and there is a growing concern that Quantum computers are able to brute force the cryptography used in blockchain systems today. While some quantum resistant ledgers already exist, the general consensus in the blockchain community is that other ledgers will adapt if needed.

7.2.5 Integration with existing systems can be complex & expensive

Blockchain applications offer solutions that require significant changes to, or complete replacement of, existing systems. In order to

make the switch, companies must strategise the transition. A new business framework is required to model processes to blockchain solutions.

7.2.6 User adoption

Blockchain represents a complete shift to a decentralised network, which requires the buy-in of its users and operators. The key shift for users is that they are going to get more power over their identity, data, etc. With more power comes more responsibility and accountability. Many users are happy with the status quo and may not be comfortable with that shift.

7.2.7 Cost & Benefits

Blockchain technology can offer tremendous savings in transaction costs and time but the high initial capital costs could be a big hurdle for executing changes.

Annex A Blockchain Types and Cryptocurrency Brands

A.1 Ethereum

Bitcoin was the first technology that allowed securely sending money across the internet, without fear of fraud or censorship. Bitcoin was not designed to do anything more than sending money and could not benefit of the full potential that was envisioned for blockchain technology. An inherent characteristic of the blockchain network was to limit functionality to improve security.

Ethereum is an open blockchain platform that lets anyone build and use decentralised applications that run on blockchain technology. Like Bitcoin, no one controls or owns Ethereum – it is an open-source project built by many people around the world. However, unlike the Bitcoin protocol, Ethereum was designed to be adaptable and flexible. It is easy to create new applications on the Ethereum platform.

Ethereum is created by Vitalik Buterin, who had a different approach to the distributed ledger. He imagined Ethereum as a “world spanning computer”; one that fits a virtual machine (the EVM), a programming language (Solidity), and its own crypto currency called Ether (ETH). This combination allowed the creation of complex programmatic computational instructions commonly known as smart contracts.

The Ethereum Virtual Machine (EVM) is the runtime environment for smart contracts in Ethereum. It is not only sandboxed, but also actually completely isolated, which means that code running inside the EVM has no access to network, file system, or other processes.


Ethereum allows developers to program their own smart contracts, or 'autonomous agents', as the Ethereum white paper calls them. The language (solidity) is 'Turing-complete', meaning it supports a broader set of computational instructions.

Smart contracts can:

- Function as 'multi-signature' accounts, so that transaction of value only executes when the required percentage of people – as written in the program - agree.
- Manage agreements between users, compared to the old “if-then-else” statements.
- Provide utility to other contracts (similar to how a software library works)
- Store information for an application, such as domain registration information or membership records.
- Manage tokens

As with Bitcoin, users must pay small transaction fees to the network. The sender of a transaction must pay for each step of the “program” they activated, including computation and memory storage. These fees are denominated in Ethereum’s crypto currency, ether.

Like Bitcoin, Ethereum uses public-key cryptography, peer-to-peer networking, and proof-of-work to process and verify transactions. The miners, responsible for publishing new blocks and validation,



compete with one another for their block to be the next one to be added to blockchain. Miners are rewarded with ether for each successful block they mine. This provides the economic incentive for people to dedicate hardware and electricity to the Ethereum network.

A.2 Bigchain DB

BigchainDB is a scalable blockchain database: a big-data database with blockchain characteristics including decentralisation, immutability and built-in support for creation & transfer of assets.

BigchainDB takes a different approach to solving the scaling problem. They claim to have developed a proven, scalable, big-data database and then adds blockchain characteristics like, decentralised (no single entity owns or controls it), immutable (tamper-resistance), and assets (you own the asset if you own the private key, aka blockchain-style permissions).

BigchainDB supports both public and private deployments. Validation of transactions is based on federation of voting nodes. Whenever a certain number of nodes vote for agreement to validate the transaction, the transaction gets validated. This system benefits the speed of which transactions are processed.

Being a decentralised database, BigchainDB is complementary to decentralised processing technologies like Ethereum Virtual Machine. Therefore, BigchainDB has no own token to reward the validation of transactions but uses the underlying network for example Bitcoin or Ether.

Many BigchainDB use cases are like traditional blockchain use cases, except focused on situations where high throughput, more capacity, lower latency, better querying, or richer permissions is necessary.

Many people in the distributed ledger community put question marks on BigchainDB not being a real blockchain.


A.3 Hyperledger

Hyperledger is an open source collaborative effort created to advance cross-industry blockchain technologies. It is a global collaboration, hosted by The Linux Foundation, including leaders in finance, banking, Internet of Things, supply chains, manufacturing and Technology.

Hyperledger incubates and promotes a range of business blockchain technologies, including distributed ledger frameworks, smart contract engines, client libraries, graphical interfaces, utility libraries and sample applications. The Hyperledger umbrella strategy encourages the re-use of common building blocks and enables rapid innovation of DLT components.

Hyperledger Fabric is a one of the blockchain projects within Hyperledger. Like other blockchain technologies, it has a ledger, uses smart contracts, and is a system by which participants manage their transactions.

Hyperledger Fabric differs from other blockchain networks by being a private and permissioned blockchain network. The members of a Hyperledger Fabric network enrol through a membership services provider instead of being identified through the use of (POW) proof of work like Bitcoin and Ethereum use.



Hyperledger Fabric also offers several pluggable options. Ledger data can be stored in multiple formats, consensus mechanisms can be switched in and out, and different MSPs are supported. Smart contracts are written in chain code and are invoked by an application external to the blockchain when that application needs to interact with the ledger

It also offers the ability to create channels, allowing a group of participants to create a separate ledger of transactions. This is an especially important option for networks, where some participants might be competitors and not want every transaction they make become known to every participant. If two participants form a channel, then those participants – and no others – have copies of the ledger for that channel.

The consensus model used by Hyperledger fabric consist of the fact that in any case transactions must be written to the ledger in the order in which they occur, even though they might be between different sets of participants within the network. For this to happen, the order of transactions must be established and a method for rejecting bad transactions that have been inserted into the ledger in error (or maliciously) must be put into place.

This is a thoroughly researched area of computer science, and there are many ways to achieve it, each with different trade-offs.



GSMA HEAD OFFICE

Floor 2
The Walbrook Building
25 Walbrook
London
EC4N 8AF
United Kingdom
www.gsma.com