Opportunities and Use Cases for **Distributed Ledger Technologies in IoT**

2018

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 industry-leading events such as Mobile World Congress, Mobile World Congress Shanghai, Mobile World Congress Americas and the Mobile 360 Series of conferences.

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

Follow the GSMA on Twitter: @GSMA.

About the GSMA Internet of Things Programme

The GSMA's Internet of Things Programme is an industry initiative focused on:

- COVERAGE of machine friendly, cost effective networks to deliver global and universal benefits
- CAPABILITY to capture higher value services beyond connectivity, at scale
- CYBERSECURITY to enable a trusted IoT where security is embedded from the beginning, at every stage of the IoT value chain developing key enablers, facilitating industry collaboration and supporting network optimisation, the Internet of Things Programme is enabling consumers and businesses to harness a host of rich new services, connected by intelligent and secure mobile networks.

Visit gsma.com/iot to find out more.

TABLE OF CONTENTS

1. Introduction

The launch of Bitcoin in 2008 showed that distributed ledger technologies could be used to create a decentralised, peer-to-peer trust network where transactions in the form of payments could be secured without depending on a central authority.

Since the launch of Bitcoin there has been widespread interest and activity in extending the application of distributed ledgers to other application areas. This has resulted in developments such as 'smart contracts' on the Ethereum[1] blockchain or specialised 'tokens' such as IOTA[2] focused on IoT applications and GDPR compliant ledgers, like the Sovrin ledger, for identity management.

This document sets out to explain the use of distributed ledgers and describe the business opportunities and use cases for ledgers connected with the IoT.

[1] See https://www.ethereum.org and http://www.ethdocs.org/en/latest/introduction/web3.html#smart-contracts
[2] https://www.iota.org

2. Technology Overview

2.1 DISTRIBUTED LEDGERS

A distributed ledger is a record of transactions or data that is maintained in a decentralised form across different systems, locations, organisations or devices. It allows data or funds to be effectively sent between parties in the form of peer-to-peer transfers without relying on any centralised authority to broker the transfer. Details of the transaction are recorded on a transaction ledger that is distributed across many network nodes. The concept applied to payments was set out in the Bitcoin white paper (https://bitcoin.org/bitcoin.pdf) – this paper addressed the requirement to prevent a key problem in distributed transactions, preventing 'double spend'.

Cryptographic techniques are used to secure the information in the ledger via digital hashes. Typically a 'chain' is progressively built where the digital hash of a new block is based on both the data within that new block as well as the digital hash of the preceding block, this process repeating to the original 'genesis block'. Therefore any member of the network can verify the integrity of the chain by recalculating the digital hashes and checking against the entries in the chain. Similarly it is considered impossible (in practical terms[3]) to amend an earlier block as the digital hash would change and the 'chain' of digital hashes would no longer have integrity.

A distributed consensus mechanism allows members of the network (nodes) to establish a common 'truth'. There are different mechanisms for this, in the case of Bitcoin and many other 'crypto-currencies' a computationally complex 'Proof of Work' algorithm is used to protect the integrity of the network against change to the public 'blockchain' by making it impractical for malevolent players to alter the chain.

Whilst Bitcoin operates on a public blockchain there is also the possibility to operate distributed ledgers privately where network participants are provided with relevant permissions to either read or write (i.e. append) to the ledger. Private ledgers are useful for applications where it isn't necessary or appropriate for the world to know what is on the ledger, just those parties relevant to the transaction.

[3] There are methods of attack for 'proof' tokens such as Bitcoin which can be implemented depending on the ability to command over 50% of the so called hashing rate of the network. For tokens with significant networks this is effectively impractical to achieve but there is a risk to other tokens.

2.1.1 BENEFITS OF DISTRIBUTED LEDGER TECHNOLOGIES

There are a number of features of distributed ledgers that benefit applications in the IoT

- **Immutability.**

Once entries have been committed to the distributed ledger they become part of a permanent history, any attempt to change the history is practically prevented since the sequence of cryptographic signatures will expose the change. This provides a robust defence against errors or fraud or systematic attacks against data.

- **Transparency.**

Any party or system which can access the distributed ledger has the ability to inspect the data recorded on it (as well as check the digital signatures). Participants have access to the same information on the distributed ledger. Note this does not mean that all data must by definition be public or available to every participant, as permissioned distributed ledgers can be used to control the access to the data stored. In addition the data recorded on the distributed ledger can itself be a digital signature of other data, so the ledger provides the mechanism to prove the integrity of data which is known to multiple parties but not actually recorded on the ledger.

- **Resilience.**

The data on the distributed ledger is replicated across many (often all) nodes that form the network. The failure of one or even many systems forming the network is tolerated because there will be many other nodes that continue to run and support the operation of the ledger. For example the Bitcoin network currently has over 12,000 'full nodes' distributed globally[4].

- **No controlling party.**

The operation of the distributed ledger is not dependent on the systems, ownership or business continuity of any one organisation. This means such an organisation cannot exert negative influence over the operation of the distributed ledger for example introduce new charging mechanisms, make technical changes to the design of the ledger or introduce a technical systems dependency which could mean a systems failure at the controlling organisation leading to an outage of the whole ledger.

- **Scalability.**

The distributed ledger can 'scale horizontally' (though see the next section on congestion) both to meet a growth in demand by applications and to support higher resilience. In addition, the network can scale globally to support international growth – applications then access more local nodes which results in lower latency for API calls.

- **Security.**

Distributed ledgers benefit from strong cryptographic techniques to secure the data recorded on them. Also the fact they are distributed and data is synchronised across the network provides extra security against point attacks including denial of service or attempts to modify the content of the ledger. Also, distributed ledger solutions are generally 'open source' with the benefit that community scrutiny helps to identify security weaknesses and improvements.

[4] See https://bitnodes.earn.com

2.2 SMART CONTRACTS

Smart contracts are a technology quite closely related to distributed ledgers, first proposed in 1994[5] and implemented in public blockchains such as Ethereum and software platforms such as Hyperledger Fabric. There is also a limited form of smart contract implemented in the Bitcoin blockchain.

The concept of a smart contract is of a set of software functions which is stored within the distributed ledger and executes when there is a request to add a transaction to the distributed ledger. The execution is performed 'in the ledger' which means the code executes in near real-time and across the network of nodes that form the distributed ledger network – with consensus rules being applied, and means the developer does not need to provide their own highly resilient systems to support transaction processing. A transaction does not need to be associated with a payment to participate in a smart contract though in many cases there will also be a linkage to payments.

Smart contracts are more generally considered to be software implementations of legal agreements between transacting parties. A big difference compared to a standard legal contract is the form of the contract is fixed up front by the party offering the contract and implemented in code.

A distributed ledger can store multiple, different smart contracts for different users or applications. One of the best known examples of smart contracts on a public blockchain is 'Crypo Kitties'[6] implemented on the public Ethereum network, there are various smart contract functions defined including support for running auctions for 'Kitties'.

A key advantage of a smart contract is that it can implement rules involving multiple parties. Therefore it can be applied to cases such as voting where it can ensure users can only vote once, or auctions where only the winning bidder will ultimately pay for the auctioned item. Similarly in the IoT case the smart contract can support cases such as a patient providing consent to their physician to receive their health records from a personal fitness device, or support for purchasing items from a vending machine.

On the Ethereum network the smart contract code is created using the Solidity[7] programming language which compiles to code that can be incorporated into and executed on the Ethereum blockchain. Any process, for example a business process, that can be described in the form of a smart contract will generally benefit from improved efficiency and transparency compared with either a legacy paper based process or a bespoke system implementation.

Due to their utility alongside distributed ledgers it is considered that smart contracts will often be applied to distributed ledger use cases as a complementary technology.

[3] http://www.fon.hum.uva.nl/rob/Courses/InformationInSpeech/CDROM/Literature/LOTwinterschool2006/szabo.best.vwh.net/smart.contracts.html
[6] https://www.cryptokitties.co
[7] http://solidity.readthedocs.io

3. Considerations in the application of distributed ledgers for the IoT

Whilst distributed ledgers have many attractive attributes for IoT applications there are a number of considerations that are relevant. A key aspect is that IoT covers an enormous spread of device capabilities from basic connected devices such as kettles to complex systems such as cars and it will not be practical for every device to participate as a distributed ledger 'full network node'[8] or for every item of data or transaction to be stored on or processed through a distributed ledger.

Main factors:

Storage space.

Distributed ledgers typically require storage space both in the form of RAM to hold unconfirmed transactions and permanent storage (hard disk/ flash memory) to store 'confirmed' transactions. The Bitcoin blockchain reached 149 gigabytes in December 2017 – and due to the design of the Bitcoin blockchain this is replicated across all 12,000 plus full nodes. The Bitcoin 'mempool' (RAM stored unconfirmed transactions) reached approximately 140 Mbytes in January 2018. Both are sizeable amounts of storage, beyond the scale that is reasonable to expect in small, low cost IoT devices. It is noted that IoT distributed ledgers might be designed differently so that the whole ledger does not have to be replicated across all nodes. There are of course many more Bitcoin users (wallets) than full nodes so as a parallel it wouldn't be necessary for each IoT device to be a blockchain node.

Computing power.

IoT devices commonly lack the computing power needed for cryptographic operations typical for distributed ledgers.

Physical security.

Distributed ledgers use asymmetric cryptography for example to sign transactions. The private key needs to be protected even if adversaries have unsupervised physical access to the IoT device which is often the case in both consumer and industry IoT use cases.

Communications bandwidth.

The Bitcoin block size is nominally 1 Mbyte and blocks are confirmed every 10 minutes meaning the daily data rate is around 144 Mbytes. Maintenance of the Bitcoin blockchain requires a continuous

[8] i.e. storing or validating every data/ transaction on the distributed ledger

data rate of 14 kilobits per second net throughput, and initial synchronisation reasonably requires multi-megabit per second connectivity to allow a node to fully participate on a network within a reasonable time. Realistically it is impractical to operate a Bitcoin 'scale' blockchain over low power wide area technologies such as Sigfox or LoRa though this could be done using cellular technologies.

Transaction confirmation time.

During 2017 the Bitcoin transaction confirmation time ranged between 20 minutes and over 400 minutes, this is somewhat better than the equivalent banking standard of 1-2 days or even 2-5 working days[9]. Such confirmation delays are not however acceptable for near real-time payments or near real-time data transfers as may be required for the IoT since until confirmed there is a possibility the transaction or data could be dropped. Alternative solutions such as Bitcoin's Lightning Network[10] or Ripple[11] achieve confirmation times measured in seconds or less therefore supporting near real-time payments or data transfers.

Consensus mechanism.

Public crypto currencies including Bitcoin and Ethereum use computationally complicated 'Proof of Work' algorithms to maintain consensus and secure the network against highly resourced attackers. The process for transaction validation is implicitly linked to the process known as mining and requires expensive dedicated hardware which typically has a significant energy consumption[12]. Such consensus mechanisms are not appropriate for low cost/ low energy IoT devices, so the IoT more likely requires alternate consensus mechanisms.

Congestion.

Whilst as noted above the Bitcoin network can be scaled through the addition of full nodes it has an effective 'throughput limit' related to the block confirmation time which limits the overall transactions per second possible on the network[13]. If more transactions are received than this upper limit there can be congestion which generally leads to average fees increasing as users pay a premium to have their transactions clear faster. Alternate distributed ledger implementations such as Ethereum and Ripple support higher transaction rates but these are still under the rates for the global banking/ payments network or realistically the payment/ data rates that might be required as the IoT expands by billions of devices each year. Blockchain use for IoT applications is likely to be orders of magnitude higher than available from even high performance blockchains such as Ripple and may therefore need alternate architectures (such as 'IOTA').

Fees.

In the second half of 2017 Bitcoin transaction fees[14] jumped from prevailing sub $ levels to reach in excess of $50 per transaction in December 2017, though this has since declined to under $2. Meanwhile, Ethereum transaction fees are currently $0.41 and Ripple $0.0035 (March 2018). There is clearly a cost of establishing and operating a network, whether that's related to a mining reward, or support for the foundations that continue development of the projects, or for purchasing 'tokens' that provide access to the respective blockchains. IoT applications will need a dependable fee structure that is price appropriate for the application.

[9] See https://transferwise.com/us/blog/making-an-international-wire-transfer
[10] Bitcoin Lightning Network details : https://lightning.network
[11] See Ripple https://xrpcharts.ripple.com/#/metrics
[12] Actually the energy consumption is a function of the popularity (and profitability) of mining – if Bitcoin had a low price there would be less competition in mining and therefore the energy usage would fall proportionally. See https://www.bitcoinmining.com/what-is-bitcoin-mining-difficulty/
[13] Comparison at https://howmuch.net/articles/crypto-transaction-speeds-compared lists Bitcoin @ 7 TPS, Ethereum @ 20 TPS and Ripple @ 1500 TPS
[14] See https://bitinfocharts.com/comparison/bitcoin-transactionfees.html

Price volatility .

Fees are not the only financial consideration as some blockchains involve charges for access to the network (e.g. Ethereum smart contracts) levied via tokens purchased on the open market, and in the case of payments it is desirable that the price of a token remains stable so that there is certainty over the amount transferred between parties. Currently many tokens are being used as speculative assets, their high price volatility creates a barrier to many IoT applications particularly if the application is using the blockchain to store 'low value' data or payments for goods/ services with fixed costs. As a result applications might need to convert conventional (fiat) currency to cryptocurrencies immediately before and after use to avoid price volatility risks. Private blockchains may not have the same price volatility as seen with public cryptocurrencies and tokens, however, there will be a cost of establishing and operating the network.

In considering the above issues it is important to note that these issues are not inherently associated with distributed ledgers in general but often relate to design choices or trade-offs made for good reasons within specific implementations of distributed ledgers.

> **"In the case of payments it is desirable that the price of a token remains stable so that there is certainty over the amount transferred between parties"**

4. Key attributes that should be considered for IoT distributed ledger applications

Whilst the benefits of distributed ledgers for the IoT are listed earlier this does not mean that they should be used in all IoT applications and for all data. The following are important tests to ensure distributed ledgers are being applied appropriately:

- **Retention.**

There should be a good reason for information to be retained in the distributed ledger. Transitory information e.g. real-time supply voltage may be important to measure in the IoT device but there is unlikely to be a good reason to retain this information permanently in a distributed ledger replicated to multiple parties;

- **Multi-party sharing.**

There is arguably no reason to store information in a distributed ledger unless there is a good reason for that information to be accessed by multiple organisations, devices or systems. If information is only ever collected and processed by a single organisation or bilaterally shared between two organisations it is likely overkill to burden the distributed ledger with that information;

- **Retrieval flexibility/ performance.**

Whilst sometimes distributed ledgers are referred to as databases they do not provide the retrieval performance or general purpose flexibility of relational databases such as MySQL, Oracle etc. or NoSQL databases such as MongoDB. If the application requires flexible and performant data retrieval then a relational or NoSQL database might be more appropriate to use in conjunction with the distributed ledger, or a hybrid open source ledger implementation such as BigchainDB could be used to obtain the advantage of a distributed ledger which provides features from the NoSQL database MongoDB on which it is based;

- **Non real-time.**

With a distributed ledger there will be a lag between when data or the transaction is generated and when the consensus mechanism confirms the information as part of the ledger. Until confirmed it is possible the information (or transaction) could be rejected. For this reason applications which require real-time processing of data should not rely on storage or retrieval of that information on a distributed ledger as the consensus might take longer to confirm than required for the real-time operation of the system.

5. Example distributed ledger use cases for IoT

The GSMA conducted a review of distributed ledger activities with the community of mobile operators to identify the most promising application areas for the IoT.

These application areas have been organised into three categories, to help understand the position in the value chain, and listed in those categories in the table below.

Category	IoT FOUNDATION (section 5.1) Supporting general IoT functionality	IoT SERVICE ENABLEMENT (section 5.2) Adding value to IoT	IoT SOLUTIONS (section 5.3) Supporting customer solutions
Use Case	◢ Identity for IoT Devices ◢ Access Controls	◢ Supporting Compliance (smart contracts) ◢ Micropayments ◢ Data Sharing & Integrity	◢ Supply Chain ◢ Sharing Economy

While all of the operators consulted for this work are actively exploring the opportunities for distributed ledgers in IoT, it is still at concept phase for the significant majority. Further exploration is needed to assess the commercial opportunity, technical feasibility and size of market. However, Figure 1 shows a collective operator prioritisation of the application areas identified suggesting where resource could be focused for the next level of activity.

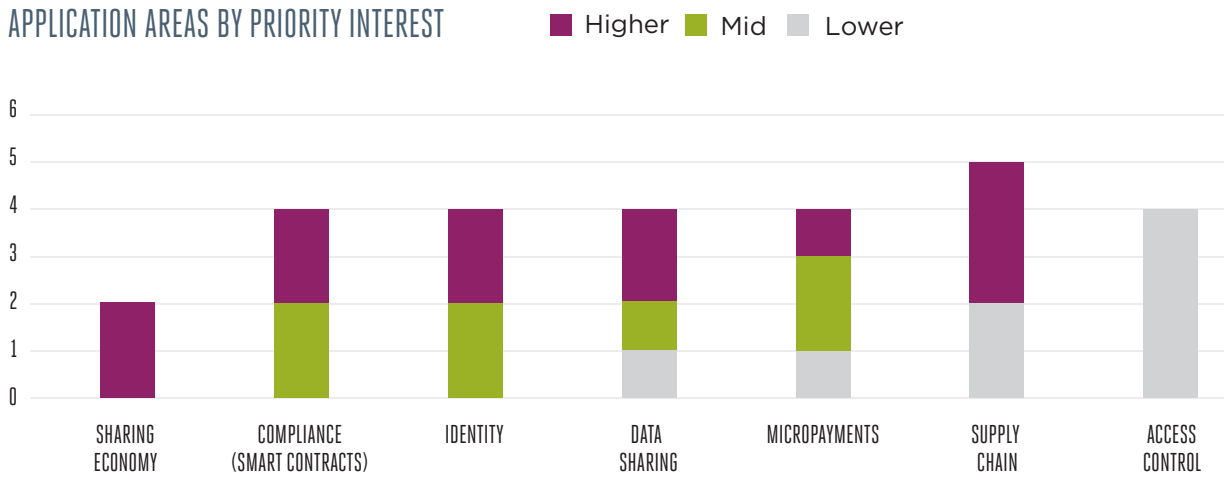


Figure 1 Application Areas by Priority Interest (5 operator member respondents)

While all applications are listed because they are of interest to at least one operator, Figure 1 attempts to show relative interest. Taking data sharing as an example, two operators indicated that this was a first or second priority, suggesting a high level of interest, whereas one operator identified data sharing in the bottom two priorities, and a fourth operator scored it in the middle. One operator did not include data sharing in the prioritisation.

5.1 IoT FOUNDATION

This section describes use cases that are considered generally applicable across the majority of IoT applications.

5.1.1 Identity for IoT devices

As the IoT expands more widely across the consumer sector it becomes more important to be sure that firstly information about devices is maintained in a way to better protect users and secondly that there is a more consistent approach in the methods for storing and retrieving identity information. The following are examples of the use of distributed ledgers for device identity purposes:

- Storing the origin, authenticity and status of a device. For example which company manufactured a specific device; did it pass Quality Assurance and on what date; what is its 'life-cycle' status; is the device serial number valid?
- Devices being able to upgrade their boot code, firmware and software from trusted sources by verification against issuer signature information secured on a distributed ledger;
- Maintaining information about devices including hardware configuration and version information, installed software/ firmware/ boot code;
- Maintaining ownership information or asset tracking data about a device in a way that is 'privacy aware';

The GSMA's Identity programme is evaluating the opportunities of the use of distributed ledger technology in Identity and has recently published a regulatory overview paper called "Distributed Ledger Technology, Blockchains and Identity: A Regulatory Overview"[15]. Based on research and structured interviews with experts this paper aims to trigger a discussion with mobile operators, regulators and policymakers and provide a high level overview on how to encourage technical and legal interoperability of distributed ledgers and blockchain solutions under existing regulatory frameworks.

What are the benefits of distributed ledgers for this use case?

There is currently no consistent approach amongst manufacturers for maintaining device identity information, and this means that whilst some manufacturers have developed solutions to one or more of the requirements above there will be many other manufacturers that have not. The problems with this 'piecemeal' approach are

- Some devices are left exposed to vulnerabilities such as 'man in the middle' hijacking of software/ firmware updates that can then be exploited by hackers;
- Addition of new manufacturer's devices to an asset base usually means those devices cannot be managed the same way as other assets, or alternatively additional integration work is needed for those new devices;
- Any party who has a legitimate interest in access to device information has to deal with basics such as confirming serial number validity in a totally bespoke way;
- Security approaches will differ between manufacturers, and therefore 'best practice' will not be ubiquitous;
- Devices can be compromised by attacks against manufacturer infrastructure, even though sophisticated attacks such as DNS takeover.

A distributed ledger addresses these concerns by providing a common and highly robust approach for device identity which uses the security of strong cryptographic techniques to secure the data on the ledger, coupled with the distribution of the ledger across multiple nodes to secure against scale attacks including Distributed Denial of Service (DDoS) attacks.

[15] Distributed Ledger Technology, Blockchains and Identity: A Regulatory Overview https://www.gsma.com/identity/distributed-ledger-technology-blockchains-and-identity-a-regulatory-overview.

Design considerations

It is thought likely that a hybrid public/permissioned distributed ledger would be most suitable for this use case allowing manufacturers to have the permission to read and write to the ledger, and devices and the 'rest of the world' have the permission to read the ledger. This would obviously require a process for manufacturers to be granted permission to write their information to the ledger and it is thought there could be an opportunity for mobile operators to provide such a distributed ledger to support the IoT across the globe, administering the permissions of verified device manufacturers to write to the ledger.

The immutability of distributed ledgers can create a risk to data privacy if personal information is stored on a shared distributed ledger. As such for compliance with regulations such as GDPR it is recommended that alternate ledger implementations are used with a hybrid of on-chain data that can be used to verify transactions with off-chain personal data storage solutions that effectively minimise the amount of data stored on the chain (e.g. via 'zero-knowledge proof' techniques). Solutions such as 'Sovrin'[16] (as being considered in the GSMA Identity programme) which allows users to assert their own identity but without having to disclose identity information directly through the ledger are recommended for applications which involve the use of personal data.

5.1.2 Access control

Connected things can benefit from the use of distributed ledgers to store access control details for physical or virtual resources, permit access to those resources, and record the access to those resources:

- A physical asset e.g. a smart lock is able to use a distributed ledger both to hold details of the people (or rather their keys) and times that the lock can be operated as well as to store a record of attempts and activations;
- A virtual asset e.g. a server sharing a data file can similarly use a distributed ledger to hold the identity of the persons or applications that can access the file, as well as other constraints e.g. the time period they are allowed to access it, and whether they are allowed to save, print, edit or forward that file;

As an example a common issue, particularly for consumers ordering goods online, relates to e-commerce purchases where the consumer is away from their home during the working day. In the absence of secure storage places there is a risk that online purchase deliveries might be stolen, or even not delivered. Rather than customers giving access to their homes by releasing keys/alarm codes that could be misused subsequently the access to the home could be enabled transactionally via a distributed ledger;

Further examples of access control appear in the upcoming sections.

[16] More information on Self Sovereign identity at https://sovrin.org

What are the benefits of distributed ledgers for this use case?

The key advantages of distributed ledgers for access control applications are

- It is possible to enable access to resources by specified individuals and for specific periods of time using a highly standardised solution e.g. using a common API;
- The access can be managed using smart contracts to implement more advanced rule sets;
- Access attempts can also be recorded on the distributed ledger, providing immutable traceability that deters unauthorised requests and providing a permanent record for later use;
- Permissions are replicated across nodes which ensures better availability and security against a directed attack;
- It is also possible to discontinue or revoke access to the resource which is much harder than if a PIN code, door lock code or password is provided to a third party.

Design considerations

It is quite feasible to build access control applications using a public blockchain which supports smart contracts. Ethereum, Sovrin and Hyperledger Fabric are open source projects supported by a wide range of organisations who benefit from the technologies and are contributing back to the projects to build and evolve the needed ecosystem. The Ethereum API can be integrated with access control modules and users and the smart contract used to manage access on behalf of users.

For the access of personal data, such as in the health information domain, crypto projects such as Sovrin[17] provide sophisticated support for managing consent and data privacy.

Solutions for access control can can also be built using Hyperledger Fabric, allowing the use of private/ permissioned ledgers for closed user groups. Again, this supports smart contracts for the enforcement of access control policies.

[17] More information about the use of Sovrin for health care is available at https://blog.sovrin.org/sovrin-use-case-healthcare-69faca0f1437

5.2 IoT SERVICE ENABLEMENT

The use cases described in this section can be viewed as service enablers that can add value to IoT applications.

5.2.1 Supporting compliance (smart contracts)

There are many situations in the real world where it is important to know that a process, particularly where it involves multiple parties, is being properly complied with. Compliance is efficiently enabled using distributed ledgers particularly through the use of smart contracts. For example

- With the rise in connected personal health monitoring equipment there is a benefit to individuals in sharing certain data with their health providers either temporarily whilst in a hospital or longer term. Individuals can control access to their personal health records using distributed ledgers, to make sure those records are only accessed by health professionals involved in their own care, and to record details of the health care professionals accessing the records to ensure good data governance. For example a person with a blood pressure monitor could permit this data to be shared with both their general physician as well as a pharmacy so that medicines can be dispensed as needed. This is particularly useful where there are many organisations involved in health care delivery;

- Providing low cost 'micro-insurance' for example where a person is taking a flight and can pay a small premium (e.g. £5) to insure for a £20 taxi ride on arrival if their flight is late. The smart contract in this case can trigger automatically on the arrival of the flight, determining whether the compensation is paid to the customer or the premium kept as profit by the provider. Distributed ledgers and smart contracts offer a lower cost of service delivery making micro-insurance available to a broader customer base;

- Granting access for specific persons to drive a connected hire car with smart contracts used to check that hire conditions are met e.g. that the hirer meets minimum age and experience requirements and has a currently valid driving licence. The distributed ledger can record the period of allowed access, and the 'address' of the user permitted access[18]. The same distributed ledger could also record the 'address' of the driver for billing purposes and confirming the driver for example for traffic or parking violations or occurrences where the vehicle has been driven off-road. A shared distributed ledger for this purpose is far more efficient than hundreds of different organisations (hire companies, police, licensing authorities, city parking management, road toll operators) having to integrate systems or processes;

[17] More information about the use of Sovrin for health care is available at https://blog.sovrin.org/sovrin-use-case-healthcare-69faca0f1437

- A connected car automatically uploading journey information, faults and service data to a distributed ledger holding vehicle information so that future purchasers are protected against odometer fraud leading to over-valuation of the used vehicle and manufacturers and vehicle licensing agencies can monitor and address the occurrences of common faults[19];
- Ensuring that commercial drivers of lorries, buses or delivery vans are complying with health & safety legislation such as maximum daily working time/ minimum break times, operating vehicles only if breathalyser readings are within safe limits, and 'tachygraphs' where required are fitted to vehicles. A connected vehicle can directly invoke a smart contract to ensure compliance, with records submitted to an immutable distributed ledger so avoiding the potential for fraud.

What are the benefits of distributed ledgers for this use case?

Smart contracts have been designed into many implementations of distributed ledgers such as Ethereum. The concept of the smart contract is of a software function that is itself 'stored' in the ledger, and is executed when there is a request to store a transaction. The smart contract can check for required pre-conditions being met, for example a journey might only be stored in the ledger for a vehicle if the odometer reading at the end of the journey is greater than the odometer reading at the start of the journey and the odometer reading of the start of the current journey is greater than or equal to the odometer reading at the end of the most recent journey for the same vehicle.

Smart contracts are generally executed by the nodes which maintain the distributed ledger network. This means there is extremely high reliability provided for applications through high redundancy against systems outages. Also the scalability and robustness increases as the distributed ledger network expands the number of nodes supporting the ledger. The application developer therefore does not need to provide their own systems with 100% availability to support their use cases.

The use of an 'off-the-shelf' distributed ledger provides other advantages including security best practices beyond the capabilities of many organisations (particularly small/ medium enterprises or with small/ mid-size development teams) and an 'out of the box' API for ease of systems integration.

[19] See https://cryptocurrencynews.com/automobile-blockchain-toyota-ford-gm/

Design considerations

There are various distributed ledger implementations which support the concept of 'smart contracts', the best established for public blockchain applications is Ethereum[20] and other open source projects such as Hyperledger Fabric[21] also support smart contracts.

It is practical and in many cases attractive to run smart contracts on a public blockchain such as Ethereum, this would leverage the Ethereum network to secure the network. However, it may be preferred to use an alternate technology such as Hyperledger Fabric as this firstly allows a dedicated ledger to be provided which is not competing for network resource with other users of a public blockchain, secondly allows administration of access to the ledger network using permissioning and thirdly is not subject to the usage fees associated with use of public blockchains[22].

5.2.2 Micropayments

With the close association between distributed ledgers and crypto currencies such as Bitcoin, Ethereum and IOTA there is naturally a strong fit of distributed ledgers for payments for the IoT.

Bitcoin was originally specified[23] to allow payments to be made without relying on a central authority, and as noted in the introduction solved a key problem in decentralised/ distributed payments – preventing 'double-spending'. The Bitcoin crypto currency can be bought, transferred and sold without relying on a central authority for clearing as transactions are verified by a consensus the Bitcoin network. Payments using Bitcoin and subsequently developed crypto currencies are significantly faster and generally much cheaper than payments through centralised banks, particularly where that involves inter-bank or international transfers.

In the IoT the applications for micropayments include both person-to-machine and machine-to-machine scenarios such as:

- A person purchasing a product such as a soft drink from a connected vending machine;
- A connected car paying a road toll automatically to an autonomous toll booth[24];
- A person paying for public transportation when passing through an automated ticket barrier;
- An autonomous electric vehicle paying a charging station for the energy consumed for recharging its batteries;
- Charging applications for consumption of API services;
- Charging for use of open data e.g. weather / mapping data;

[20] https://www.ethereum.org See also the Enterprise Ethereum Alliance https://entethalliance.org
[21] https://www.hyperledger.org/projects/fabric
[22] Public blockchain fees may be cost advantageous however, compared with setting up a private blockchain infrastructure, for lower volume use
[23] See the Bitcoin 'white paper' at https://bitcoin.org/bitcoin.pdf
[24] See for example 'mobility open blockchain initiative' https://www.dlt.mobi

- Smart machines which can autonomously order 'things' such as

  1. a smart refrigerator which can order fresh supplies of basic groceries,
  2. a smart vending machine which orders product refills or
  3. a smart car which can order regular consumables such as screen wash, windscreen wipers, tyres or brakes.

What are the benefits of distributed ledgers for this use case?

Compared with established payment services the following benefits are obtained when using distributed ledgers:

- The fees involved in processing transactions are much lower[25] than comparable bank or credit card fees – suiting payment amounts from the 'cent level' necessary for mass market micro-payments. At June 2018 prices the fees for using the Ripple crypto currency are around $0.54 for 100,000 transactions whereas fees for services such as Stripe[26] start at $0.30 per transaction. For comparison same day CHAPS transfers for larger payments in the UK cost £20 with the Royal Bank of Scotland[27] whereas the typical fees with Bitcoin (June 2018) are less than $0.20;
- The transaction processing time of a few seconds for the Ripple crypto currency is significantly lower than cleared inter-bank payments which are generally 'same working day but not guaranteed', and this is especially true for international payments which can take 2-5 working days for banks to process;
- Vendors are not subject to the risk of 'charge backs' for disputed purchases therefore overall costs are lowered. Smart contracts can be used to ensure the sale/purchase contract is properly fulfilled and paid for.

Design considerations

There are many public distributed ledgers including Ethereum[28], Ripple and IOTA that can be used for micro-payments depending on required scale and support for smart contracts. Ripple is already scaling to a level that compares favourably with the Visa payment network, and IOTA is designed to meet the further increased scale required to suit the IoT.

One issue with these public crypto tokens is that they are also traded as crypto assets. This means there is usually a high level of daily price volatility which may not be desirable for micro-payments related to goods/ services with low margins as there could be a risk that the seller makes a financial loss on the sale if the asset value drops. Buyers and sellers can mitigate this risk by quickly exchanging between crypto assets and 'fiat' currencies.

Crypto currencies can also be developed to be permissioned i.e. with access only to members granted specific permission. Development of new crypto currencies is made easier by the fact that most crypto currencies are themselves open sourced, and also with the availability of projects such as Hyperledger Fabric which can be used generically for asset transfers. For a permissioned crypto currency there would also need to be establishment of processes for converting fiat currencies to the crypto asset equivalent (i.e.

[25] There was a period at the end of 2017 where fees for Bitcoin payments were unusually high, a function of network congestion. Alternate crypto currencies including Ethereum, Ripple and IOTA have much lower fee structures. See https://bitinfocharts.com/bitcoin/ for current Bitcoin data.
[26] See https://stripe.com/us/pricing - fees start at $0.30 + 2.9 % of the transaction value
[27] See https://www.business.rbs.co.uk/content/dam/rbs_co_uk/Business_and_Content/PDFs/Business_Account_summarised_charges_RBS.pdf
[28] There are many other crypto tokens which are based on Ethereum's technology and network using the 'ERC20' token standard. https://theethereum.wiki/w/index.php/ERC20_Token_Standard

the process often performed by crypto currency exchanges) but this could provide an advantage in having a stable currency conversion rate. It is feasible that mobile operators could establish such a stable crypto currency network for the IoT with associated fee income rewarding the operator for establishing the network. However, local financial regulations may have significant implications that should be included in any evaluation of this potential opportunity and it is very likely that this will appeal most to operators with mobile money initiatives.

5.2.3 Data sharing and integrity

It is expected that the true power of the IoT will be enabled through the sharing of data, a process that can be made significantly more efficient using distributed ledgers. An important aspect of a distributed ledger is that it can be used to assert the integrity of IoT and associated data, effectively through the sequence of digital signatures and data hashes that are captured in the distributed ledger.

Many IoT devices are expected to send data to their manufacturer's servers as an implicit function of being 'connected devices'. Examples include intelligent thermostats which use cloud services to determine when to start/ stop heating based on weather conditions and connected washing machines which can send the manufacturer information about component wear. For these simple cases a distributed ledger is not strictly necessary as the manufacturer can design a bespoke solution – though the manufacturer might still benefit from using distributed ledger technology to avoid the need to re-invent processes such as ensuring data integrity.

There are more advanced use cases where a distributed ledger helps the wider need for sharing data outside of the immediate product/manufacturer case:

- Home/ business alarm systems can be operated by different individuals with a separation between user privileges (e.g. home owner, alarm maintainer, cleaner), also the need to send certain events to different emergency services such as police forces for intruders or fire services if smoke alarms. The 'anti-tamper' mechanism of the distributed ledger allows assertion of the integrity of significant events being recorded such as alarm enabling/ disabling that could further be of relevance to insurance claims;
- Personal fitness tracker data is additionally useful to both health care professionals looking after individuals as well as health researchers. The sharing of this data in a controlled way via a distributed ledger allows a wider range of services to be delivered than just the monitoring by the owner and fitness tracker manufacturer. In addition users might even be willing to directly monetise their fitness tracker data, using the distributed ledger to distribute the data and receive micro-payments;
- Consumers might purchase home weather station/air quality monitoring station equipment with the express intent of monetising the data by selling to interested third parties such as weather agencies. The distributed ledger then provides the mechanism for releasing data, potentially using a smart contract, and providing payment to the consumer;

- Smart Electricity Grids can use distributed ledgers to record both the amount of energy generated by a network of micro-generators e.g. home solar, solar farms or wind turbines, as well as time of day in order to determine the net payment to each individual supplier. The distributed ledger provides the immutable record of energy generated which can be audited by both parties, and if enabled for payments also allows the supplier to be paid for the energy generated. Again Smart Contracts can be used to implement the payment process according to defined rate cards – allowing much faster payment to suppliers. The distributed ledger makes this market more efficient by allowing multiple energy companies and micro-generators to participate in this market.

What are the benefits of distributed ledgers for this use case?

The key advantages of distributed ledgers for data sharing/ data integrity are

- Distributed ledgers are implicitly designed for multiple parties to read/write the information on the ledger and to be able to validate the integrity of the ledger using cryptographic techniques. Other bespoke solutions, such as a web application based on a relational data base, require considerable development and operational effort to achieve the equivalent result;
- There is no need for each manufacturer to develop their own bespoke API when using the functionality offered by a distributed ledger, the 'common' API and functionality of the ledger itself saves the manufacturer the work involved in sharing data and the partners effort connected with interfacing to multiple manufacturer APIs;
- Distributed ledgers have an inbuilt system of ensuring data integrity, and whilst there are other ways to support the checking of data integrity these require a complex bespoke build using complex system processes;
- It is possible to incorporate process into the distributed ledger through smart contracts, allowing rules to be defined around the conditions under which data is accepted to the ledger (i.e. integrity checks) or potentially shared with other parties;
- Micropayments to monetise data are easily implemented.

Design considerations

Public distributed ledgers such as IOTA are designed to support data sharing and micropayments at scale for the IoT through the adoption of a 'tangle' architecture which is designed for extremely high scalability. This addresses a key issue with ledgers such as the public Bitcoin or Ethereum ledgers which have insufficient transaction throughput to realistically support these use cases at scale for the IoT.

A permissioned ledger based on, for example, Hyperledger Fabric can also support the data sharing/ integrity use cases. This is able to support more advanced use cases and provides mobile operators with the opportunity of delivering advanced distributed ledger solutions to their customers.

It is not necessary, or even desirable, to store all IoT data on the distributed ledger. The ledger should be used to store data which is expected to be shared with multiple parties, or should be recorded for proving integrity at a later date. It is not desirable to 'clog' a distributed ledger with general data e.g. per-second battery level as this requires permanent storage across all the nodes replicating the ledger data. Another design approach to reduce 'clog' is using off-chain techniques for example where the data resides in a separate file that can be accessed by required parties but a 'hash' of that file is stored to the distributed ledger so that integrity can be verified.

5.3 IoT SOLUTIONS

This section describes use cases that can support vertical markets with specific enterprise products.

5.3.1 Supply chain

There is a great deal of publicised commercial activity in the application of distributed ledgers for improving the supply chain e.g.

- Improving the efficiency of global containerised shipping and reducing the potential for fraud through recording of environmental and location information as well as associated 'paperwork' to a distributed ledger;
- Maintaining the provenance of high value and often faked items including pharmaceuticals, cosmetics and high end fashion goods including in cases like fashion and accessories through secondary (e.g. resale) markets. The distributed ledger is used to record details of the product, producer and actions through the supply chain;
- Food safety applications where it can be important to be able to track from the original producer through the food chain to deal with issues such as biological contamination which could risk the health of many people. The distributed ledger in this case records details of both raw materials (origin, supply chain) as well as the processing plant and destinations so that it is possible to work from origin or destination in addressing any food safety issues;
- Ensuring that products can be traced as being produced ethically e.g. by factories which do not employ child labour and maintain good working conditions, or ensuring diamonds are sourced only from ethical producers.

Blockchain is useful in these cases to provide transparency of actions; the ability for many parties to add information (actions, parties and documents) to the blockchain and inspect such information; protection against criminal activity including fraud and counterfeiting; and much improved process efficiency.

The IoT enhances such applications. For example the following information, sourced from IoT devices, can be added to the blockchain

- GPS location data to store the location of the goods at periodic intervals;
- Environmental data e.g. temperature, humidity, orientation data;
- Weight/ mass of goods;
- Exceptional conditions e.g. shocks measured by accelerometer, flood, freezer power failure, opening of a shipping container, Closed Circuit TV (CCTV) movement images.

Examples of companies that are actively working on supply chain solutions include

- IBM Maersk blockchain for shipping - https://www.ibm.com/blogs/blockchain/2018/01/digitizing-global-trade-maersk-ibm/

- FedEx/ Blockchain in Transport Alliance https://www.freightwaves.com/news/fedex-bita-blockchain-logistics-plans
- Pfizer / Mediledger application of blockchain in the pharma industry http://fortune.com/2017/09/21/pharma-blockchain/

What are the benefits of distributed ledgers for this use case?

The key advantages of distributed ledgers for supply chain improvement are

- The typical supply chain today has information 'locked away' in multiple siloes from the supplier, through transportation providers and customs authorities to the end customer. Systems are not connected and much of the supply chain process involves paperwork. Distributed ledgers can transform these processes so that all actions and documentation are recorded in near real-time on a tamper proof ledger secured using strong cryptographic techniques;
- Information is available 'on-demand' to any party involved in the supply chain making it possible in near real-time to determine the current status of a product within the supply chain;
- Distributed ledgers help to eliminate fraud and corruption because of information transparency and immutability.

Design considerations

Permissioned distributed ledgers are expected to be used for many supply chain solutions addressing vertical sectors, as demonstrated already by announcements such as the IBM/ Maersk joint venture for global trade involving shipping. The IBM/ Maersk solution is based on the Hyperledger Fabric open source distributed ledger, and it would be possible for mobile operators to similarly apply Hyperledger Fabric to support local supply chain solutions.

There are also various dedicated supply chain focused crypto projects including 'Waltonchain', 'Ambrosus', 'Modum' and most notably 'VeChain'[29] which is the highest capitalised supply chain crypto token.

It would also be possible to create simple supply chain solutions on for example the Ethereum blockchain, however, as that is a public ledger there needs to be consideration regarding the protection of commercially sensitive information.

[29] Information about VeChain : https://www.vechain.org/, Waltonchain : https://www.waltonchain.org, Ambrosus : https://ambrosus.com and Modum : https://modum.io

5.3.2 Sharing economy

Peer-to-peer sharing of goods, services and other resources has been enabled through platforms such as Airbnb for home rentals. The concept of the sharing economy is applicable though to other peer to peer marketplaces such as the loan of cars and bicycles, ride-sharing services, lending of tractors and related agricultural equipment, tools, private parking spaces or even medical equipment. The sharing economy typically enables better utilisation of owned resources and usually generates fee income for the person lending out the resource, and a saving for the person loaning the resource compared with acquiring it outright for themselves or via the likes of traditional hotel bookings/car hire companies.

A key attribute of the sharing economy is that there is principally a peer-to-peer relationship, though often enabled via a bespoke platform such as Airbnb that manages certain aspects of the sharing relationship. Peer-to-peer is also a key attribute of distributed ledgers so there is a natural complement between the sharing economy and distributed ledgers.

Examples of companies already working to apply distributed ledgers to the sharing economy include

- CanYa (https://canya.io) – a marketplace for services;
- Bee Token (https://www.beetoken.com) – home sharing;
- HireGo (https://hirego.io) – car hire and sharing;
- Brixby (https://www.brixby.io) – parking and electronic vehicle charging.

The key advantage of distributed ledgers is that these enable the shared economy without requiring a totally bespoke complex systems build as required for the well-known internet platforms. There is also the integral support for payments which with the low fee structures of crypto currencies can also provide low cost micropayments relevant to sharing of even low value items.

What are the benefits of distributed ledgers for this use case?

Sharing economy solutions are clearly being developed for specific market segments as quite siloed systems. This is despite the fact that many of the concepts to the sharing economy are quite generic. Distributed ledgers offer the following benefits over the current situation:

- Distributed ledgers can be used as a generic 'platform' for the sharing of any good/ service/ resource, particularly if smart contracts are used to define any specific workflows that are required for a particular market. Fees for operating the market can also be considerably lower as a result as there is a much reduced investment needed in building the sharing platform;
- It is easy to integrate peer-to-peer payments or micropayments for the sharing economy using the 'crypto currency' features of distributed ledgers, there is no need for a user to have a bank account or credit card to make or receive payments;
- Users would not need separate accounts on each sharing economy platform to participate in multiple markets;

- Participants in the market can gain increased trust in the peers they wish to work with based on the immutable records that get stored in the distributed ledger. This can provide more trust than the typical, and often abused 'ratings systems'.

Design considerations

Public blockchain solutions such as Ethereum can easily support sharing economy applications, using the distributed ledger for agreeing the contract between parties supported by smart contracts, enabling global payments with a competitive fee structure, and providing the immutable record of transactions that is useful in building trust amongst users.

The example sharing economy services listed earlier are all based on the distributed ledger project 'Origin Protocol'[30] which in turn uses the Ethereum blockchain as part of its solution. Origin Protocol could be used by mobile operators to deliver sharing economy services in a country based on the Ethereum blockchain.

[30] https://www.originprotocol.com/en/product-brief

6. Relevant solutions

There are now hundreds of crypto currencies, tokens and solutions which target different applications including use in the IoT. Listed below is a small selection of solutions which are considered appropriate for use in the IoT.

6.1 Hyperledger

The Linux Foundation backed Hyperledger project (https://www.hyperledger.org) provides a number of open source distributed ledger solutions. This includes the general purpose Hyperledger Fabric[31], a project developed in conjunction with IBM which the company offers commercially to enterprise customers (such as used in the IBM Maersk joint venture).

Hyperledger Fabric has been used to develop proofs of concept including document management, authentication, KYC (Know Your Customer), supply chain transparency and banking/ finance. Fabric also supports smart contracts and permissioned distributed ledgers.

6.2 IOTA

IOTA (https://iota.org) is described as a 'next generation blockchain' focused on use in the IoT as a 'ledger of things'. IOTA uses a revised distributed ledger design known as a 'tangle'[32] which aims to be massively scalable as well as avoiding the cost of replicating all data to all nodes. The IOTA foundation is working with companies including Orange, DT, Volkswagen, Microsoft, Fujitsu and Bosch[33].

IOTA supports micro transactions, data transfer, voting and broadcast messaging. IOTA is also a crypto token which can be used for micro transactions between parties. No 'mining' is required for IOTA tokens, and there is no fee for access to the IOTA DLT as each node which participates on the network validates two random unconfirmed entries on the tangle.

[31] https://www.hyperledger.org/projects/fabric
[32] http://iota.org/IOTA_Whitepaper.pdf
[33] https://oracletimes.com/bosch-group-has-purchased-a-significant-amount-of-iota-miota-tokens/

6.3 Ethereum

The second best known and valuable crypto currency Ethereum (https://www.ethereum.org) provides a foundation for applications as well as a means for the transfer of value in the form of the crypto currency. Ethereum supports smart contracts (described in section 2.2) which are relatively small code functions that are executed directly by the nodes supporting the Ethereum network. In addition other 'tokens' can and have been built onto the Ethereum technology platform (using a protocol known as ERC-20[34]).

These smart contracts are scalable and highly available as they benefit from the scalability and availability of the Ethereum network. Smart contracts can be used for example to trigger payments for goods subject to external conditions such as having the correct paperwork in place for transportation and customs clearance along with maintenance of correct transportation conditions as measured by related IoT sensors.

[34] https://github.com/ethereum/EIPs/blob/master/EIPS/eip-20.md

6.4 Ripple

Ripple (https://ripple.com) describes itself as the '... enterprise blockchain solution for global payments', and is designed to address the complexities and delays inherent in inter-bank payments and settlements. As with Ethereum there are two facets to Ripple, one as a crypto currency in its own right which enables users to directly transfer funds to other users. The second facet is 'RippleNet' which is used for business to business funds transfer by banks, exchanges and corporates.

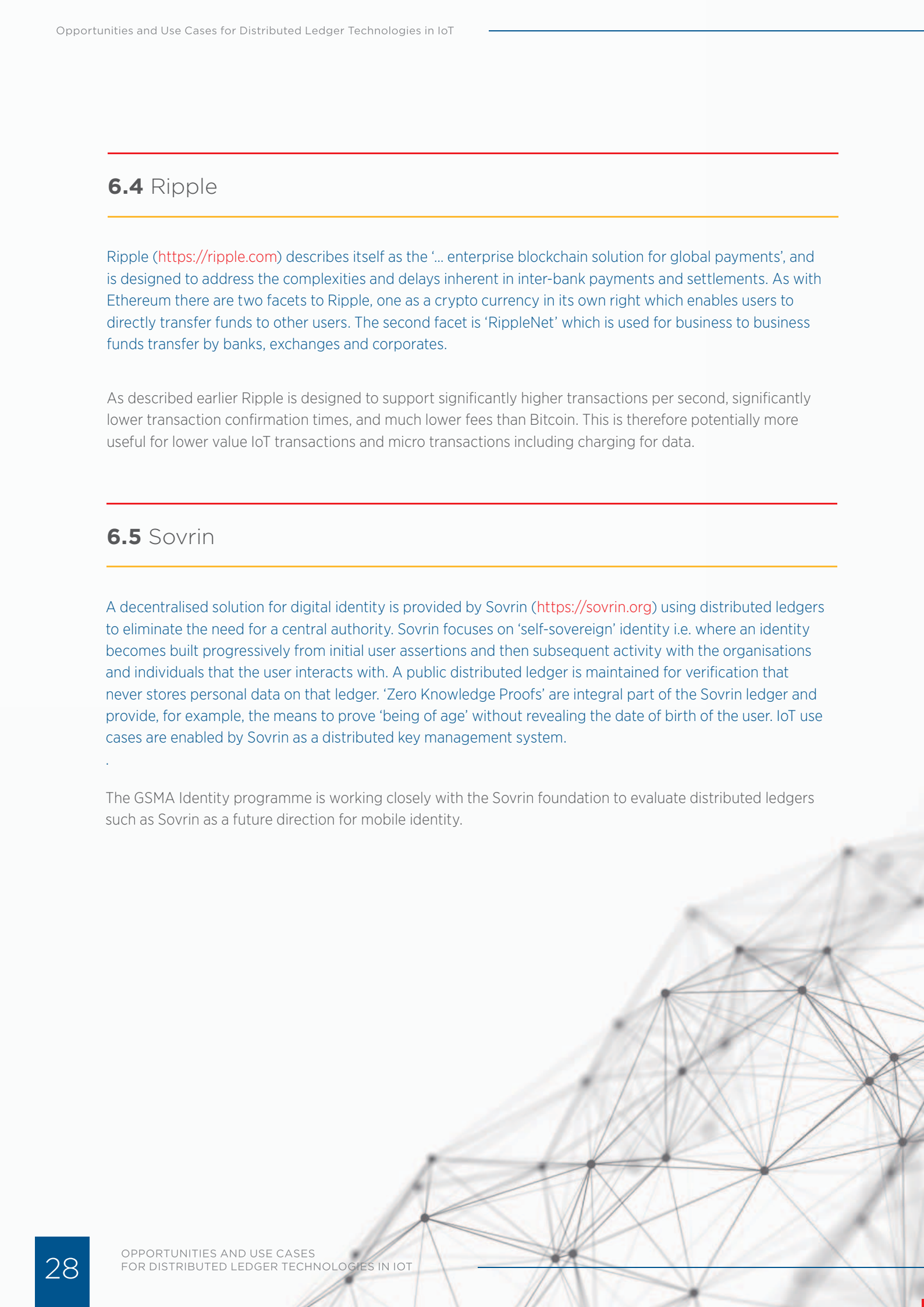
As described earlier Ripple is designed to support significantly higher transactions per second, significantly lower transaction confirmation times, and much lower fees than Bitcoin. This is therefore potentially more useful for lower value IoT transactions and micro transactions including charging for data.

6.5 Sovrin

A decentralised solution for digital identity is provided by Sovrin (https://sovrin.org) using distributed ledgers to eliminate the need for a central authority. Sovrin focuses on 'self-sovereign' identity i.e. where an identity becomes built progressively from initial user assertions and then subsequent activity with the organisations and individuals that the user interacts with. A public distributed ledger is maintained for verification that never stores personal data on that ledger. 'Zero Knowledge Proofs' are integral part of the Sovrin ledger and provide, for example, the means to prove 'being of age' without revealing the date of birth of the user. IoT use cases are enabled by Sovrin as a distributed key management system.

.

The GSMA Identity programme is working closely with the Sovrin foundation to evaluate distributed ledgers such as Sovrin as a future direction for mobile identity.



6.6 BigchainDB

The open source project BigchainDB (https://www.bigchaindb.com) offers blockchain type services (asset transfer, immutability) combined with true NoSQL database functions for data querying. Distributed ledgers or blockchains are often called databases, however, whilst the storage is structured effectively for validating the integrity of the ledger and ensuring immutability there is not really the high performance database functionality that is required by application developers such as for returning a set of ledger entries matching a particular criteria. BigchainDB uses a decentralised, distributed NoSQL database (MongoDB) as the basis for its blockchain solution allowing the application to efficiently search the ledger.

7. Complement to edge computing

Edge computing is also by nature distributed and often also decentralised therefore bearing similarities to distributed ledger technologies. With edge computing there is a movement of processing out from typical centralised servers or cloud platforms. Distributed ledgers can therefore provide edge computing environments with a complementary technical platform to support applications at the edge and similarly edge computing platforms can be useful to support distributed ledgers.

Some of the options for edge computing

- Lower end edge devices with limited storage space, communications bandwidth and processing power are not really suitable to support resource intensive Bitcoin or Ethereum like distributed ledgers but can utilise the services of a distributed ledger network (e.g. using an API) or be a member of an IOTA style distributed ledger network;
- 'Gateway' devices such as a home gateway could potentially support blockchains such as Bitcoin and Ethereum as it is possible to use even a Raspberry Pi as a 'full node'. However, the requirement for large amounts of disk storage adds cost and complexity which would make it more likely this would be reserved for higher end gateway products. Lower end gateways, and connections with limited bandwidth, are more likely to use solutions like IOTA or access the distributed ledger network using an API;
- High end edge nodes such as industrial controllers, smart building controllers and enterprise systems would be able to run more capable distributed ledger solutions such as Hyperledger or Ethereum. Maintaining a local copy of the distributed ledger provides for local high performance access to the data held on the ledger as well as continuity in the case that connectivity to the Internet may be disrupted;
- Mobile edge computing nodes (i.e. deployed in the carrier network) can be used to build new distributed ledger solutions offered by carriers typically to enterprise customers as a permissioned distributed ledger. The delivery by carriers benefits customers across government and enterprise as they do not have to build their own enterprise blockchain.

8. Operator opportunity and potential next steps

8.1 Operator opportunity

8.1.1 IoT Foundation

For mobile operators participating in the IoT, there is a potential opportunity to play a foundational role by providing, or enabling, IoT foundation services such as device identity or access controls.

With device identity for example, mobile operators could collectively provide a distributed ledger to support the IoT across the globe, administering the permissions of verified device manufacturers to write to the ledger. A hybrid public/ permissioned distributed ledger could allow manufacturers to have the permission to read and write to the ledger, and devices and the 'rest of the world' have the permission to read the ledger.

Mobile operator network infrastructure already manages devices, data and security and there is an opportunity to build on these existing capabilities and further strengthen their position in Connectivity and Device Management roles.

8.1.2 IoT service enablement

As the number of IoT solutions and propositions proliferate, and as mobile operators move up the value chain, there is an opportunity to deliver horizontal enablers, not only for operator's own services but for end customers and the ecosystem broadly. Mobile operators can become the "glue" between different IoT systems and solutions utilising experience in deployment and system integration.

A distributed ledger technology capability would enable mobile operators to act in this role, ensuring that their IoT systems interoperate with others. For example, a distributed ledger that received and validated information about a smart vehicle entering a city's congestion zone, can trigger smart contract authorisation for the congestion zone charge to be automatically debited from the car owner's bank account, and a notification can be sent to the end user. This type of system interoperability, along with core distributed ledger features features such as immutability, will

be particularly important for SME customers who may not have the resources to invest in bespoke interoperability or systems integration. Research carried out by the GSMA and IDC[35] indicates that mobile operators could benefit from developing 'off the shelf' IoT propositions to meet the needs of the SME market. Developing horizontal enablers for the easy replication of interoperable IoT propositions is a potential opportunity.

8.1.3 IoT solutions

Some operators are moving even further up the value chain providing end-to-end services for selected verticals. Some verticals have particularly complex ecosystems where many players require access to data, records and/or transactions.

One example is IoT and distributed ledger combined together to support food production and distribution. In some food offerings, provenance is very important to the end customer, and can have a significant impact on the price of the commodity. IoT sensors can track and validate the relevant development and distribution lifecycle for certain produce and the distributed ledger can record and validate the immutable facts.

Similarly in the Sharing Economy data collected from various sources including IoT sensors can be validated and immutably recorded enabling use cases such as cycle or vehicle sharing.

Building distributed ledger capabilities, either independently as part of a horizontal enabler or in partnership with the vertical ecosystem, could enable mobile operators build a comprehensive and secure end-to-end service for these verticals.

[35] Link to "Beyond Connectivity New Roles for Operators in the Internet of Things (GSMA – IDC)

8.2 Potential next steps

A number of options are envisaged for potential next steps for DLT in IoT. For more information contact IoT@gsma.com

8.2.1 Common framework

- Define 'end user'[36] requirements and user stories for key mobile operator use cases
- Develop an architectural blueprint for operators wishing to develop IoT propositions that utilise distributed ledgers.
- Evaluate the opportunity for cross operator IoT distributed ledger solution for one key use case (e.g. supply chain, device identity)
- Work with relevant parties to develop an IoT sandbox implementation for operator investigation.

8.2.2 Evaluate solutions

- Define key criteria for assessing distributed ledger technologies (latency, security etc.) and evaluate a selection of existing solutions (Hyperledger Fabric, TBCASoft etc.)
- Support the effective evaluation of potential solutions, by collating best practice criteria from mobile operators for selecting a DLT solution.

8.2.3 Operator role

- Whilst distributed ledgers are an important technology it is important to understand how these can be turned into or used within business opportunities offered by operators. Value chain mapping for key use cases may help mobile operators pinpoint potential roles and opportunities that can be pursued.
- Document relevant operator activities and case studies that demonstrate the opportunity for mobile operators to use DLT within the IoT.

[36] Such as business or enterprise customers, IoT partners.

9. Glossary

51% ATTACK – this is a method of attack against public distributed ledgers (Bitcoin, Ethereum etc. which use consensus algorithms such as 'Proof of Work') which allows an attacker to 'rewrite' the most recent part of the ledger historical record. This attack requires concerted computing power to achieve at least 51% of the 'network processing power' and is essentially not commercially viable against the large ledgers like Bitcoin or Ethereum. It has been used against a limited number of some of the smaller crypto-currencies that have small networks of validating nodes (miners).

See also https://medium.com/coinmonks/what-is-a-51-attack-or-double-spend-attack-aa108db63474.

ADDRESS – Addresses are used when sending data/ payments to another party using the distributed ledger. They are typically derived from the Private Key of the other party and help preserve anonymity of the other party.

See also https://blockgeeks.com/guides/blockchain-address-101/

API – Application Programming Interface, the means by which an application can consume services provided by a third party system. In this case the relevance is APIs that allow applications to consume distributed ledger services e.g. sending data or a payment to another party.

BITCOIN – The first, successful, implementation of a decentralised method for supporting payments between parties without needing any centralised function for example for payments clearing.

See also https://bitcoin.org/en/

CONSENSUS – A mechanism that is used in distributed ledgers whereby the decentralised parties come to a consensus on what represents 'truth' given that there is no centralised arbiter of such truth. Consensus is achieved by multiple participants (nodes) validating both the transactions and the contents of the ledger and signalling their support that everything is correct.

See also https://unblock.net/cryptocurrency-consensus-algorithms/

CRYPTO CURRENCY - a 'digital currency' which builds on cryptographic techniques as part of its design. Generally synonymous with there being a decentralised design and no party in a position of control or scrutiny of the parties transacting. Crypto currencies are generally designed around a distributed ledger which has consensus established by multiple network nodes.

See also https://cointelegraph.com/bitcoin-for-beginners/what-are-cryptocurrencies

CRYPTOGRAPHIC SIGNATURE – a method of signing a digital asset (e.g. a transaction on a distributed ledger) that allows any party with access to a 'public' key to verify that the party with the corresponding 'private' key generated a digital signature for that asset (e.g. payment transaction). This allows the recipient to be sure that no change to the asset was made since it was originally generated.

See also https://www.ibm.com/developerworks/cloud/library/cl-blockchain-basics-intro-bluemix-trs/index.html

DISTRIBUTED LEDGERS – an online record, which is replicated across two or more system nodes, forming a record of transactions between parties using the ledger. Sometimes also called distributed databases but somewhat different from these in that the ledger is constructed by a distributed process without the need for a centralised control function.

See also https://www.coindesk.com/information/what-is-a-distributed-ledger/

DL – see distributed ledgers

DLT – distributed ledger technology, the specific implementation of a distributed ledger, Bitcoin, Ethereum, Hyperledger Fabric, IOTA are all examples of distributed ledger technology implementations.

ETHEREUM – After Bitcoin, Ethereum is currently the 'second largest' (by market capitalisation) crypto-currency. Ethereum importantly supports the concept of generalised 'smart contracts' and allows custom crypto tokens to be delivered using a standardised mechanism built into Ethereum.

See also https://www.ethereum.org

GENESIS BLOCK – the very first 'block' in a distributed ledger, generated by the 'creator' of the distributed ledger and used by any network participant as part of the validation of the distributed ledger.

See for example https://en.bitcoin.it/wiki/Genesis_block

HASH – a method of computing a 'check value' on data so that a recipient is able to check that the data has not been tampered with since created by the originator. 'Hashes' are used extensively in cryptography, crypto-currencies and distributed ledgers to allow parties to check that data (e.g. transactions) have not been modified.

See also https://en.wikipedia.org/wiki/Cryptographic_hash_function

HYPERLEDGER – an organisation, hosted by the Linux Foundation, aiming to advance open source blockchain (distributed ledger) technologies. As part of its work Hyperledger has made available a number of technical implementations of distributed ledgers, for example 'Fabric', which can be used to support customer implementations.

See https://www.hyperledger.org

IOT – Internet of Things, enabling communication, over the Internet for everyday devices, home appliances, vehicles, sensors, actuators, industrial machines etc.

For further information on GSMA activities related to the IoT see https://www.gsma.com/iot/

IOTA – An 'IoT' focused implementation of distributed ledgers which aims to address important issues relating to the IoT around the expected number of IoT devices, the limitations of many of those devices, and requirements for data exchange and micro-payments.

See https://www.iota.org

MINER – this is a computing device which provides computer power to public distributed ledger networks (such as Bitcoin and Ethereum) for use in validating transactions and achieving consensus. A 'reward' is distributed to the miners (or more correctly the individuals or organisations that own the devices) that contribute computing power to incentivise the miners to validate transactions and consensus.

See also Mining below and https://www.webopedia.com/TERM/C/cryptocurrency-mining.html

MINING – see also Miner. Mining involves the use of high performance computing to solve complex computational tasks and as a result receive rewards in the form of a share of 'block rewards' that are incentives issued to the first system to solve the set problem (the 'problem' is set via the design of the relevant crypto currency). Mining is a competitive task in that the first 'system' or 'pool' that finds an answer to the mining problem will receive the block rewards. Miners generally 'pool' their efforts to improve their chances of obtaining a reward.

NODE – in the context of distributed ledgers this principally means any device which maintains all or part of the distributed ledger record. A distributed ledger requires at least two nodes, but increased resilience and scalability is obtained when many more (even hundreds or thousands) of nodes come together to support the network. Note that there can be orders of magnitude more users of the distributed ledger than nodes that record the distributed ledger.

For further information see https://www.investopedia.com/terms/f/full-node.asp

PRIVATE KEY – Related to cryptography a private key is a unique, generally exceedingly long, numerical value that is used to sign data (see Cryptographic signature) or decrypt data. The private key is never disclosed by the owner to any party. In crypto-currencies the 'Private Key' ensures only the 'owner' can spend their currency.

See https://en.bitcoin.it/wiki/Private_key

PROOF OF WORK – A mechanism for consensus on public distributed ledgers such as Bitcoin and Ethereum which 'secures' the network against attacks by malicious parties by requiring computationally complex processing to be performed when verifying new transactions. This is normally associated with 'mining' (see above).

PUBLIC KEY – Related to cryptography a public key is paired with the owner's private key and can be used by a third party either to check that the owner signed data / transactions, or alternatively can be used to encrypt data that only the owner of the private key can decrypt.

See also https://en.wikipedia.org/wiki/Public-key_cryptography

SMART CONTRACT – This is a 'self-executing' contract that can be implemented in software code and is frequently associated with monetary (or at least crypto currency) transactions. Smart contracts are executed by the nodes of the distributed ledger which means the processing benefits from the same decentralisation as the ledger itself.

See https://www.investopedia.com/terms/s/smart-contracts.asp

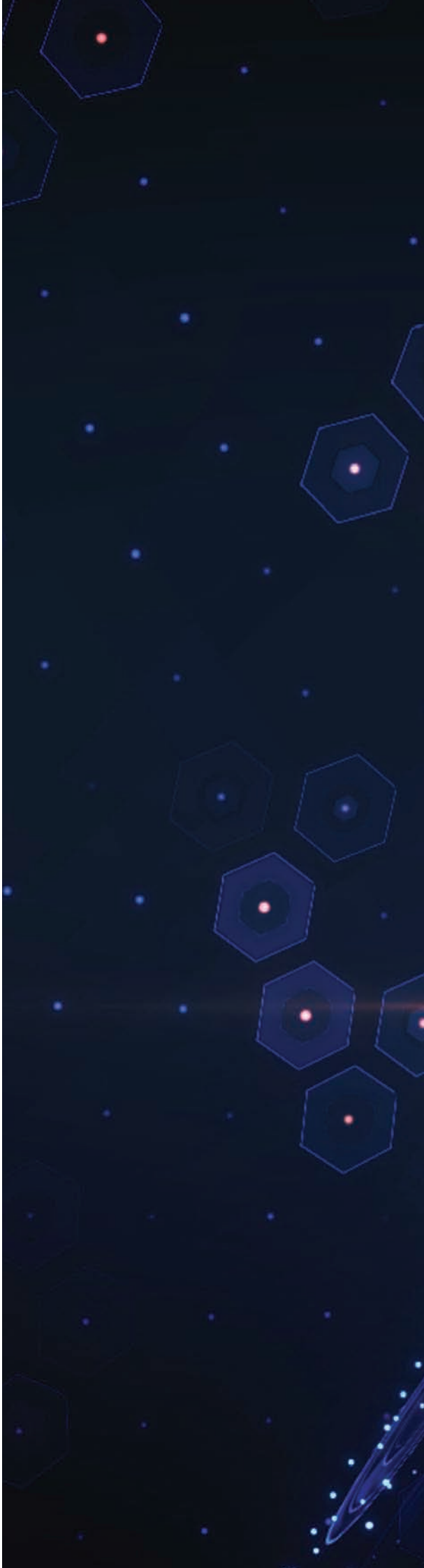
TANGLE – A design of 'distributed ledger' developed by IOTA that differs from the typical sequential ledger (of Bitcoin or Ethereum) to support massively higher scalability suitable for the IoT. Specifically the IOTA distributed ledger uses a design known as 'Directed Acyclic Graph' which features shorter 'strands' of ledger.

For more information see https://blog.iota.org/the-tangle-an-illustrated-introduction-4d5eae6fe8d4

WALLET – In crypto-currencies, a wallet is used to manage virtual currencies belonging to the owner. The wallet is the direct interface that a user interacts with to send and receive virtual currencies – and that in turn uses the APIs of the respective distributed ledger network to generate transactions when spending funds, or checking the receipt of funds. The user's private and public keys are in reality what is stored in the wallet, and not the funds themselves.

See also https://en.wikipedia.org/wiki/Cryptocurrency_wallet

For more information please visit:
www.gsma.com/IoT



GSMA HEAD OFFICE
Floor 2
The Walbrook Building
25 Walbrook
London EC4N 8AF
United Kingdom
Tel: +44 (0)20 7356 0600
Fax: +44 (0)20 7356 0601