WHITE PAPER V2.0 AUG 2018

DIADEM

A FLEXIBLE MOBILE TELECOM CONTRACT AND BILLING SOLUTION BUILT WITH BLOCKCHAIN TECHNOLOGY

TABLE OF CONTENTS

TABLE OF CONTENTS

APPENDIX

Disclaimer:

The purpose of this document is to present the Diadem project to interested parties and to provide them with sufficient information to enable them to determine whether they wish to be further involved in the development of the project. In no way should this document be construed to constitute a prospectus or solicitation for investment. This document has not been prepared in accordance with any regulation or laws of any jurisdiction, and any interested parties should satisfy themselves that under the laws of their relevant jurisdiction they are legally able to engage or invest in such a venture.

This is an initial overview of the project. The contents of this paper are liable to change as is the direction, scope, progress, and prospects of the project. This paper does not form a contract or agreement in any way.

Copyright

Statement:

EXECUTIVE

Summary

The Diadem solution provides a billing, payment, and subscriber contracting system for Mobile Network Operators (MNO) using de-centralised smart contracts on a blockchain platform. Handling contracting and billing processes on a blockchain platform as opposed to the operator's traditional support systems provides huge benefits for MNOs such as contract flexibility and transparency, additional security, cost reduction, and scalability.

There are over 7 billion global mobile service subscribers generating trillions of calls, messages, and data sessions annually. Servicing this demand whilst attempting to offer compelling propositions in a highly competitive market environment is an ongoing challenge for all MNOs. In many cases, MNOs are constrained by ageing billing systems or traditional ways of forming a contract with the subscriber.

Legacy mobile business support systems have mostly been built around the ability to deliver a simple handset and combi tariff, generate a regular paper or electronic bill for the subscriber, and to take payment via a direct debit or payment card. However, now there is an increasing need for MNOs to offer different products, to provide pricing and payment flexibility, and to provide a better and more immediate experience for the subscriber.

The Diadem solution will lever the innate ability of blockchain technology to provide a secure and decentralised environment and the power of electronic smart contracts to provide an alternative billing, payment, and subscriber contracting architecture for MNOs.

The Diadem solution aims to improve the experience in many key use cases in which Mobile Network Operators currently experience constraints, find difficult to deliver change, or which require significant overhead costs to service. The initial use cases for consideration have been drawn from the Project Team's extensive combined experience of working with MNOs. Further use applications for the solution will be developed as the project progresses and the team will seek MNO partners to gather further insight into potential operational 'pain-points'.

There are real-world problems which can potentially be resolved using blockchain and smart contract technologies, and there is huge potential for a solid business to be built from the Diadem project. One of the key strengths of Diadem is that the project was initiated by identifying tangible and immediate business problems that the team believes can be addressed by current or forth-coming technology, rather than building a 'template' platform and then searching for viable use cases.

Project Introduction

1.1. Purpose and status of Document

This document is an initial overview of the Diadem intended to give potential partners and investors an overview of the objectives and possibilities of the project. It will describe the business problems that exist in the mobile telecoms sector which could be addressed by the application of blockchain technology. It will outline some of the use cases that the Diadem solution could support and provide a high-level summary of the Diadem architecture. Finally, it will give a rough idea of the delivery plan for the Diadem project.

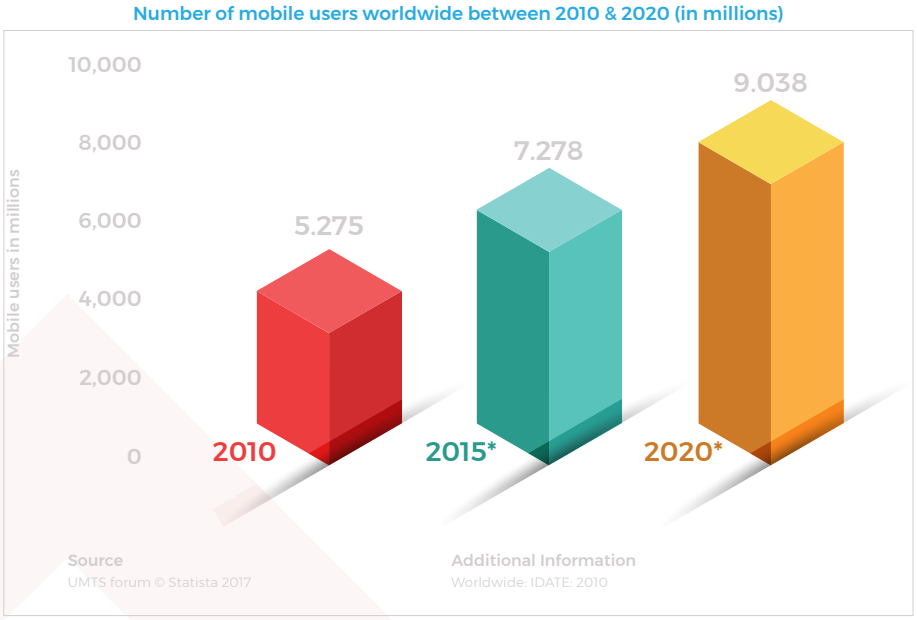
1.2. The Market Size

The global mobile telecoms market continues to grow. In developed markets where handset and subscriber levels have plateaued, Mobile Network Operators are increasingly focussed on growing the average revenue per user by offering new products and improving customer satisfaction. Furthermore, MNOs are now looking to expand their future connection base from emerging technologies such as the Internet of Things (IoT). In less developed markets, handset and tariff uptake remains strong.

Key facts and figures

- Total mobile revenues reached $1.05 trillion in 2016 .
- In 2015, the mobile ecosystem generated 4.2% of global GDP1.
- Operator investments totalled around $880 billion between 2011 and 20151
- The number of mobile phone Subscribers continues to grow:

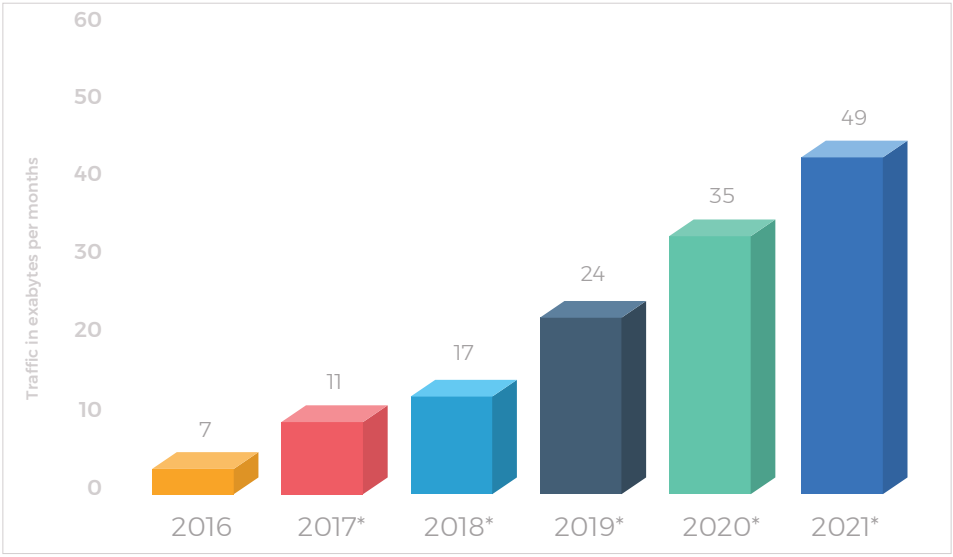
Source: GSMA 'The Mobile Economy' 2017.



- The average mobile phone subscriber in the U.S and Europe is estimated to make over 8 calls per day or 3,000 phone calls per year.
- In June of 2014, 561 billion text messages were sent worldwide, an average of 18.7 billion texts sent every day. not including app-to-app 'data' messages.

The amount of data traffic is forecast to continue to grow massively each year:

Global mobile data traffic from 2016 to 2021 (in exabytes per month)



Source
Cisco System © Statista 2017

Additional Information
Worldwide: IDATE: 2010

Statistics for the number of global usage events (calls, SMS, and data sessions) per year do not exist, but a calculation based on the above statistics suggests a figure of over 300 trillion usage events are completed every year.

1.3. Challenges in the Mobile Telecoms Industry (the Problem)

Mobile Network Operators typically aim to expand for rapid growth of their subscriber base upon market entry and to secure a significant subscriber share. This puts pressure on the maintenance and improvement of business support systems (BSS) - the rapid growth phase is delicate and disruption of operations can impede the influx of new subscribers. Many MNO business support systems are 'legacy' systems - increasingly unable to offer the flexibility needed to deliver new products and services, but difficult to change.

Billing systems in particular, are often problematic for MNOs. They often carry a high overhead in terms of the operating cost and the specialist resources needed to implement changes. In addition, some legacy billing systems are approaching capacity limits which could present a real problem if the operator wishes to enter the Internet of Things (IoT) and machine-to-machine (M2M) markets where the processing of large numbers of call records is required.

As the market has matured and the subscriber base has become increasingly saturated, many operators have shifted their strategy to focus on customer retention and to offer increasingly flexible and diverse propositions to their subscribers. However, they are often hampered in their efforts to do so by the dated nature of BSS architecture and the inflexibility of traditional software solutions.

Traditional contract forms and tariff/service structures, enshrined in inflexible billing and pricing systems, are now handicapping the rollout of new proposition and product offerings; product marketing departments are developing new bundles, tariffs, and services but are frustrated by the time needed to get them to market as delivery projects must manage numerous complex system changes to implement minor product improvements.

In addition to the inflexibility and cost of many BSS systems, their bespoke or proprietary nature results in them often forming 'silos' of data, meaning that it is difficult to extract information and expose or transfer the data to other systems. Operators are under increasing pressure to improve the transparency of contracts and ensure their subscribers are getting value for money. In most countries, there are regulatory targets around the accuracy of billing which can be difficult to meet.

Most operators would like to offer better digital tools for customer service and reduce the need for expensive call centres, but are hampered from doing so by the need to integrate with complex BSS systems.

The current state of BSS systems is a primary issue holding back progress and efficiency in the MNO sector.

1.4. What Is Blockchain Technology?

Blockchain is a peer-to-peer technology which provides a de-centralised and secure distributed ledger of digital assets by distributing that data throughout a wide network of computer nodes which constantly verify and secure the contents.

De-centralised - Data is not stored in a single (or small set of) location/s but instead is shared across the blockchain network. The network is fundamentally resilient and has no-single vulnerability for hackers to exploit. The abstraction of data from traditional architecture also means that it also far more accessible and in effect works like a shared distributed database.

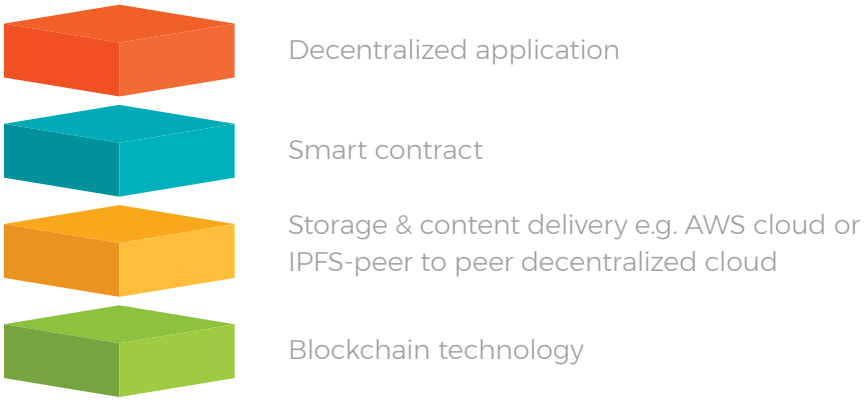
Distributed Ledger - Most blockchain platforms feature the concept of a record of transactions and processes called a distributed ledger which can be openly, transparently scrutinised by all members of the network. Transactions across the network need to be verified by a number of network 'nodes' before they are accepted as validand this concept of consensus ensures that data in the blockchain is incorruptible and cannot be altered by any single entity. Because the members or nodes of the network need to all 'agree' on the validity of new data, the network is highly secure and far less vulnerable to attack than traditional architecture.

Secure - Data is secured using cryptographic keys, sequences of numbers and characters which act as passwords to decipher encrypted data. Although the transaction history of an asset can be seen, the contents can only be changed with an appropriate key. The distributed nature of blockchain networks ensures that the ledger cannot be compromised by a single entity and requires many network nodes to mutually confirm a transaction or contract in order to update the ledger, disempowering potential bad actors.

Blockchain was initially launched as the underlying protocol for the BItcoin network as a means to provide a de-centralised method of exchanging the digital asset peer-to-peer. However, developers quickly realised the potential for blockchain to transact and store many different types of digital assets and information. In theory any information which can be digitised, from text to sound and image files, can be used as a digital asset.

There are many different blockchain technologies, with two examples listed below:

- Ethereum.
- Hyperledger Fabric.



De-centralised applications (DApps) are one use case of blockchain platforms which allow software to be deployed on a network and operate with little to no oversight or maintenance.

When choosing a blockchain platform, the following points are key to building a dDApp with blockchain technology.

- Platform
- Consensus algorithm
- Network technology
- Cloud storage
- Scalability
- Smart Contract
- Currency

The following table illustrates the differing approaches to the above key points taken by two blockchain platforms:

	Ethereum	Hyperledger Fabric
Platform Type	Generic blockchain platform	Modular blockchain platform
Consensus algorithm	Proof-of-work	PBFT (Practical Byzantine Fault Tolerance)
Network	Permission less, public or private	Consortium (Permissioned), private
Smart Contract	Smart contract code e.g. Solidity	Smart contract code e.g. Go, Java
Currency	Ether or Tokens via smart contract	Currency and tokens via chaincode.
Scalability	Scalable	Consensus algorithms
	implementation of Ethereum is achieve business transactions	supports scalability.

Platform

Hyperledger Fabric, Corda and Ethereum platforms have very different visions with respect to possible fields of application. Development of Corda is based on financial services applications. Fabric provides a modular and extendable architecture that has various applications in different industries, from banking and healthcare over to supply chains.Ethereum is independent and very generic for its field of application, with a great many DApps performing various functions running on the platform.It is not modular in contrast to Hyperledger.

Consensus

With Ethereum, all participants have to reach consensus over the order of all transactions that have taken place, irrespectively of whether a participant has taken part in a particular transaction or not. The order of the transactions is crucial for the consistent state of the ledger. This is to prevent one of the biggest challenges faced by digital asset networks - double-spending. If a definitive order of transactions cannot be established there is a chance that double-spends might have occurred, that is, two parallel transactions transfer the same coin to different recipients, thus making money out of thin air and compromising the network. As the network might involve mutually distrusting and anonymous parties, a consensus mechanism has to be employed that protects the ledger against fraudulent or adverse participants that attempt double-spends. In the current implementation of Ethereum, this mechanism is established by mining based on the proof-of-work (PoW) scheme. All participants have to agree upon a common ledger and all participants have access to all entries ever recorded.

The consequences are that PoW unfavourably affects the scalability, the networks ability to process greater volume of transactions at high speeds as the amount of network users grows. Transaction records on the network are pseudonymous - while a user's personal details are not attached to their transactions, the records of the amounts each public key (much like an 'account' on the blockchain) sent and received are visible. If a public key can be linked to a specific party their entire transaction history is visible, which is problematic for applications that require a higher degree of privacy.
In contrast to Ethereum, Fabric and Corda interpretation of consensus is more refined and does not merely boil down to mining based on PoW or a derivative thereof. Due to operating in a permissioned mode, Fabric and Corda provide a more fine-grained access control to records and thus enhance privacy. Furthermore, a gain in performance is achieved as only parties taking part in a transaction have to reach consensus.

Smart Contract

Smart contracts code is designed to be written in the programming language Go or Java for Fabric, in Solidity for Ethereum, and in Java or Kotlin for Corda. In Fabric, the term "chaincode" is used as a synonym for smart contract. As an illustrative example, the reader is reminded of the usage of a smart contract code in the consensus mechanism of Corda in order to ensure transaction validity.
However, there is a notable difference between Fabric and Ethereum on the one hand and Corda on the other that is connected to the second way the "smart contracts" term is used. For Corda, smart contracts not only consist of code but additionally are allowed to contain legal prose. The Corda was explicitly designed to account for the highly regulated environment of the financial services industry. Both Fabric and Ethereum lack this feature.

Currency

Operational costs on the Ethereum platform are paid for with the network's native, built-in cryptocurrency which is called Ether. It is used to pay rewards to nodes that contribute to reach consensus by mining blocks as well as to pay transaction fees. Therefore de-centralised apps (DApps) can be built for Ethereum that allow monetary transactions. Furthermore, a digital token for custom use cases can be created by deploying a smart contract that conforms to a predefined standard for one's own currencies or assets.

Fabric and Corda do not require a native cryptocurrency as consensus is not reached via mining. With Fabric, however, it is possible to develop a native currency or a digital token with chaincode. For Corda, a digital currencies or tokens is not possible. It should be noted that Ethereum was designed and launched prior to the development of Corda and Fabric, both of which had the opportunity to learn from the rapid innovation in the field and develop more bespoke and contemporary systems.

Scalability

Scalability refers to the ability of a blockchain platform to handle the increasingly high volume and speed of transactions as the user base grows. The nature of first-generation blockchain platforms made scalability a major issue - for example, the Bitcoin network provides a complete record of every transaction ever processed since the launch ten years ago. The more data that the network stores and the more people using the network, the more congested the network becomes pending efficient scaling solutions. It is not uncommon for certain applications on these networks to requires thousands of tps (transactions per seconds). Below are the tps capabilities seen on different block-chain platforms:

- Bitcoin: 6 tps
- Ethereum: 20 tps per node, or 7 tps per node for ERC 20 smart contracts per node.

As the consensus algorithm used by the underlying platform provides the highest level of security, it also comes at a cost of scalability. The consensus algorithm is such that every node in the network can validate, authenticate and process every transaction on the blockchain. Recall that blockchains have one inherent critical characteristic—"de-centralisation"—which means that every single node on the network processes every transaction and maintains a copy of the entire state.

Scalability solution

Ethereum in effort to provide scalable solution, it is proposing to provide two-layer solution to provide transactions and smart contract scalability.

- Layer 1 sharding
- Layer 2 sidechain (off-chain transactions) e.g. Plasma.

There are two main paths to improving blockchain scalability. The first ("sharding") involves creating better-designed base-layer blockchain protocols, which still maintain most of the desired de-centralisation and security properties of a blockchain that we see in the simple designs available today but only require a small percentage of nodes to see and process every transaction, allowing many more transactions to be processed in parallel at the same time.

The second involves creating "layer 2" protocols that send most transactions off-chain and only interact with the underlying blockchain in order to enter and exit from the layer-2 system and in the case of attacks on the system.

Among of the assets that can be housed in the Blockchain are smart contracts - secure code containers which can not only store contractual information but can execute changes and operations depending on certain pre-established conditions. This 'self-execution' allows the contracts to function outside of traditional architecture and therefore to be far more flexible and accessible.

The combination of the accessibility and security of Blockchain network platforms with the functionality of smart contracts has huge potential in many areas. Previously many projects have focused on building the core Blockchain and Smart Contract platforms, but as this development matures new projects such as Diadem are emerging which can look at how this combination of technologies can be applied to solve specific real-world problems.

1.5. How Diadem will solve the problem through use of the blockchain

The Diadem solution applies blockchain technology to overcome many problems around the cost, flexibility, and scalability of business support systems faced by MNOs, and to provide extensive opportunities to enhance product offerings and customer experience.
These include:

A shared view – the smart contract is abstracted from the Operator and exists on the blockchain allowing direct interaction by both Operator and Subscriber. Both parties can inspect the contract for full transparency and have a shared view of billing and contract situation; this will reduce misunderstandings and reduce billing enquiries.

New products, services and bundles - The abstraction of the contract from proprietary and 'hard-wired' BSS allows greater flexibility to build new deal types and offer different products to customers.

Easy billing – The Subscriber is billed through an app, eliminating the need for and cost of sending out paper bills.

Easy and instant secure payments – Subscribers pay their bills directly in the app. Payments are made via the blockchain and the Operator receives the balance lightning fast. There shall be an option for secure payments via cryptocurrency.

Targeted and conditional messaging – The contract can be analysed for certain product and usage conditions, and targeted messaging sent to the subscriber app to promote new offerings, offer top-ups, etc.

A scalable solution – Freeing the billing and contracting processing from physical hardware and constraints significantly improves the Operator's ability to scale to explore new expansion opportunities.

The flexibility to respond to changing conditions – the contract mechanism give the operator the ability to change the contract to meet new market challenges and respond to new prospects.

Confidential and secure client contracts – Using consortium blockchain technology i.e. permissioned and private de-centralised ledgers, the mobile operator shall be able to maintain the contract's complete confidentiality with respect to other clients on same decentralised ledgers.

Secure communications – The DApp will securely connect the Smart Contract with the Subscriber and Business App.

The Diadem Solution – Selected Use Cases

Drawing on extensive experience in mobile telecoms operations, the Diadem project has identified several use cases. Further cases will be considered as a result of the project's collaboration with MNO partners.

2.1. Building a contract

Building a contract for a Subscriber will be easy using the Diadem Solution. The solution allows simple tariff and product structures to be built directly into the Smart Contract. Whilst this simplification will challenge the complex interdependent tariff and usage relationships that many Operators have been bound to use by current BSS technology, it will hugely improve the flexibility to provide mobile contracts which offer better value for their customers, and the transparency of the solution will allow the Subscriber to have a far clearer understanding of how their mobile plan works.

When the Diadem Subscriber App is first opened on the Subscriber's device, they are presented with a start-up wizard. The user enters basic information including some straightforward security responses and the app then checks whether the Subscriber already has an existing contract. If no existing contract is found, the app creates a blank smart contract on the Blockchain and populates it with some basic contact information.

The contract contains two key parts; the smart contract which contains the product and tariff structure for the subscriber's deal along with general terms and conditions.

When the Subscriber is ready to discuss a deal with an Operator, they provide the Operator Agent with the Operator key. This can be done by exposing a QR code to the Agent when in a face-to-face situation, e.g. a retail conversation, or by sending a secure message to the agent via the app. Using the Operator Key, the agent now has the ability to inspect their existing contract and offer a better deal for the Subscriber.

The Operator Agent can then build a deal directly with the customer using the Diadem Agent Tool. The Agent drags and drops tariffs, booster packs, devices, and other products and services into a sample contract – a facsimile of a real contract showing exactly what the final agreement will contain. This is then sent to the Subscriber App for the Subscriber to consider. When a deal has been agreed, the customer signs the contract using their private Subscriber key and the deal is transposed from the 'sample' contract into the actual smart contract on the Blockchain.

The Operator's provisioning systems are informed automatically via the Diadem API and the contract can be inspected to obtain the necessary setup information. Alternatively, the Operator can obtain details of all newly contracted customers via a report from the Diadem search tool.

If an agreement is not reached and the subscriber clicks to reject the offer, the Operator Key is invalidated for security reasons. A new one is generated when the Subscriber next re-opens a deal discussion.

In theory, a deal can be discussed, built, signed and provisioned in minutes. The transparency of the contract allows the customer to obtain the best deal possible and ability of the Agent to build contracts rapidly and flexibly means that Operators can begin to offer far more tailored customer offerings.

2.2. Contract signature

When a contract deal has been agreed both the Subscriber and agent provide specific approval using the Subscriber app to form a contract. This approval is recorded in the contract with a time-stamp. Both the Operator and Subscriber must provide their keys to record this approval. The Subscriber key is provided automatically by the Subscriber app (after the Subscriber has entered their pin code as additional validation). The Operator key is provided by the Operator agent in the form of a QR code which is scanned by the Subscriber app. The QR code would also provide additional information to be recorded in the contract, such as agent ID. The contract is enforceable as soon as it is validated in the blockchain. The whole process from approval to validation should take minutes.

2.3. Subscriber Billing

The Subscriber bill is calculated directly within the Subscribe App using the product and usage event data extracted from the Smart Contract. The Subscriber can view their bill directly on their device and make the appropriate payment. No paper bill is issued, but the Subscriber App can send an electronic version of the Bill to the Subscriber's email as an option. The Subscriber App allows the Subscriber to view their allowances, usage, top-ups, etc. for complete bill and consumption transparency. The Operator has the option of including helpful notes against each tariff or product which may explain why it appears on the bill in the way that it does. For example, 'If you don't have our Worldwide Roaming add-on, this call may incur fees.' This messaging will help to reduce billing enquiries to the Operator's call centre.

2.4. Credit, Billing Cycles, and Payments

The Smart Contract contains two values (set when the contract is signed) which determine the mechanism for billing and customer credit. Bill Limit – The bill limit is a numeric value which sets a maximum time after a weekly or monthly bill has been generated by which the customer must pay the balance of the bill. For example, if the bill limit is set at 4 weeks the customer must pay their bill within 4 calendar weeks. The application will provide reminders when 50%, 75%, and 90% of the limit has expired, and a final warning at 95%. If the bill limit expires, the application will set a flag in the contract to report the limit has been breached. The Operator can use this flag to search for all subscribers which have gone beyond their bill limit for collections purposes.

Setting a bill limit flag sets the app to 'bundle' billable events within a set period into a regular traditional bill. If no value is specified for Bill Limit the Credit Multiplier is used.

Credit Limit – Setting the credit limit means that billing occurs on a rolling basis. Instead of a regular bill, the Subscriber is presented with a rolling balance. The credit limit determines the 'unpaid balance' the customer can accumulate before a flag is set in the Smart Contract to say that the limit has been breached. Again, the application will provide multiple warning as the credit limit is approached. Subscribers can pay their balances directly from the Subscriber App using the built-in currency wallet. The funds are sent directly to the Operator via the blockchain. As an option, the Subscriber app can email a receipt for the payment to the Subscriber.

2.5. Billing and Contract Inspection

The Diadem Solution includes a desktop and tablet App for Operator agents to view both the smart contract and billable events. As all contract and event information is contained in the smart contract, the agent will have exactly the same view as the Subscriber which facilitates easier billing query support. The Subscriber can view their bills and recent usage using the Subscriber app.
If a change is made to the pricing or terms by the Operator, the Subscriber app notifies the Subscriber automatically.

2.6. Subscriber Messaging and Identification

The Diadem solution provides a messaging centre app to the Operator through which they can send messages to Subscribers. These messages are displayed in the application. The messaging solution provides assistance in formatting the message so that it can be viewed correctly on a device and contains several pre-set responsive messaging templates. Important messages can be marked as a 'recordable event' which forces the Subscriber to confirm that they have been read and this fact is recorded in the smart contract. The Diadem solution also provides a simple reporting tool which allows the Operator to pull-off list of Subscribers who have specific contract features such as tariffs, contract expiry dates, etc. These lists can be used with the messaging centre to easily send messages to specific Subscriber groups.

2.7. In-Life Contract Variation and Care

Network Operators do their utmost not to change pricing, allowances, or terms whilst the contract is in effect. However, it is not uncommon that a change in the economic or regulatory landscape occurs during the contract lifetime forces the Operator to alter the terms of the contract. This can often be a difficult exercise for the Operator, especially those using legacy or complex BSS systems. The challenges of identifying all impacted Subscribers (e.g. those on a specific tariff), of communicating the reasons for the change and its impact to those Subscriber, and in applying the contract change itself, can be extremely painful and risky.

The Diadem solution makes this process far more straightforward. Firstly, Subscriber smart contracts can be readily inspected to determine which Subscribers have the specific terms or price-points which need to be altered. Then, appropriate messaging can be pushed to the Subscriber app for those Subscribers identified and an acknowledgement recorded that the Subscriber has read and understood that communication. Finally, the changes can be applied directly to the smart-contract by the Operator (using the Operator key to access the contract). If required, a further communication can be sent to the Subscriber confirming the changes have been made, but in all cases the application will automatically alert the Subscriber that a change has been made to the contract. In some circumstances, the Operator may need to the Subscriber to specifically accept or reject the proposed changes. This can be done via the app with a flag registered in the contract to record this event. If the Subscriber rejects the change, and if the legal terms of the contract allow them to do so, they may trigger a contract cancellation process. n-life contract variation may also occur where an Operator/Subscriber Care agent might (providing they have the appropriate internal approval) change the contract terms for the Subscriber to rectify a problem, or for example apply a discount to compensate the Subscriber for some inconvenience. In this case, the Subscriber can approve the contract variation in real-time using the app and feel confident that the issue will be rectified 'on the call'. The Diadem Solution provides a method for mass application of contract variations and an app through which care agents can apply changes for specific Subscribers. All contract changes are logged in the smart-contract and can be viewed by either the Operator or Subscriber.

2.8. Lock/Suspend Billing

If a device is reported lost or stolen, or if the Operator needs to stop the Subscriber from being billed for another reason, the Operator can set a 'lock' flag in the smart contract which stops any subsequent usage events being billed in the Subscriber app (until the flag is reset).

2.9. Allowance Alerts

The application will automatically monitor the Subscriber's usage and notify them when they approach their usage allowance limit. This will prevent users overspending and support the Operators efforts and obligations to ensure Subscribers do not fall into debt.

2.10. Portable Contracts

Because the smart contract is both de-centralised and is 'electronic' it is far more transparent.
The Subscriber can choose to expose the contract terms to other parties who can scrutinise their contract duration, allowances, pricing, and information on the best deal providers.. To do this the Subscriber would unlock their application, visit the relevant contract screen, and opt to show the contract details. The app would then generate a Quick Reader (QR) code which could be scanned by the third-party. The QR would direct to a secure file which would provide contract and pricing information.

This case facilitates better competition in the market and ensures contracts to ensure that the Operator is providing the best value for the Subscriber. This is key industry issue in many countries with regulatory bodies placing increasing pressure on Operators to improve the transparency, simplicity and fairness of contracts.

2.11. Further Use Cases (The Waiting Room)

In addition to the use cases outlined above, the project will consider the following functions:

- Contract cancellation/termination (using conditional checks to determine whether a contract can be ended any subscriber cancellation charge).
- Advertising/promotion through the app based on the Smart Contract conditions, e.g. promoting a top-up as the user approaches their usage allowance cap.
- On demand premium content ordering and unlock.
- Credit checking using information from the smart contract.
- Porting process initiation.
- Out of Allowance Alerting.
- Know Your Customer (KYC) and Data Protection (DPA) information – capture through the app and storage in the smart contract.
- eSIM integration/interoperability.

Furthermore, the project proposes to engage with MNO partners to refine and expand the use cases already identified, and to scope out new applications of the solution.

Technical Application Overview

3.1. Overview of The Diadem Architecture

The Diadem Architecture shall employ Client/Server architecture, the Diadem Smart Contract on blockchain shall act as a Server and there shall be two different applications, the Business application and Subscriber application. Security is an essential part of blockchain technology and to meet the highest standards of security and trust the Client/Server architecture shall use mutual authentication using PKI and certificates.

The Diadem Architecture consists of three core components:

The Diadem Smart Contract – contains the baseline contract information such as contract term, products & tariffs, pricing, subscriber information, service information, and a record of usage (voice, SMS, data, etc.), contract amendment history, payments, key events, etc.

The Diadem Subscriber App – the customers control panel for their mobile service. The app reads information from the Smart Contract to provide a view of usage, spend, payments, allowances, etc. The app takes care of billing for the Operator. The customer can also make payments for products and services via a built-in wallet.

The Diadem Operator Control Centre –

The Operator Control Centre consists of are four core components:

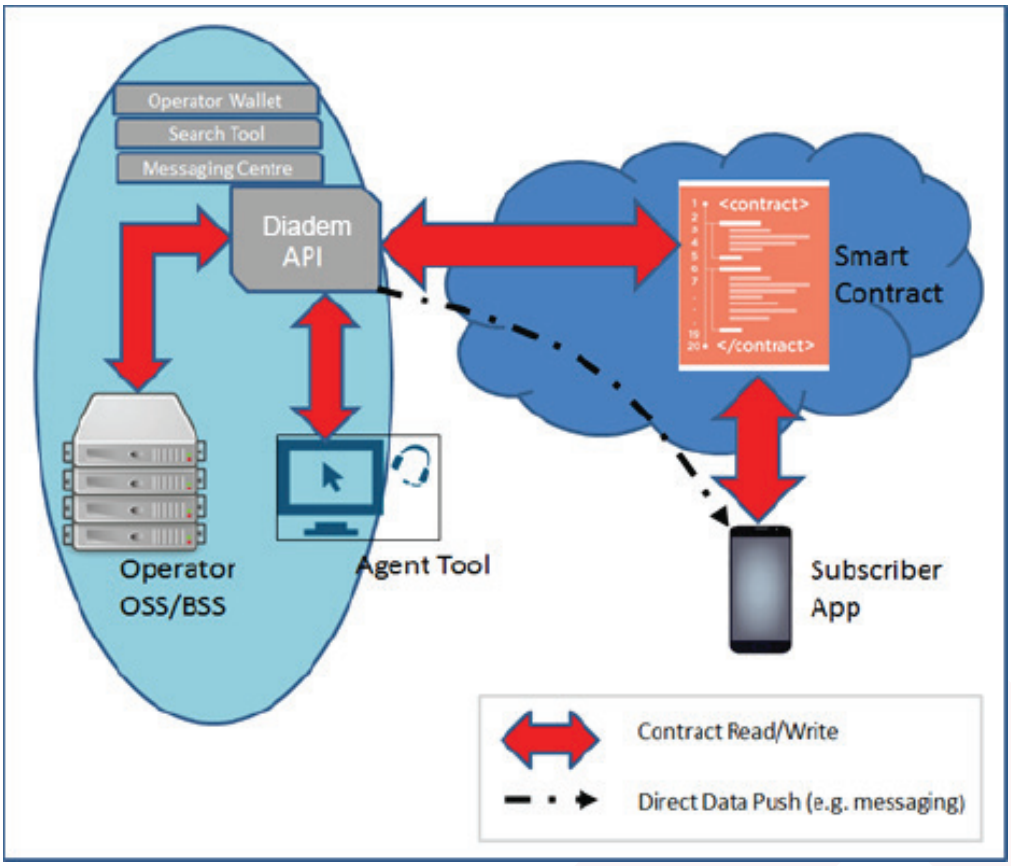
API - the interface with the operator infrastructure through which the Operator can send usage information to the Smart Contract which is recorded in the contract and used by the Subscriber App as part of billing. The API can be used to write other information to the Smart Contract as part of controlled contract amendment events, and read key contract information for the purposes of customer care, payment tracking, etc.

The Messaging Centre – capable of sending messages to subscribers.

The Search Tool – interrogates customer contracts to retrieve lists of customers with selected attributes

The Agent Tool – to provide customer care. The tool gives the Operator Agent a shared view of the Smart Contract and the Agent can make agreed changes to the Smart contract. In addition, the agent tool is used to build the initial contract with customer.

The Operator Wallet – allows the operator to store Diadem Tokens as payment for usage transactions. The operator loads funds in the form of Diadem tokens into the wallet and the API will trigger the wallet to deduct the charge for transacting each billing event from the wallet balance. The charge is transacted via the blockchain to the corporate Diadem wallet.



3.2. The Smart Contract

The intention is that the Smart Contract will be designed around Ricardian principles. One of the key benefits of Ricardian contracts is that they present electronic, cryptographically-secured contracts, in a way that they can still be read in a similar format to traditional paper-based agreements, i.e. whilst having all the features of a blockchain-based smart contract they can be outputted with the same legal structure and terminology as current contracts. One of the challenges for the project might be possible resistance to the solution from Operator legal teams who may be uncomfortable with the completely new form of agreement type presented by a straight blockchain smart contract. By designing the contract in such a way that it still presents in a way that resembles a traditional agreement, the project aims to mitigate this risk. The project will also attempt to design the contract to be able to accommodate in-life structure changes. This will allow Diadem to update the contract fields and schema to be adapted for new functionality,products and services that an operator may want to introduce. Whilst preserving specific terms and conditions (with the subscriber) and core data, expanded contracts can be deployed to the subscriber base with minimal impact.

3.3. Contract Content

The following file provides an outline of the information that might be contained in the Smart Contract.

Contract Access Control

The Diadem contract can be changed with two keys; the Subscriber key, and the Operator key. Both keys have full read access to the contract for complete transparency between parties. Write access differs depending on the key type. The table below shows a sample of different access cases and permissions:

	Build initial contract and deal1	Write usage data	Write personal and DPA data	Expose contract information (to third -party)	Update pricing and contract terms	Write 'Recordable Event'	Make a payment (payment event)
Subscriber	✓	✗	✓	✓	✗	✓	✓
Operator	✓	✓	✗	✗	✓	✓	✓

1 Both keys are needed to build the initial deal and form the contract.
2 The Operator might request the Subscriber to expose contract information to chosen third-parties, but the Subscriber must give specific permission to do so. The mechanism for doing so is TBD.

The Subscriber Application

The functions of the Subscriber Application are outlined in the Use Cases in Section 2 of this document and include contract view and signature, bill and usage viewing, and payment (via the wallet)

The Subscriber Wallet

The Subscriber Wallet allows the Subscriber to make payment for their bills direct to the Operator via the blockchain. In common with the Smart Chain solution, it is likely that the project will integrate an existing wallet and payment solution to provide this functionality. Preferably, the wallet system will allow payment in fiat currency as well as a variety of cryptocurrencies.

App Maintenance and Updating

The application will be designed so that updates to introduce new features and optimisations can be made easily over the air (or via a download) without losing any key information such as keys or wallet balances.

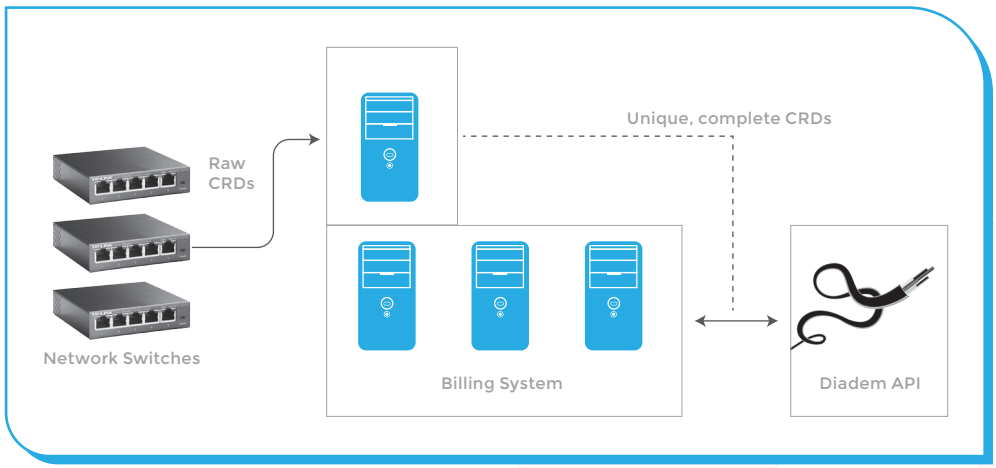
App Skinning

Although the general layout and functionality of the Subscriber Application will be common to all Operators, the app will allow the deployment of custom branding so that each Operator can make the app appear to be unique to them.

3.4. The Diadem Control Centre

API

The Diadem API provides the primary method for interfacing an Operator's core Network and Business Support Systems with the Diadem smart contract on the blockchain. The API will translate usage data provided by the Operators 'back-end' systems and write it into the Smart Contract. Usage data is supplied to the API in the form of unique (de-duplicated) and complete (non-partial) Call Data Records (CDR) from the Operators Business Support Systems. Typically, these CDRs would be served in ASN.1 format but some Operators may use an alternative standard or proprietary format, in which case customisation of the API will be required.



The API also serves as a conduit for writing/reading contract information as part of customer care and contract amendment operation. Although the API allows straightforward integration between the Operator BSS, it will not be a plug'n'play component as each MNO's architecture and data standards is likely to be different and configuration of the API will be needed. The operation, hosting, load balancing, security, monitoring, resilience, backup, and recovery of the API will be the responsibility of the MNO, but it is envisaged that the Diadem team will provide remote support during a major incident as part of ongoing customer service provided by Diadem.

3.5. The Blockchain (Transaction) Platform

There are number of considerations in choosing the blockchain platform which will underpin the solution:

- The platform must be able to support the Diadem smart contact including the requirement to have different access levels (contract access control).
- The platform supplier must demonstrate that they can professionally support an enterprise business; the platform developers should have clearly defined support processes, resources, and infrastructure.
- The platform must be able to support high-numbers of simultaneous transactions.
- The ability to identify rejected (invalidated) write operations should be established.
- The project team need to be assured that the transactions can be processed in a 'reasonable' time and that future increased throughput will not compromise this speed. Although 'real-time' transaction speeds are not crucial to the service, customers will expect updates to be written to the Smart Contract within a few minutes.
- The cost associated with completing a transaction and the impact of low value transaction amounts on payment validation time.

There are a number of existing blockchain platforms which fulfil many of these criteria; however there are no mature networks which have demonstrated that they can scale to the large number of operations – potentially in excess of 100,000 transactions per second – needed when the project has achieved its target 5-year growth.

The project therefore needs to identify a blockchain supplier who has demonstrated that they are developing their platform to address future scaling needs whilst retaining a focus on delivering a network capable of supporting an enterprise-level business.

Having researched and discussed the appropriate blockchain platform for the project, Hyperledger has been selected as the preferred network for development.

Revenue Ecosystem

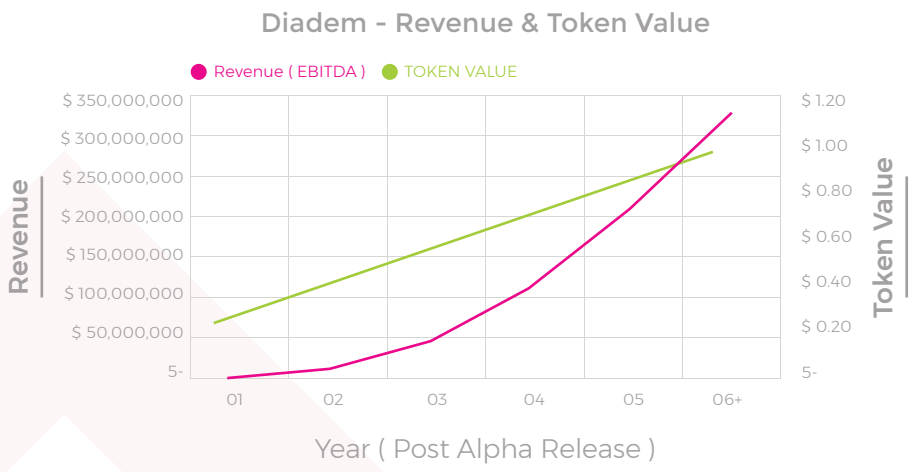
Diadem will generate income by making a fractional 'micro-charge' (which could be for example, the equivalent of $0.005) to the operator for each usage event transacted to the Smart Contract. For simplicity, the micro-charge amount will be fixed for each usage and negotiated with each MNO customer as part of the commercial process (along with the period that the fixed amount will apply for before review). Payment of the micro-charge is made using the Diadem Token (see below). An Operator can purchase Diadem tokens on the open market (via a cryptocurrency exchange) and the token can be loaded into a wallet which is provided as part of the Diadem Control Centre. The micro-charge is deducted from the wallet when a usage event occurs and sent by the API to the Diadem corporate wallet via the blockchain. Diadem tokens received by the project in payment can be sold back on the open market to generate revenue for the project.

The Diadem Token

The Diadem Token is a simple utility token used by the operator to fund usage transactions, and thereby pay for the Diadem solution and service. The Diadem Operator Control Centre associates a unique ID with each billable usage event, the ID is also attached to the wallet payment for the event. In this way usage events and payments can be reconciled for audit purposes. A single Diadem token will fund multiple micro-charges (usage events). For example, a single Diadem Token could fund a block of 10,000 usage events.

Revenue Potential

Even with modest market penetration and token value growth, the business which would emerge from the project is projected to generate significant income. The following graph illustrates the revenue stream which could be seen if the solution was to transact 1% of the annual global mobile usage events and see a growth in token price to $1 per token:



Token Volume and Distribution

1,000,000,000 Diadem tokens will be created. Initially, the Diadem tokens will be allocated as follows:

- 10% (100M) tokens will be offered as part of the initial funding sale event and used to fund the project to the point at which the token mainsale event can be launched.
- 44.8% (448M) tokens will be released to general buyers as part of the token mainsale event.
- 5% (50M) tokens will be available to a private investors who are able to buy tokens outside of the initial funding and mainsale events.
- 10% (100M) tokens will be used by the project as a 'pump prime' fund to incentivise engagement and early adoption from strategic operator partners.
- 15% (150M) tokens will be distributed to partners, founders, and core members of the Diadem team. These tokens will be allocated at the time of the initial funding sale, but will be locked until - 3 months after the mainsale event; at which point team members will receive 25% of their allocation with a further 12.5% released every 3 months thereafter.
- 15% (150M) tokens will be retained as a reserve to ensure continuance of the project in case of adverse market conditions, unexpected events, etc.
- 0.2% (2M) tokens will be used to fund a bounty campaign of growth hacking and social media networking

Diadem Project Roadmap

The following section outlines the high-level milestones for the Diadem project

Q4 2017

- Diadem Project is conceived.
- Founding team assembled.
- Initial project summary drafted.

Q1 2018

- Core use cases documented.
- High-level architecture and data flows validated.

Q2 2018

- Blockchain platforms researched; HyperLedger chosen as preferred platform.
- Token economy and future distribution defined.

Q3 2018

- Whitepaper published.
- Website published.
- Initial Funding Event strategy defined.
- Terms and Conditions of Initial Funding Event drafted.

Q4 2018

- Secure Angel investment to fund legal review of Initial Funding Event.
- Develop Initial Funding Event mechanism/platform.
- Commence Initial Funding Event awareness campaign.

Q1 2019

- Initial fund raising event.
- Recruit full development and management team.
- Detailed solution design.

Q2 2019

- Develop Smart Contract.
- Build Proof of Concept Demonstrator.
- Secure strategic partnerships with MNOs.
- Prepare token mainsale Proposition and mechanism.

Q3 2019

- Commence token mainsale awareness campaign.
- Develop functional integrations with Strategic partners.
- Functional uplift of Proof of Concept Demonstrator.
- Token mainsale.

Q4 2019

- Expand development team.
- Develop Beta build.

2020

- Commercial pilot with strategic partners.
- Alpha release and full commercial release.

The Diadem Team

MATTHEW ARMISHAW
CEO - Founder

Matthew has worked in the mobile telecommunication sector for 10 years as a Senior Project Manager, delivering solutions ranging from IT network and data-centre builds to complete multichannel service propositions. In many cases, he has lead these projects from initial conception right through to transition to operational service and this experience has provided a deep understanding of the challenges and opportunities within the mobile telecoms industry. Matthew is a qualified Project Management Professional (APMP PMQ) and a Certified Blockchain Expert.

DIVYANG PATEL
CTO - Co-Founder

Divyang has 17+ years of diverse experience in Software and Systems for Mobile telecom, IoT, etc. with the latest interest in Blockchain and Cryptocurrencies. In past Divyang has worked at different levels in organisation with responsibility for steering business towards new technologies, leveraging robust technology-centric business strategies and technical innovation. Divyang has held variety of senior leadership roles in technology and has served global markets U.S., Europe, Asia Pacific. With the passion for Software and Hardware, he has worked with large corporations, as well as SMEs and start-ups.

AMAURY AUBRÉE
CCO - Co-Founder

Amaury is an experienced senior executive (CxO) with 24+ years in innovation and digital transformation, globally. He has founded and advised multiple start-ups and digital agencies and supervised programs handling millions in assets for major organisations covering planning, development and implementation to award-winning levels of results recognised by the Project Management Institute. His objectives are to help people and organisations to outperform while being part of undertakings leveraging technologies that will fundamentally reshape the world.

GET IN TOUCH

hello@diadem.one

FOLLOW

DIADEM

APENDIX

Hyperledger as a Blockchain Platform for Business

Hyperledger is an open source collaborative effort - hosted by The Linux Foundation - created to advance cross-industry blockchain technologies. Hyperledger is backed by some key industry names such as IBM, Oracle, Intel, J.P.Morgan, Fujitsu, and others.

Hyperledger is focussed on developing a modular architectural framework for enterprise-class distributed ledgers. This includes identifying common and critical components, providing a functional decomposition of an enterprise blockchain stack into component layers and modules, standardizing interfaces between the components, and ensuring interoperability between ledgers.

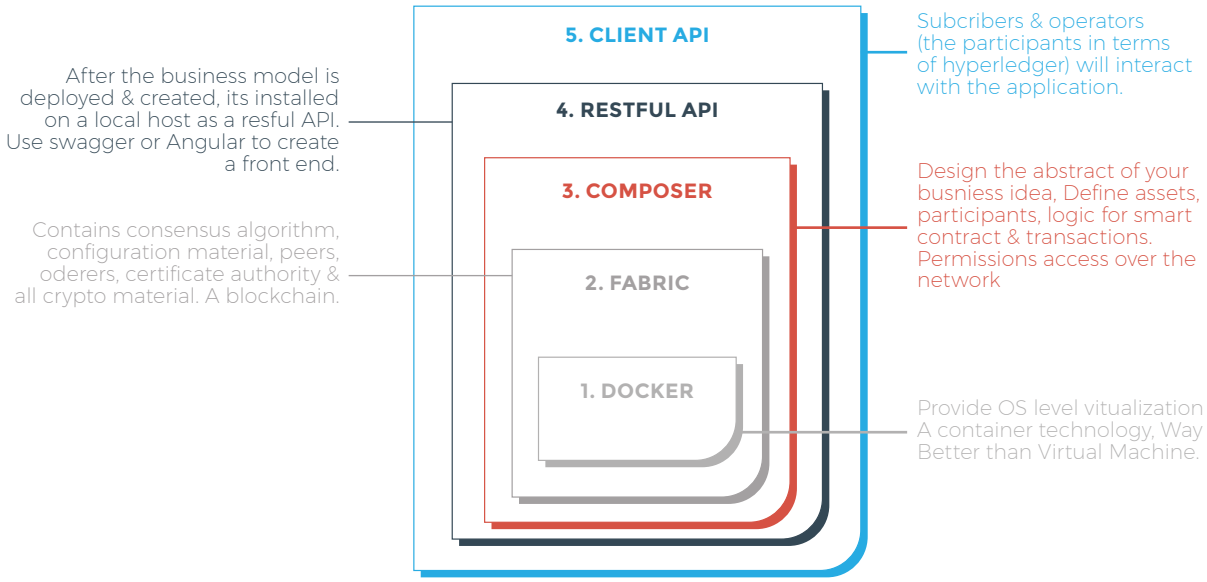
The Hyperledger Architecture

Requirements vary. Scalability, confidentiality, compliance, workflow complexity, and even security requirements differ drastically across industries and uses. Each of these requirements, and many others, represent a potentially unique optimization point for the technology.

The Hyperledger Architecture has distinguished the following business blockchain components:

- **Consensus Layer** - Responsible for generating an agreement on the order and confirming the correctness of the set of transactions that constitute a block.
- **Smart Contract Layer** - Responsible for processing transaction requests and determining if transactions are valid by executing business logic.
- **Communication Layer** - Responsible for peer-to-peer message transport between the nodes that participate in a shared ledger instance.
- **Data Store Abstraction** - Allows different data-stores to be used by other modules.
- **Crypto Abstraction** - Allows different crypto algorithms or modules to be swapped out without affecting other modules.
- **Identity Services** - Enables the establishment of a root of trust during setup of a blockchain instance, the enrollment and registration of identities or system entities during network operation, and the management of changes like drops, adds, and revocations. Also, provides authentication and authorization

To provide these component layers, Hyperledger has developed as suite of tools and services as part of a unified architecture:



Hyperledger Fabric

Hyperledger Fabric is an open source enterprise-grade permissioned distributed ledger technology (DLT) platform, designed for use in enterprise contexts, which delivers some key differentiating capabilities over other popular distributed ledger or blockchain platforms

Fabric is comprised of the following modular components:

- A pluggable ordering service establishes consensus on the order of transactions and then broadcasts blocks to peers.
- A pluggable membership service provider is responsible for associating entities in the network with cryptographic identities.
- An optional peer-to-peer gossip service disseminates the blocks output by ordering service to other peers.
- Smart contracts ("chaincode") run within a container environment (e.g. Docker) for isolation. They can be written in standard programming languages but do not have direct access to the ledger state.
- The ledger can be configured to support a variety of DBMSs.
- A pluggable endorsement and validation policy enforcement that can be independently configured per application.

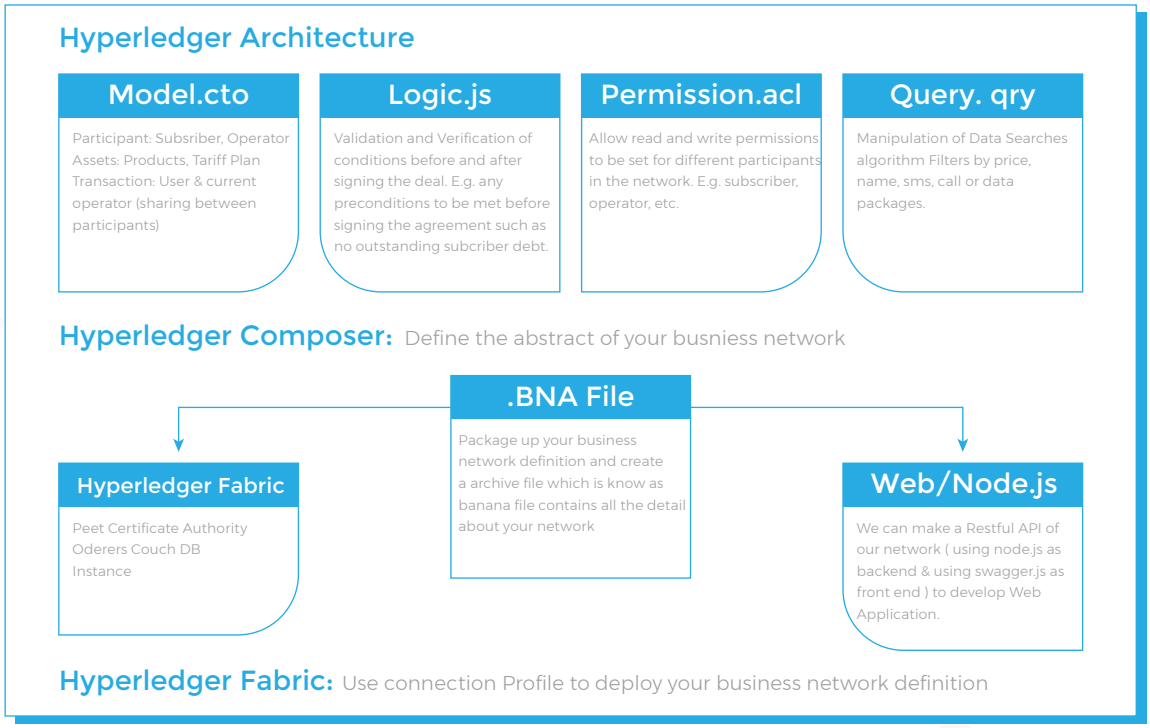
Hyperledger Composer:

Hyperledger composer is used to define the business network including the smart contract (the 'chain code') and the overall business logic. The network can be thoroughly tested in a composer playground before deploying to a main chain.
The main components of our Hyperledger Composer are:

- **Participants:** The users who will interact with the system such as the Subscriber, Admin and the Operator.
- **Assets:** Products and services such as devices and tariffs. Any commodity which can be provided to the subscriber is an asset.
- **Transaction:** The logic of chaincode responsible for validation and verification of every action happening on the Diadem blockchain network by the Operator and the Subscriber.

  These three components are combined into a single 'model' file which contains the basic working structure for the solution. In addition, there are two additional supporting components
- **Query:** To apply search filters which can be used to search for specific information in the records and assets contained within the network.
- **Permissions:** Provides access control for participants over the network.

Ultimately, the component files are combined in a 'banana' (.BNA) file which packages all the logic and definitions for the business network. The following diagram illustrates the Hyperledger components in the context of the 'Build Contract' use case.



It can be seen that the Hyperledger component structure is both designed for business networks, and maps closely to the architecture of the Diadem project; for example, the Permissions component will provide the Contract Access Control functionality for the solution, and the Query component can be harnessed to deliver reporting and customer search capabilities with the operator control centre.

Blockchain Segregation in Hyperledger

Hyperledger offers the ability to build a private blockchain network within the public blockchain. This is achieved the harnessing of channels; private subnets of communication between two or more specific network members. Within a channel, transactions are confidential to the peers in that channel and the channel has its own private ledger which is stored in each peer. Channels are made possible by the HyperLedger Ordering service which groups the transactions related to a specific channel into channel-specific block. The ordering service sends the block related to the relevant peers members of that channel. The peers then perform the consensus operation and the add that transactions in the channel ledger.

Use of the channel facility within HyperLedger by the project provides the a twofold benefit in that it gives operators confidence that sensitive customer data is being transacted across a secure and segregated network whilst allowing the resilience and performance of a public blockchain infra-structure.

Example Workflow of Use Case in Hyperledger (Building a Contract)

In the use case of building a contract, we can define three participants in our network.

- The Subscriber – the customer who is purchasing a product
- The Operator – the network operator who is selling the products; the operator participant is a system participant rather than an individual
- The Agent – the operator sales agent who works with the subscriber to agree a deal package

The following steps would be taken when building a new contract:

Download the Subscriber Application

The Subscriber downloads the Diadem application and registers (in this application).

Subscriber Registration

After providing some basic information and setting an application PIN/passcode, the Subscriber is asked to enter their MSISDN into the app. The app has specific network search privileges (determined by the Hyperledger Permissions component) and interrogates the blockchain to see if the MSISDN is associated with an existing contract with the operator. If an existing contract is found and the subscriber is able to pass additional identification verification steps, the details are retrieved and duplicated to form a new draft contract. Alternatively, a new blank contract is created if no existing subscriber agreement with that operator is found. The draft contract is created on the blockchain.

This request to create a draft contract passes through all the endorse nodes of the Hyperledger Fabric network. The endorsers validate the contract and ensure that a number of business conditions have been met; for example that the subscriber has no outstanding debt.

If a draft contract can be formed the subscriber can extend a temporary agent key to the agent. This allows the agent to inspect the contract and work with the subscriber to add/remove products to create an appropriate deal. A set of business logic rules in the Hyperledger Composer components determine what combinations of devices, tariffs, add-ons, etc. can be combined in a deal.

Note that an agent might be a web agent (service), as telesales agent, or a retail agent.

Agreeing The Deal

When a deal ready and both Subscriber and Agent have clicked to approve it, the draft contract is submitted to the blockchain as a final agreement. All the peers node will see it and the consensus algorithm process will take place. Once validated means the contracted is added in the ledger and it will world state of the blockchain is updated. The contract is now active.

If both parties can not arrive at a deal the draft contract can remain active for a pre-set period (determined by the Operator and set as part of business rules) allowing the subscriber to return and re-attempt the deal making process.

Blockchain Architecture