AIR | TECHNICAL WHITEPAPER
PRODUCT BY SPHRE

TABLE OF CONTENTS

DOCUMENT DISCLAIMER

This Document has been prepared solely for informational purposes for Sphre Limited ("Sphre", "SPHRE" or the "Company") and is being furnished by Sphre to a limited number of parties (the "Recipients") who have a potential interest in contributing to the technical development of the Air Platform (and associated products thereof). All Document content (wording, phrasing, structure, other) is supplied in 'good faith', and any similarity to any existing Document or Documents is therefore to be considered coincidental.

ABSTRACT

In an interconnected, open digital world it does not make sense that digital identity is still fragmented in outdated, closed systems. The reason that identity management has not progressed is due to the at best haphazard nature of the various solutions thus far implemented by numerous organizations and enterprises. This has resulted in a poor and confusing user experience via the necessity to maintain multiple service registrations, logins, usernames and passwords, to largely differing service provider security policies.

This whitepaper describes how decentralized technologies such as blockchain offer a potential solution for the digital identity challenge. Blockchain technology reverts the ownership of a given digital identity from centralised systems so that the individual is in control. This approach further decentralises data and computing capacity, and thereby greatly increases user and/or organizational security and privacy.

"The nature of identity is changing profoundly, and the nature of money is also changing equally profoundly because of technologically change, and that these two trends are converging, so that all we need to transact is our digital identity, there will be no trade off." David Birch, 2016.

THE CENTRALIZED VERSUS THE DECENTALIZED MODEL

THE CENTRALIZED MODEL

Centralized models rely heavily on singe party (government, company, individual, server, etc.) to manage and make core decisions. The large majority of models today are centralized (some may include decentralized components but do not fit the criteria of a truly decentralized model). Examples of centralized models include businesses where the stakeholders make all core decisions, government organizations, and Information Technology (IT) systems that hold all user information and company data. Even peer to peer companies such as Uber and Airbnb do not fit under the decentralized classification because all users are routed through the service provider for all activity.

Identified flaws of the centralized model include:

- Bureaucracy in decision-making which slows down innovation. If most the employees or customers want to see a change, it is ultimately up to the owners (or managers) to make the final decision.
- Single point of failure risk. If something happens to the service provider it affects employees, customers, and other affiliated parties which creates unnecessary risk for participants.
- The model is not designed for innovation. Due to the bureaucratic structure where employees lack the ability to partake in the decision-making process it creates obstacles for implementing innovative updates.

THE DECENTRALIZED MODEL

Truly decentralized models rely on the entire network of participants to make decisions and run the business. Only very few organizations follow truly decentralized models to date. Prior to the recent emergence of further innovations within blockchain technology (e.g. the smart contract) decentralization was not considered feasible. Over the upcoming years, you will most likely see a massive shift into decentralized models. According to Johnston's Law, "Everything that can be decentralized, will be decentralized." Current examples of decentralized models include Bitcoin, Inter-Planetary File System (IPFS), Storj and others. The foundational structure of these technologies will be explained in the later sections of this Document.

The biggest advantages of the decentralized business model are as follows:

- No single point of failure risk. Since there is no service provider (or centralized party) which the network relies on to function properly, if one (or several) network participants are corrupted or leave the network it will not affect functionality nor the other participants.
- Incorporates truly democratic principles by providing every participant an equal say in the vision, development, and objective of the organization.
- Fuels innovation via the enablement of experts from a variety of verticals to equally participate in operations and suggest changes.

A disadvantage of the decentralized model is that organizational issues have the potential to arise during the decision-making process if there is a lack of agreement among members. This issue is addressed and made much more manageable with blockchain consensus technology.

THE ROLE OF GOVERNMENT

The European Commission put forward its EU Data Protection Reform in January 2012 to make Europe fit for the digital age. More than 90% of Europeans say they want the same data protection rights across the EU – and regardless of where their data is processed.

The Regulation is an essential step to strengthen citizens' fundamental rights in the digital age and facilitate business by simplifying rules for companies in the Digital Single Market. A single law will also do away with the current fragmentation and costly administrative burdens, leading to savings for businesses of around €2.3 billion a year. The Directive for the police and criminal justice sector protects citizens' fundamental right to data protection whenever personal data is used by criminal law enforcement authorities. It will ensure that the personal data of victims, witnesses, and suspects of crime are duly protected and will facilitate cross-border cooperation in the fight against crime and terrorism.

On 15 December 2015, the European Parliament, the Council and the Commission reached agreement on the new data protection rules, establishing a modern and harmonized data protection framework across the EU. The European Parliament's Civil Liberties committee and the Permanent Representatives Committee (CORPER) of the Council then approved the agreements with very large majorities. The agreements were also welcomed by the European Council of 17-18 December as a major step forward in the implementation of the Digital Single Market Strategy.

It is expected that upon implementation that the GDPR will yield the following core potential benefits:

- The new right to data privacy and portability will allow individuals to move their personal data from one service provider to another. Startup and smaller companies will be able to access data markets dominated by digital giants and attract more consumers with privacy-friendly solutions.
- 'Data protection by design and by default' will become an essential principle. It will incentivize businesses to innovate and develop new ideas, methods, and technologies for security and protection of personal data. Used in conjunction with data protection impact assessments, businesses will have effective tools to create technological and organisational solutions.
- The Regulation promotes techniques such as anonymization (removing personally identifiable information where it is not needed), pseudonymisation (replacing personally identifiable material with artificial identifiers), and encryption (encoding messages so only those authorised can read it) to protect personal data.

You can find more details in regards to GPDR, its implementation and implications here and here.

SUMMARY

If the service provider (Airbnb platform for example) is removed, all the users are affected and unable to continue utilizing the service. This creates a single point of failure risk. In the decentralized model, there is not a reliance on a single service provider in which all users must be routed through for the system to function thus eliminating a single point of failure risk. The actions, roles, and responsibilities of the service provider are written in computer code therefore ensuring execution according to community dictated decisions (commonly referred to as consensus).

Consensus is a vital characteristic of decentralized application architectures which requires that most users must agree on any core change to the business model before it can be implemented. Whereas, in a centralized model, if a company decided to update an aspect of their business operations such as raising fees, changing terms and conditions, or altering their model in any way, it could be completed without the approval of users.

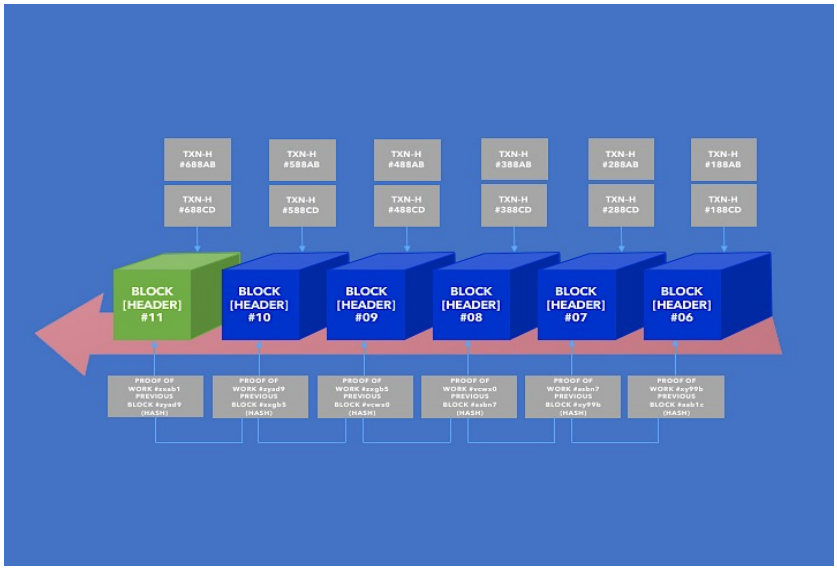
It should be noted that differing blockchain based implementations leverage differing consensus methods to achieve the automated trust model previously described, these include Proof of Work (as stated in the example above), as leveraged by Bitcoin, and Practical Byzantine Fault Tolerance (PBFT), as leveraged by such blockchain implementations as Tendermint and Linux Foundation's Hyperledger.

The role of government organizations, and the realization that individuals have lost control of their personal data is now leading naturally to the implementation of decentralized models that rely on technologies such as blockchain. This loss of personal data control is also noted by Tim Berners-Lee (Inventor of the World Wide Web) as follows: "As our (personal) data is held in proprietary silos, out of sight to us, we lose out on the benefits we could realise if we had direct control over this data and chose when and with whom to share it. What's more, we often do not have any way of feeding back to companies what data we'd rather not share – especially with third parties – the T&Cs are all or nothing."

BLOCKCHAIN OVERVIEW

A blockchain is a is a data structure and state machine that makes it possible to create a tamperproof digital ledger of assets and transactions which are shared among a distributed network of users. Blockchains utilize advanced cryptography to allow each participant on the network to interact with the ledger in a secure way without the need for a central authority.

Once a block of data is recorded on the blockchain ledger it is often referred to as immutable in that it is extremely difficult to change or remove because all past transactions are continuously revalidated before an addition can be added. When a user wants to add to a blockchain, participants in the network (all of which have copies of the current blockchain) run algorithms to evaluate and verify the proposed transaction (all of this happens in the background in a matter of seconds). If most nodes agree that the transaction looks valid, (identified information matches the Blockchains history) then the new transaction is approved and written to the blockchain. Please see below for a diagram illustrating new block addition based on Proof of Work consensus.



Transactions are grouped into 'blocks' and stored forever in a 'chain' by linking each block chronologically with the hash* of the proceeding block.

*A cryptographic hash function is a mathematical algorithm that maps data of arbitrary size to a bit string of a fixed size. Designed to be a one-way function, they are infeasible to invert.

THE BLOCKCHAIN APPLICATION LAYER

Commonly referred to as Bitcoin 2.0 technology, the blockchain application layer is a set of bitcoin derived technologies designed to further the functionality, scalability, and performance of the Bitcoin blockchain.

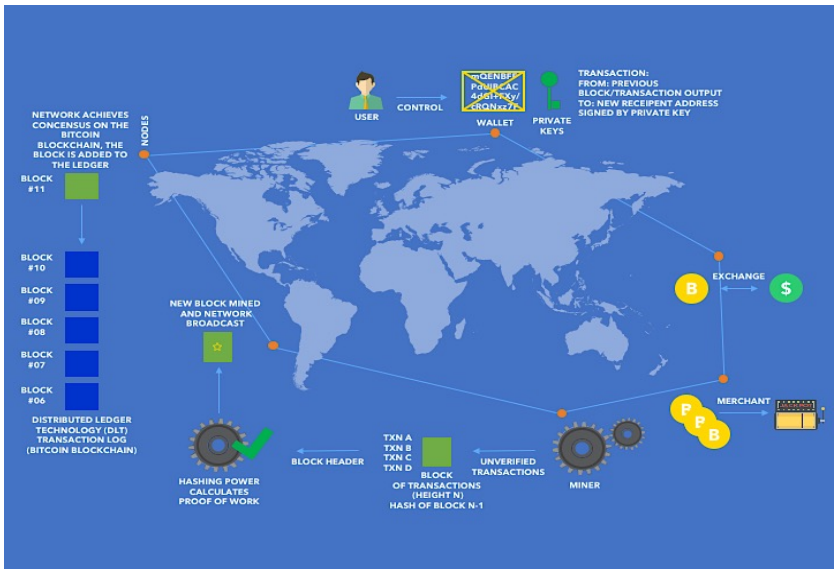
With blockchain application layer technology, we have seen the emergence of smart contracts. Smart contracts are computer protocols that facilitate, verify, or enforce the negotiation or performance of a contract, or that make a contractual clause unnecessary. Smart contracts usually have a user interface and often emulate the logic of contractual clauses which can be partially or fully self-executing, self-enforcing, or both. Smart contracts aim to provide security superior to traditional contract law and to reduce other transaction costs associated with contracting.

Other innovations that have accompanied blockchain application layer technology are increased performance such as faster block processing times, ability to process more transactions in a single block, and more efficient algorithms to secure the network that are not as resource heavy as Bitcoin's Proof of Work algorithm. Other application layer technologies facilitate interacting with the blockchain such as easily deploying on various environments, Software Development Kits (SDK) to interact with common application programming languages, and advanced consensus technologies to manage organization of network participants. New applications are constantly emerging that cater to a specific need or area.

BITCOIN OVERVIEW

Bitcoin is often referred to as the first major decentralized (blockchain) application. Since it was launched in 2009, it has had 100% uptime with zero network breaches which is remarkable. A common misconception regarding major Bitcoin hacks is the Bitcoin network itself that was exploited; that was not the case. The hacks that have gained much attention were Bitcoin exchanges starting with Mt. Gox and including Bitstamp, Bitfinex, as well as other small platforms. These hacks, which lead to millions of dollars' worth of Bitcoin being stolen, had nothing to do with the security of the Bitcoin network, but rather how the exchanges managed user account access and private keys.

An example overview of the current Bitcoin ecosystem is as follows:



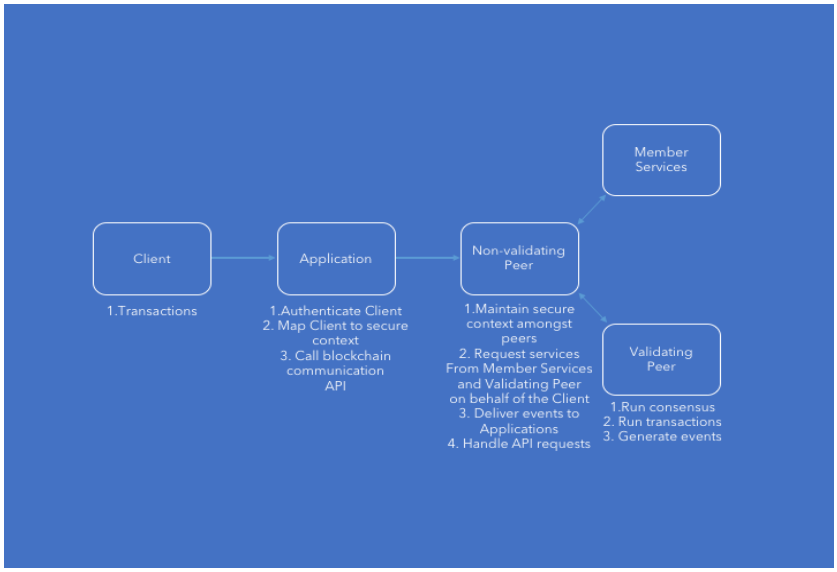
THE HYPERLEDGER BLOCKCHAIN

OVERVIEW

Hyperledger (or the Hyperledger project) is an open source blockchain platform, started in December 2015 by the Linux Foundation, to support blockchain-based distributed ledgers. It is focused on ledgers designed to support global business transactions, including major technological, financial, and supply chain companies, with the goal of improving many aspects of performance and reliability. The project aims to bring together several independent efforts to develop open protocols and standards, by providing a modular framework that supports different components for different use cases.

ARCHITECTURE

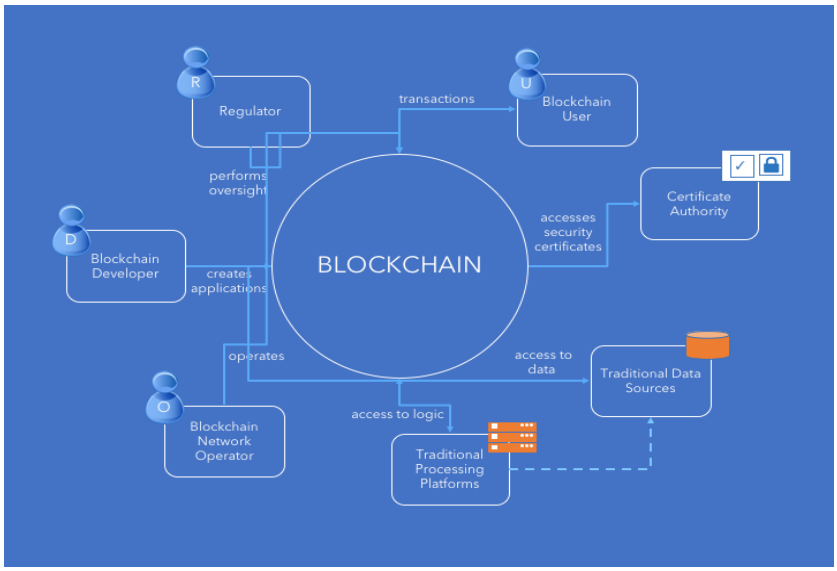
The Hyperledger architecture provides core blockchain services, on which the Air Platform is built. Further information regarding the architecture of the Hyperledger fabric can be found here. However, at a high level, the Hyperledger architecture consists of the following core activities/workflow:



It should be noted that the only role of the Member Services module is to issue digital certificates to validated entities that want to participate in the network. It does not execute transactions nor is it aware of how or when these certificates are used in any blockchain network.

ACTIVITIES AND PARTICIPANTS

There are many activities and participants within the Hyperledger blockchain network at any one point of its operation, as stated within the following overview:



PRACTICAL BYZANTINE FAULT TOLERENCE (PBFT)

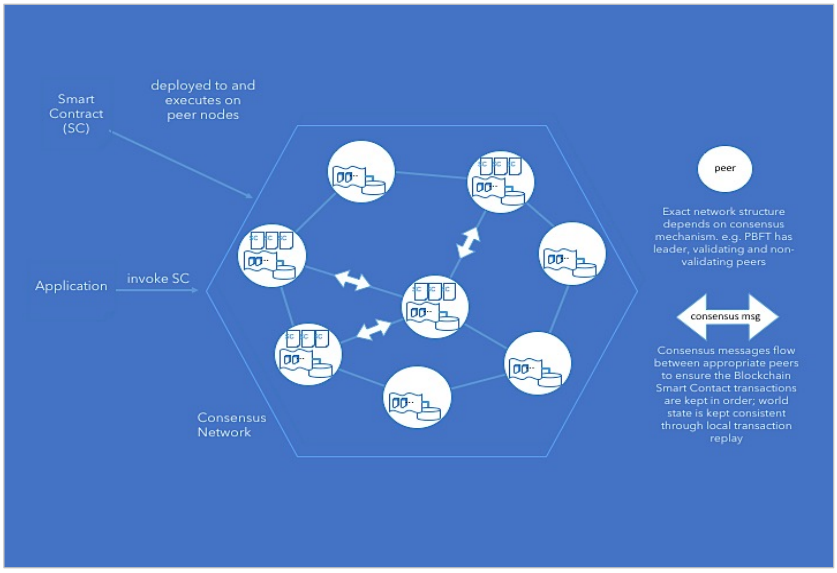
One of the key considerations of the Air Platform system, is its use of Hyperledger's Practical Byzantine Fault Tolerance (PBFT) consensus model. This has been selected due to the node and transaction scaling advantage (to ~5,000 tps) over and above 'traditional' Proof of Work consensus models, as found implemented within the Bitcoin and current Ethereum blockchain implementations.

The PBFT consensus model enables each contributing node within the blockchain network to publish a Public key. Any message parsing through this node is signed by the node to verify its format. Once there are enough responses that are identical is reached, then agreement is made that this is a valid transaction and consensus agreement is achieved. Just as bitcoin uses Proof of Work to confirm transactions without the need for a trusted third party, PBFT relies on the sheer number of nodes (at a minimum of four nodes) to confirm trust. As a result, Proof of Work 'block mining' is not required in this process.

Further information regarding PBFT consensus, can be found here.

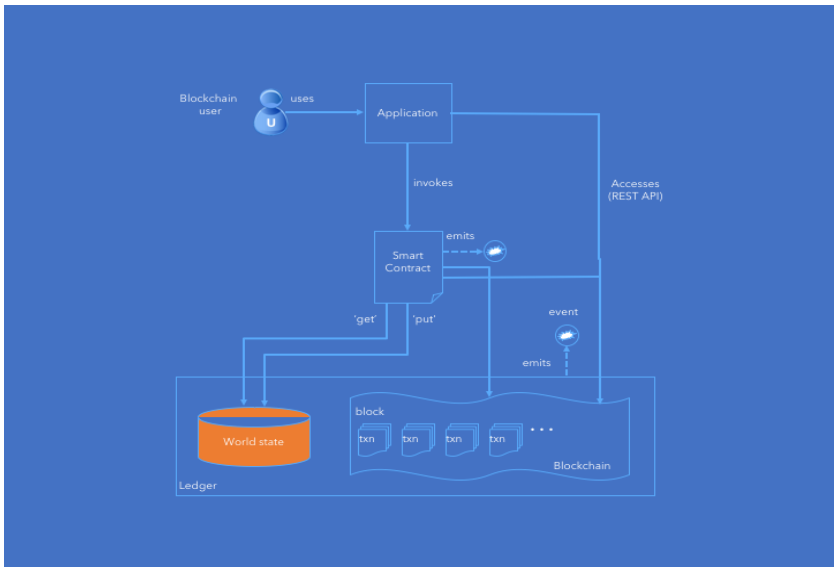
HOW PBFT CONCENSUS IS ACHIEVED

The following diagram describes the Hyperledger network, and its PBFT implementation (as denoted by the hexagon). It should be noted that each operation only needs to be sent into the network once where it is then distributed across the network. The items being inputted into the network are via the implementation of Smart Contracts and other associated applications:



EXAMPLE CLIENT TRANSACTION WORKFLOW

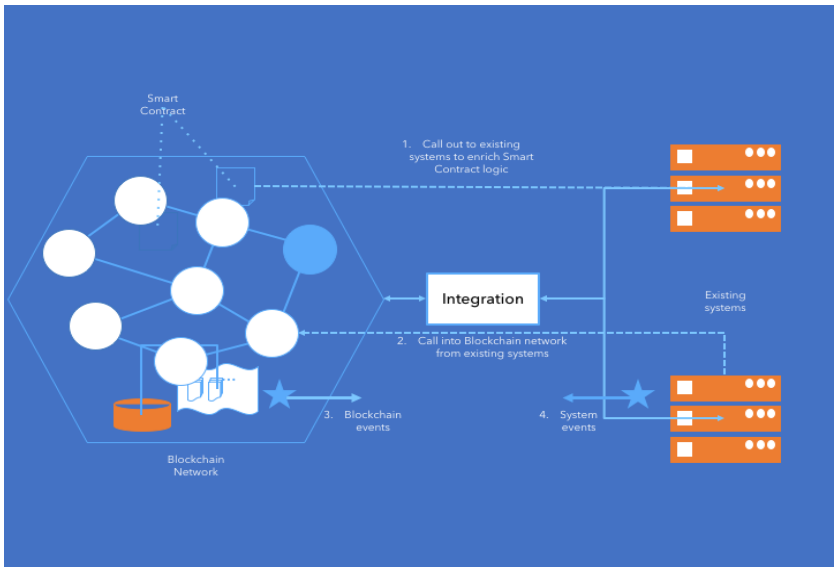
From an example client transaction perspective, the following diagram illustrates all components required to complete a Hyperledger blockchain based transaction. As stated during a transaction taking place via frontend application and smart contract innovation.



Note: World state: Key-value database used by smart contacts to store their state when executed by a transaction.

EXAMPLE EXTERNAL SYSTEM INTEGRATION

The Hyperledger blockchain allows integration with external non-blockchain systems as per the following example configuration:



THE AIR PLATFORM

OVERVIEW

The Air Platform is a highly secure platform for digital identity, built upon the Hyperledger blockchain.

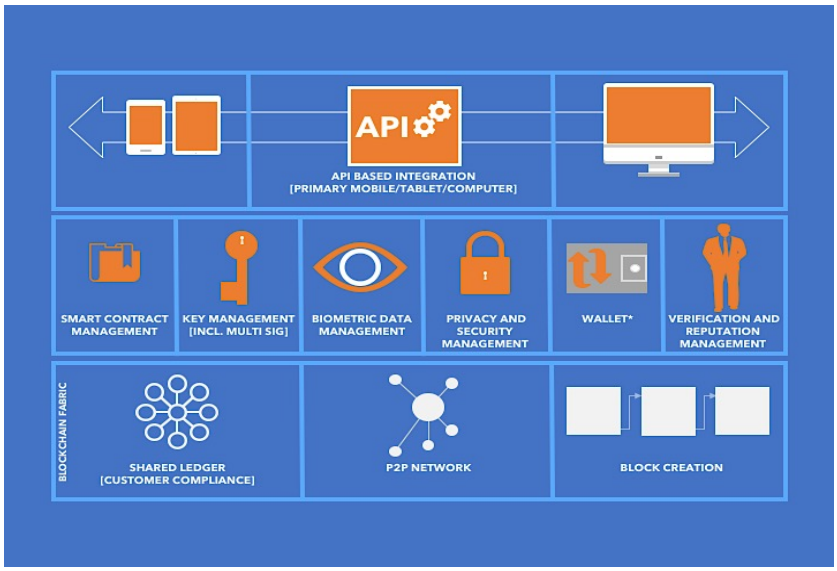
The baseline technology of the Air Platform is composed of two major components: Chaincode (to be known as a 'smart contract' throughout this Document) and Application Programming Interface (API). The API will allow third-party organisations and enterprises to integrate support for the Air Platform into their existing and new systems.

It is expected that Air-based digital identities will take a variety of forms, such as individual, enterprises, organisations or devices. These identities will be fully owned and controlled by the creator, and will not rely on any centralised third party for validation.

At its core, an Air-based digital identity facilitates the ability to digitally sign and verify an action or transaction, thereby enabling a variety of potential use cases.

ARCHITECTURE

The Air Platform architecture features several components that take advantage of the potential of blockchain technology in general, and the additional enhanced services provided by the Hyperledger fabric, an overview of this architecture is as follows:



*Please note: It is understood that the current (1.0) Hyperledger fabric does not natively support Cryptocurrency based implementations. However, it is expected that the Air Platform will facilitate a micropayment service to support potential consumer based applications (including our own). Technical design discussions regarding this requirement are at time of writing, currently ongoing with our partner, the Omni Foundation.

WHAT IS AIR?

Interacting with blockchain based platforms such as the Air Platform necessitates the use of Public key cryptography. Blockchain technology itself can assist to make Public key cryptography more useable and secure by acting as a fully decentralized Public Key Infrastructure (PKI). Thus, the blockchain platform can be thought of as a decentralized Certificate Authority (CA) that can maintain the correlation of a given digital identity to an individual's Public key. The further implementation of blockchain based smart contracts can further add program logic that assists with key revocation and recovery, thereby decreasing technical requirements for the individual.

The core functionality of the Air Platform consists of two initial activities:

- The ability of a given user (or organisation) to authenticate/authorise themselves against their registration.
- The ability of 3rd parties to attest/verify a given individual (or organisation) with whom they have successfully transacted.

COMPONENT LAYERS

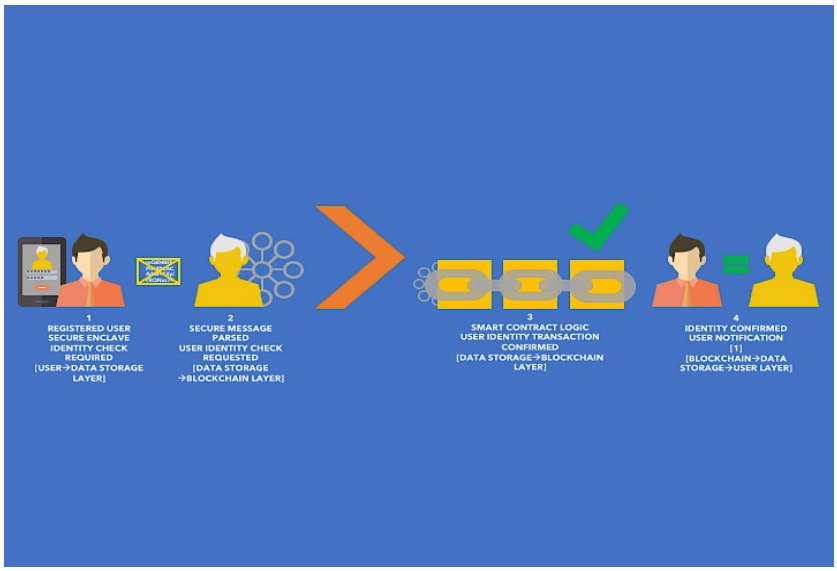
The Air Platform is built leveraging the following component definitions and layers:

- User:
  - User management layer, and front end based functionality towards the Air Platform.
  - The User management layer feature all necessary functions to register and message parse between the user's device (personal computer, tablet (via web browser integration), cell/mobile) and the Air Platform.
- Data (Storage):
  - Data storage/management layer, for initial user registration and data integration and management (including user Biometrics and Attestation) functionality towards the Air Platform.
  - It should be noted that this layer will feature both on-chain and off-chain components to support the Air Platform.
- Blockchain:
  - Blockchain layer, for immutable database functionality towards the Air Platform.

The following diagram details each component function within each layer of the Air Platform:

AUTHENTICATION/AUTHORISATION OPERATIONS

In its simplest form, the Air Platform performs the following core identity based transaction for authentication/authorization on behalf of registered users:



In summary, a secured message is parsed from the Air enabled user application (User Layer) towards the Data (Storage) and Blockchain Layers, whereby the user specific smart contract will be invoked, a `get()` operation will be performed and an identity check completed. Additionally, this operation can be considered as follows:

Functionality (F), Operation (O) performs a Confirm (C) to blockchain (C') and generates a Response R:

$$(C', R) \leftarrow F(I, O)$$

An Operation validation condition needs to be valid in current state, according to a predicate P():

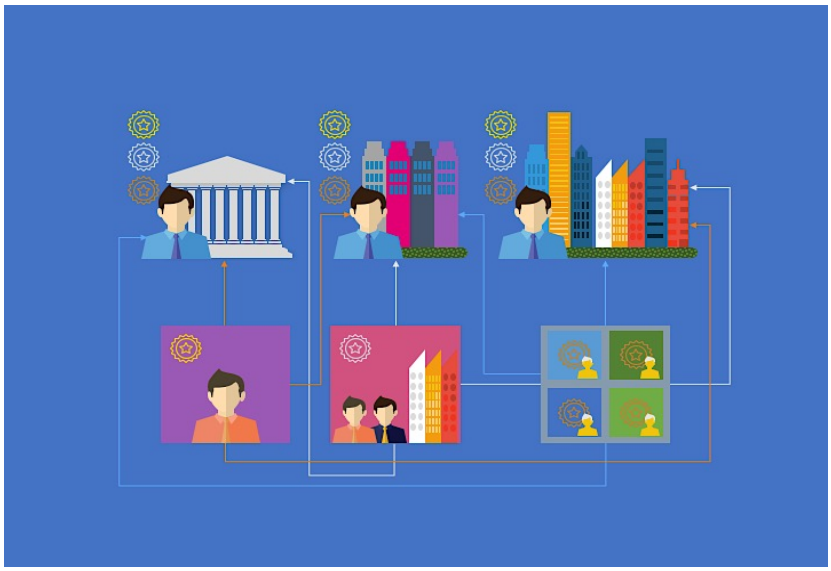
$$P(C,O) = TRUE$$

The blockchain append only log is updated per transaction (not shown within the above diagram), and every operation (O) appends a "block" of valid transactions (tx) to the log. The log content is verifiable from the most recent element.

$$ht \leftarrow Hash([tx1, tx2, \ldots] \,||\, ht\text{-}1 \,||\, t)$$

ATTESTATION OPERATIONS

A further key component of the Air Platform is the ability for a 3rd party/parties to 'attest' to my identity, as per the following overview:



In summary, post completion of a successful identity based transaction with an organization or company, an attestation can be made. This attestation is digitally signed by the organization's decentralized identifier and a timestamp proof that is confirmed towards the blockchain. This attestation can then further assist to verify the relevant identity and perform data validation without the requirement for signee trust. Attestations are expected to be kept securely at the Data (Storage) Layer of the Air Platform, and fully controlled by its users. Additionally, this operation can be considered as follows:

Functionality (F), Operation (O) performs an Attestation (A) to blockchain (A') and generates a Response R:

$$(A', R) \leftarrow F(A, O)$$

An Operation validation condition needs to be valid in current state, according to a predicate P():

$$P(A,O) = TRUE$$

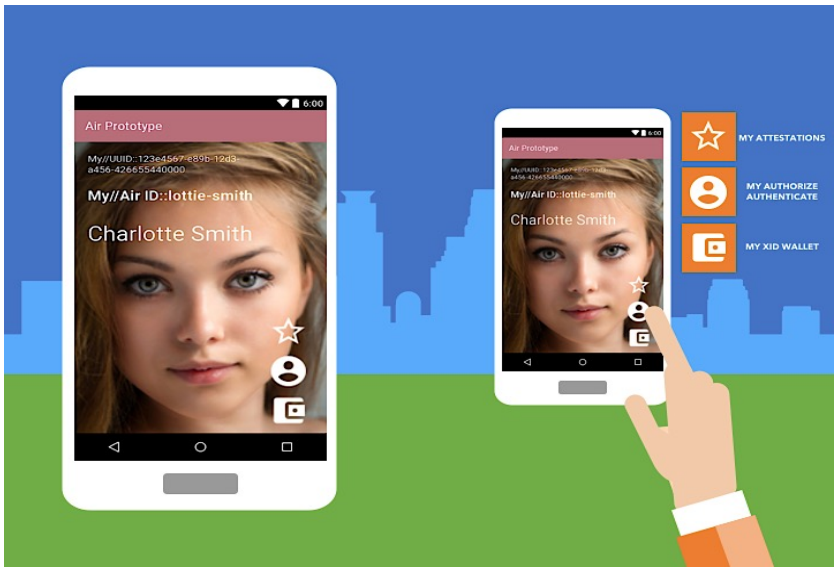
The blockchain append only log is updated per transaction (not shown within the above diagram), and every operation (O) appends a "block" of valid transactions (tx) to the log. The log content is verifiable from the most recent element.

$$ht \leftarrow Hash([tx1, tx2, ...] \,||\, ht\text{-}1 \,||\, t)$$

THE AIR CONSUMER APPLICATION

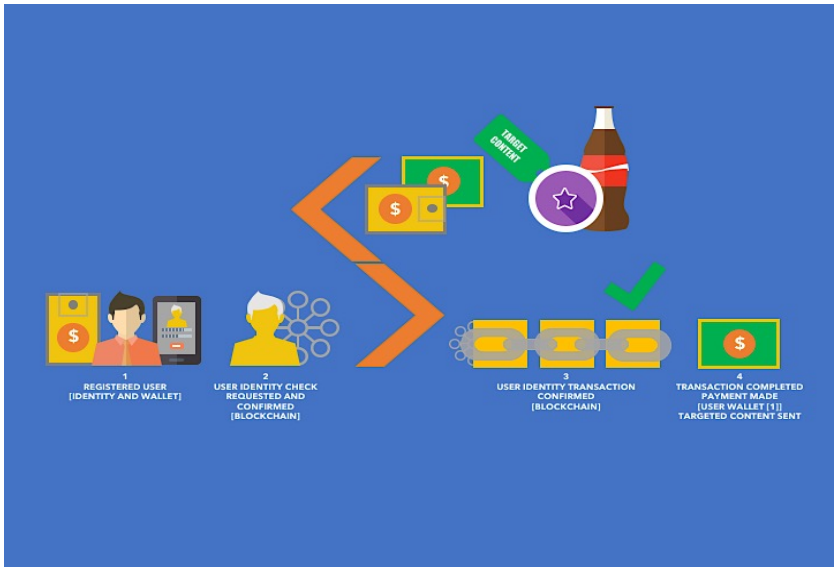
OVERVIEW

To support the operation and user adoption of the Air Platform, a mobile/cellphone application (initially for Apple iOS/Google Android, with other platforms to follow on an incremental basis) will be created for individual use. The application will secure and maintain an individual's digital identity, and is expected to be as 'lightweight' and as implicit to use for the individual as possible during operation.



Note: The screen defined within the above diagram is for illustration purposes only, and is therefore subject to change. However, the application design principles of simplicity and ease of use are to be maintained during the application finalization process.

Air also implements a novel approach to user adoption whereby an individual will receive an XID digital token micropayment to a digital wallet (to be integrated within the Air cell/mobile phone application), upon a successful identity transaction having taken place. Upon completion of the transaction, a targeted advertisement (or other content) based on the user's interests, will then be communicated via the cell/mobile application.



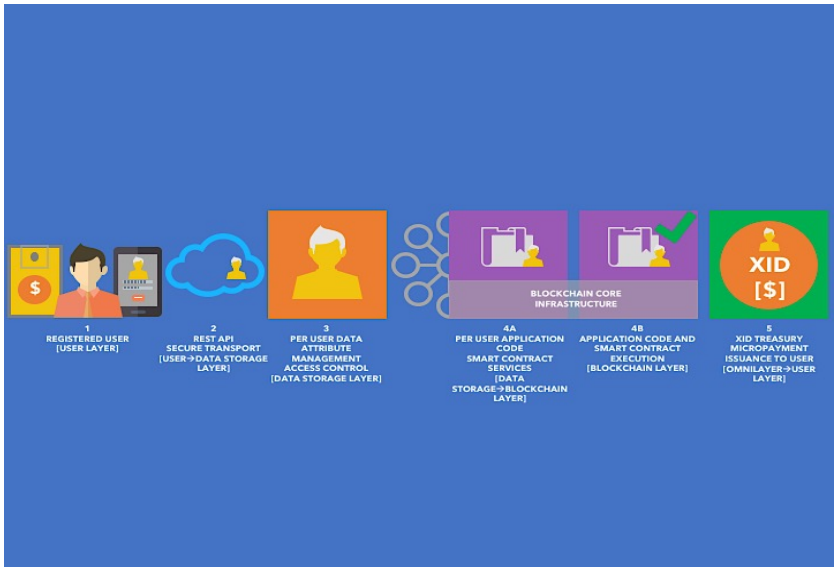
THE XID TOKEN AND OMNILAYER

XID tokens are 'minted', leveraging our partners Omnilayer asset issuance technology. Omnilayer is a platform for creating and trading custom digital assets and currencies. It is a software layer built on top of the Bitcoin Blockchain that enables next-generation Bitcoin features. The usage of the Omnilayer platform further enables XID and Bitcoin wallet compatibility for ease of use exchange.

XID will be held in Omnilayer treasury awaiting distribution upon a successful user identity based transaction taking place for any component within the Air consumer application domain.

COMMUNICATIONS AND INTEGRATION

All Air consumer application activities will communicate bi-directionally from the User Layer, towards the Data (Storage) Layer, leveraging the Representational State Transfer (REST) and Transmission Layer Security (TLS) protocols for onward secure communication towards the blockchain layer. Communication integration between blockchain and external systems will be completed in-line with the external systems integration overview as previously described.



CONCLUSION

This white paper has presented Air, a secure digital identity system that aims for ultimate flexibility and ease of use. The system aims to remove the need for knowledge regarding Public key cryptography from a user perspective, thereby enabling an enhanced management of a given identity, and a greatly simplified approach to Internet security.

We use a novel approach to user engagement via the facilitation of user micropayments, thereby allowing advertisers (or other parties) to increase content targeting, and enhance customer engagement.