TrustChain

A joint project conducted by Qumodo and Aleph Insights

QUMODO

ALEPH INSIGHTS

Executive Summary

This paper supports research undertaken by Aleph Insights and Qumodo to develop a proof of concept for TrustChain - a blockchain-based Airside Identity Card (AIC) management system.

Today, AIC management systems face myriad obstacles in their efforts to deliver a secure, consistent service. Several factors - including the varieties of pass, the diversity of the user community, a lack of consistency and the sheer volume of data involved – make these systems potentially inefficient and vulnerable to exploitation by insiders and other malicious actors. The systems are not designed to meet the standards of continuous vetting to which governing authorities aspire. There is a pressing need for an alternative that offers greater security, efficiency and compliance with modern standards of data protection.

We believe the TrustChain concept presents such an alternative solution. In its use of blockchain technology, it promises to overcome these problems and deliver tangible benefits in terms of security and efficiency. A blockchain is a decentralised database spread across independent nodes; it uses a chain of blocks to provide a secure, valid consensus between each node. In identity management, the blockchain offers a mechanism for verifying claims relating to identity properties (e.g. name, date of birth). The properties' values need not be included on the blockchain; instead, it stores an immutable record related to these values for verification.

The structure of a blockchain offers several distinct advantages over traditional identity management systems, including:

- Increased resilience, due to a decentralised structure.
- Immutable data, protected against the threat of tampering by insiders or malicious actors.
- Real-time, instantaneous updates to access control, supporting the goals of continuous vetting.
- Compliance with recent data protection legislation and the promotion of 'self-sovereign identity' - an increasingly prevalent concept espousing the individual's sovereignty over the use and storage of their own personal data.

A wide range of potential blockchain solutions have already been adopted by authorities in various jurisdictions, with innovative applications across identity management and other fields. Given the direction of travel, it would be prudent to explore how blockchain-based solutions can be leveraged to enhance AIC systems in greater detail.

We propose further research to test an adapted, bespoke version of the TrustChain concept demonstrator within a live (but controlled) operational setting. This will allow government to assemble more evidence and identify barriers to implementation, ultimately enabling stakeholders to determine the feasibility and timeframe for delivering a TrustChain solution.

Introduction

This paper supports research conducted by Aleph Insights and Qumodo in response to the APHIDS project run by the Vivace consortium on behalf of the UK government. The project sought to develop a proof of concept regarding TrustChain, a blockchain-based Airside Identity Card (AIC) system. TrustChain has been designed to allow authorised individuals working at commercial airports (such as baggage handlers, flight crew or maintenance workers) to access restricted areas securely. As a blockchain-based solution, it offers the opportunity to overcome many of the difficulties encountered by organisations running AIC systems today, delivering real benefits in terms of security and efficiency.

There are two components to the TrustChain project:

- First, the development of a TrustChain Concept Demonstrator. The demonstrator implements a basic instantiation of a blockchain-based identity management system, focusing on the use case of issuing, monitoring and revoking (where necessary) AICs. A summary of its methodology is captured in our Concept Demonstrator Report.
- Secondly, the production of this White Paper, which summarises TrustChain's underlying technologies, sets out the system's strengths and challenges and explores how TrustChain would function when fully deployed.

The paper addresses the following issues:

- Current challenges around identity management
- Vulnerabilities associated with traditional identity management systems
- The principles behind blockchain-based solutions and distributed ledger technology
- How blockchains work in the context of identity management
- The key benefits of using blockchain technology, in terms of security and efficiency
- Examples of blockchain-based identity management solutions already in use
- Conclusion

Current challenges facing AIC management systems

Commercial airports in the UK manage tens of thousands of personnel per annum with a legitimate right to access restricted areas - each of whom requires an AIC to do so. Managing this volume of AIC data comprehensively, efficiently and above all *securely* is a major challenge. In reality, the practicalities of verifying identity are far more complex than the simple act of checking someone's pass. A range of variables are in play, each complicating the process. For example:

- There are different varieties of pass, both temporary and permanent, conferring different rights on the user.
- There are different levels of security in certain areas within airports. Some (e.g. the runway) are more sensitive than others, with a variety of different access rights and physical security controls.
- The user community is diverse, and some roles have specific access requirements (e.g. permission to carry equipment, or unsupervised access).
- Most crucially, different airports use different systems, rather than adopting a common approach. There is very little consistency in how records are managed between airports. Large airports may use well-resourced, centralised, integrated databases, whereas, small airports may take a more *ad hoc* approach. Some AIC holders (including flight crew) move daily between airports; their access rights must be verified wherever they go.

Even the act of issuing of one AIC pass involves multiple data transactions. Currently, the process might operate step-by-step along the following lines:

1. An employee submits their personal data to their employer.
2. This information is verified by the employer's Authorised Signatory.
3. It is then submitted via a third party platform to the relevant security team in the airport itself.
4. The information is scrutinised and approved by an individual within the airport security team (possibly requiring additional checks with the Disclosure and Barring Service - DBS - or other external safety bodies).
5. This approval and the underpinning personal information is entered onto the airport's pass approval system.
6. The approval is communicated back to the employer and employee, who receives the appropriate pass for that airport.
7. The pass is activated and the various access control permissions are transferred to the access control system used by those responsible for monitoring access within the airport.

8. When the employee reports for work and displays their newly-issued pass at the airside access point, a security official is then able to confirm that the employee has legitimate airside access using this system.

The vulnerabilities of existing systems

Standard identity management systems used today, as broadly described above, have a number of critical vulnerabilities.

- Individual identity data may be spread across multiple systems and databases, each of which offers a different vector through which information could be tampered with. In other words, each additional database or system used to store data increases the size of the 'attack surface'. We should consider the susceptibility of this data to the insider threat. At each of these points, across multiple systems and databases, the data could be vulnerable to alteration by a wide pool of individuals with *legitimate* access.

- The proliferation of data across multiple locations means that any changes (e.g. information regarding a new criminal conviction) may not percolate through the system. In these conditions, there can be little assurance that a dataset is fully consistent. This creates a manual synchronisation challenge, which if unresolved can lead to error conditions broadly defined as the Byzantine Generals Problem.[1] The resulting inconsistency constitutes a genuine security risk and undermines the integrity of any aspirations towards a meaningful continuous vetting process.

- Personal data proliferation also means that personal data gain a wide exposure, often to users who have no requirement to know this information. The 'right to be forgotten' (codified under Article 17 of the GDPR) thus becomes more difficult to implement using current systems.

- Within any identity management system, there are central authorities (e.g. an airport's pass approver/security manager) that may represent a single point of failure or a point of vulnerability to insider attack.

- A direct trust relationship is required between these authorities and external verifiers (e.g. a Certificate Authority, or employers vouching for staff). Efforts to maintain this trust relationship carry an administrative burden for all parties.

- Isolated systems used across different airports do spread risk - but they also mean that every airport is different. The resultant lack of interoperability between airports gives rise to potential errors as data is shared between them; some information may be lost in translation. An obvious solution would be the adoption of a universal, centralised system (e.g. a single airport ID card). However, if implemented using the technologies in widespread use today, this would increase the risk of single point of failure, and require an increasingly complex range of solutions to accommodate local variations and idiosyncrasies.

- The continued reliance on paper documents or physical passes to confirm identity creates a forgery risk and seems anachronistic in today's digital workplace.

[1] Lamport, L., Shostak, R. and Pease, M., 1982. The Byzantine generals' problem. *ACM Transactions on Programming Languages and Systems (TOPLAS)*, *4*(3), pp.382-401.

Blockchain as a potential solution – key principles

The emergence of blockchain technology offers a potential solution to the problems outlined above. A solution such as TrustChain promises to deliver a more secure, robust approach to identity management for AICs. The underlying technologies supporting this solution are summarised below:

Distributed ledger technology

A distributed ledger, of which blockchains are a subset, is a database spread across several nodes or computing devices. Each participant node replicates and saves an identical copy of the ledger, updating itself independently.

The groundbreaking feature of distributed ledger technology is that the ledger is not maintained by any central authority; updates to the ledger are *independently* constructed and recorded by each node. The nodes then communicate with each other to agree on these updates to ensure that the majority agrees with the conclusion reached. This agreement on one copy of the ledger is called consensus and is conducted automatically by a consensus algorithm. Once consensus has been reached, the distributed ledger updates itself and the latest, agreed version of the ledger is saved on each node separately.

Distributed ledger technologies can drastically reduce the financial cost of running trust and assurance systems, while at the same time improving the trust relationships between users and nodes on the network. In their general application across a number of spheres, the architectures and structures of distributed ledgers offer an alternative model of assuring information - potentially helping to alleviate our dependence on banks, governments, lawyers, notaries and regulatory compliance officers.

Blockchains

One form of distributed ledger technology is blockchains, which were pioneered during the development of cryptocurrencies such as Bitcoin. Blockchains employ a chain of blocks to provide a secure and valid distributed consensus. A blockchain is distributed across and managed by peer-to-peer networks. It can function as a standardised medium of exchange using a network of independent nodes, without a centralised authority or server managing it. The blockchain's data quality can be maintained by database replication and computational trust.

A central precept in the use of blockchains is the principle of ensuring that a consensus is reached and agreed on by all nodes. For example, in cryptocurrencies this represents a snapshot of currency ownership at any given time. In the context of identity management, this represents the status of various fields of personal data which may need to be authenticated.

There are different approaches to developing consensus algorithms; the choice of approach may depend on factors such as the goal of the distributed ledger, the degree of trust in its nodes and the volume of nodes involved. Some of these different approaches are discussed later in this paper.

How do blockchains work in identity management?

Figure 1 - The identity challenge (Peter Steiner, The New Yorker)

In applying blockchain technology to identity management, blockchain entries come to represent references through consensus about the status of various people or organisations (hereafter known as 'Owners'). 'Identity' in this context refers to a series of properties or characteristics relating to an individual that can be verified - for example, a person's name, date of birth (DOB), home address, photographic ID, fingerprints and other biometric information. Proving an identity in this context is achieved through the verification of claims relating to these properties. The exact properties that must be verified will vary; in more stringent identity management scenarios, more properties may require verification (and by higher levels of authority) than for less stringent cases.

Blockchain offers a mechanism for verifying these claims. The blockchain comes to represent a unified 'ground truth' about an individual's identity properties - similar to the use of blockchains in cryptocurrencies to verify claims about a person's wealth. The actual values of these properties (e.g. DOB) need not be included on the blockchain, remaining hidden from all users. However, the blockchain stores an immutable record related to these values for verification. This is achieved through a decentralised public key infrastructure (DPKI)[2] which facilitates selective and secure access to information.

There are several system features and design variables that determine how a blockchain-based solution might be implemented, and how it might function. These include:

- User roles
- Transactions and verification
- Information storage
- Agency and agents
- Data input
- System integration
- Level of centralisation

[2] Christopher Allen, Arthur Brock, Vitalik Buterin, Jon Callas, Duke Dorje, Christian Lundkvist, Pavel Kravchenko, Jude Nelson, Drummond Reed, Markus Sabadello, Greg Slepak, Noah Thorp, and Harlan T Wood (2015) Decentralized Public Key Infrastructure, Rebooting the Web of Trust. http://www.weboftrust.info/downloads/dpki.pdf

User roles: the TrustChain

One of the fundamental differences between traditional identity management and a blockchain-based approach is how trust operates within the verification process. Within the current paradigm, centralised sources of authority serve to verify an individual's identity properties.

- For example, the Passport Office acts as an authority to verify a range of identity properties, such as name, DOB, photographic likeness etc.

The trust relationship is hierarchical, with authority often being delegated downwards - such as where an employer is entrusted to verify an identity claim by reviewing a passport and vouching for various identity properties based on this.

Blockchain identity management uses no such hierarchy. Instead it should be thought of as a network, or an interconnected web of trust - known as the TrustChain. Any user can verify an identity claim; it is then up to the entire user group to determine how much trust they place in the verifier. In some cases, trust can be an emergent property of the network; for example, a user may become a trusted verifier over time based on a reliable track record. This system does not preclude the ability to use pre-selected nodes of authority (such as a government agency), but it does not structurally *require* them.

Within the network of users within a blockchain-based system, there are a range of specific roles which might be considered as different nodes within the network. Indeed, some users (whether organisations or individuals) might fulfil multiple roles.

- (Information) Owners: Owners are the subjects of the identity management system - in this context, the AIC pass holders themselves. They are responsible for populating their records and making claims about their own identity properties, which others may or may not verify. They should be viewed as owners of their own personal data, who temporarily grant access to some elements of that data in order to prove their identity and gain access as required.

- Verifiers: These individuals authenticate the identities of different 'Owners' to support security and business objectives. Verifiers might include the airport security teams or those responsible for issuing AICs.

- Issuers: Issuers are the bodies that issue verification of claims about an 'Owner'. They might be trusted authorities (such as the Passport Office for citizenship information, or the DBS for criminal records checks). Alternatively, they might be other types of organisational bodies (e.g. airside safety training providers, verifying that the Owner has completed mandatory training - or the employer, in this case verifying that the Owner has an employment contract). Issuers may even be independent individuals (e.g. a person verifying a photographic likeness of an acquaintance).

- Overseers/Auditors/Special Users: These are organisations that may have a sanctioned role in reviewing identity claims for the purposes of national security - such as the police, the Office for Security and Counter-Terrorism or the National Crime Agency. They may have dispensation to obtain data under warrant, or strategic oversight of AIC data (including analytical capabilities). They may even be responsible for implementing an AIC blacklist, flagging relevant pass applications of concern as they arise.

The way these roles are implemented - including their permissions to access data, the way they interface with the system and their required responsibilities - will be crucial in determining how a future TrustChain might function.

Transactions and verification

A blockchain-based identity management system is founded on the basis of 'verifiable claims'[3] - i.e. statements about an individual (the Owner)'s identity properties which others may verify as true. A verifiable claim can be likened to a physical piece of identification, such as a passport, except that the identity information therein is more highly atomised.[4] Rather than containing lots of information in one place (as in a passport), a verifiable claim will only contain a small packet of personal data.

- For example, a single verifiable claim might contain only your DOB, while another may contain your place of birth. This makes the sum of the information less vulnerable to identity theft or tampering at any point.

In the context of AICs:

- the subject of the verifiable claim is the Owner (e.g. an airport worker)
- the claim is supported (or 'issued') by the Issuer (e.g. a trusted authority such as a government agency).

This support for the claim is achieved through what is known as an 'issuing protocol', in which the Issuer confirms an identity property is true for an Owner. This verified claim is then recorded on the blockchain in a highly encrypted, immutable fashion (a 'hash') by a cryptographic algorithm.

Consequently, the actual property value itself cannot be determined outside of the 'verifying protocol'. This protocol occurs when the Owner needs to prove their identity (for example, on visiting the airport). At this point the Owner makes a statement about their identity to the Verifier (e.g. the airport security team); the verifying protocol is then enacted. This requires the Owner's cryptographic key and the value of the identity property (e.g. DOB). This is checked against the corresponding hash on the blockchain by the blockchain's cryptographic algorithm. If the value and the key match, the claim is verified successfully.

Although the various transactions within this process (*illustrated below*) may appear convoluted at first glance, a blockchain-based system would be designed with user-friendly interfaces, accessible on any computing device, to deliver these transactions seamlessly and securely.

[3] Also referred to as Verifiable Credentials (see https://w3c.github.io/vc-data-model/). We have opted to use the original term verifiable claim throughout this paper in order to be consistent with the Sovrin Foundation terminology.

[4] The transactions underpinning verifiable claims are based on the implementation of pairwise decentralised identifiers, which are created for every individual claim and every individual. It is the requirement for matching these two separate identifiers that gives blockchain encryption its strength. For more detail see https://sovrin.org/wp-content/uploads/2018/03/How-Sovrin-Works.pdf

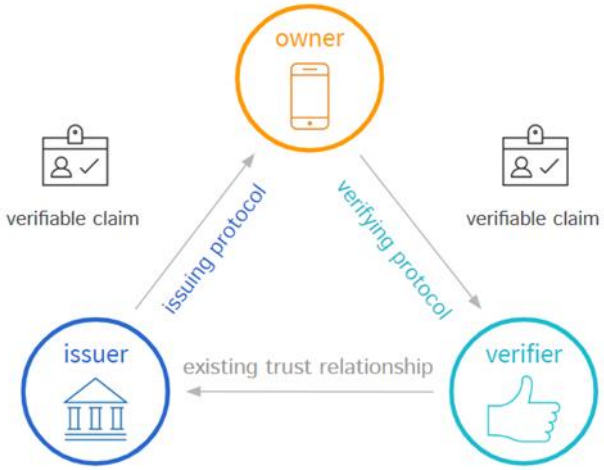

Figure 2 - Transaction and verification in the TrustChain

Verifiable claims need not be tied to an individual's specific attributes, but might also represent more abstract concepts such as the ownership of a valid AIC. They can also enable zero-knowledge proofs (ZKPs) that help to protect personal data by providing only minimal information with which Verifiers might satisfy their access criteria.

For example, ZKPs might be used to confirm that an individual is over 18 years of age, rather than verifying their precise date of birth.

Information storage

Information storage is a key consideration in the development of a blockchain-based identity management system. The following data must be stored to enable successful functionality:

1. Protected Personal Information (PPI): e.g. Personal data such as name/DOB or images/scanned documents.
2. Verifiable claims: These primarily relate to claims that an Owner makes about themselves, verified by Issuers - but might also relate to the permission for an individual or organisation to access particular parts of an Owner's data.

Storing sensitive PPI in the blockchain is not without risks. The blockchain may be partially or fully visible to users, and though its content is pseudonymised and encrypted, it will remain vulnerable to brute force decryption. There is also a risk that private keys for encrypted data may be accidentally compromised through loss or the theft of devices.

Storage of sensitive PPI should therefore be held 'off-ledger'. In other words, PPI can be stored on *another* secure system and referenced by records on the blockchain. The only data stored on the blockchain itself are pseudonymous public keys and unique addresses that enable the exchange of private data. If any part of the chain is compromised, access to the corresponding 'off-ledger' information may be revoked by external content management systems (for example, by changing encryption keys or removing the data entirely).

Crucially, the ledger-based solution allows you to track exactly who should have access, enhancing the detection and prevention of unauthorised access and helping to mitigate the insider threat. Additionally, if the secure external system where PPI is stored is compromised and values for identity properties are changed (e.g. alterations or substitutions to the photograph associated with an AIC passholder), these changes will not be validated by the blockchain. This significantly reduces the system's vulnerability to record tampering.

To improve performance and security controls further, additional layers of security are available if required. This might include reducing the amount of data stored on a block (lessening the impact of any breach), or decreasing the volume of storage (and resulting computational load) within the chain.[5] A wide range of storage solutions may be employed, including:

- completely centralised offline storage[6]
- cloud-based solutions
- totally decentralised peer-to-peer (P2P)[7] solutions

This provides enormous flexibility, both in how data is stored and how associated costs are managed.

Agency and agents

Another difference between traditional identity management systems and blockchain-based solutions is the onus on enabling Owners to exercise agency over their own personal information. This relates to the ability to determine who sees what information, but also covers the right to withdraw their personal information from the system altogether. Given that a blockchain-based system does not contain the values of the identity properties themselves, it is easier for an Owner to maintain ownership of their own information. This enables the Owner to update that information and grant or withdraw access permission as desired.

[5] Maesa, D.D.F., Mori, P. and Ricci, L., 2017, June. Blockchain based access control. In *IFIP International Conference on Distributed Applications and Interoperable Systems* (pp. 206-220). Springer, Cham.
[6] In extremis, it would be possible to store only offline, paper library references, if so desired. A user awarded access rights to a particular datum could present this claim to the librarian and gain physical access.
[7] Blockchain is able to reference data held in decentralised storage via url/torrent identifiers. Zyskind, G. and Nathan, O., 2015, May. Decentralizing privacy: Using blockchain to protect personal data. In *2015 IEEE Security and Privacy Workshops* (pp. 180-184). IEEE.

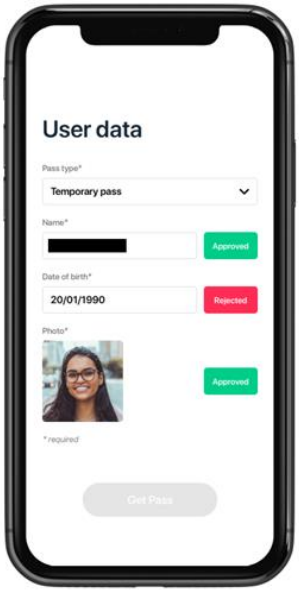

Figure 3 - Using agents to manage data (screengrab from the Concept Demonstrator)

- In the example of applying for an AIC, it would be a precondition for obtaining and maintaining a pass that access permissions be granted to the relevant authorities. However, it may be that when the pass is no longer required, the Owner may be able to withdraw these permissions.

In addition, it is possible to engineer the solution so that particular trusted parties - or 'agents' - may act on behalf of the Owner with regards to controlling private data.

- In the context of AICs, employers could act on behalf of employees to maintain or manage some of their identity properties - for example, within the process of applying for a pass. This obviates the need for employees to have their own accounts or devices.

Each user has a software agent that acts on their behalf, protected against interference by other parties. These agents are responsible for the control of private data, handling keys and alerting the user to requests for information and the status of verifiable claims (whether 'pending' or 'approved'). These agents could take the form of a smartphone app and/or or a web app, for example. In some blockchain-based identity frameworks (such as the Sovrin Network,[8] a public service utility enabling self-sovereign identity on the internet), these agents are designed in a highly compartmentalised manner in order to maintain high levels of security.[9] The degree of agency given to Owners, and the use of agents, therefore represent crucial design variables for any future TrustChain system.

Data input

Individual users and institutions acting on their behalf require a means to input data. For example, a national authority can issue qualified identity data about a person, and provide verification of that data directly. In contrast, an Owner can enter personal data themselves, but this self-reported data will invariably have a lower degree of assurance.

While the authenticity of data entered by oneself is very difficult to guarantee, trusted third parties could verify claims about these data directly onto the blockchain, offering greater levels of assurance. This is analogous to the widespread practice of obtaining 'verified copies' of document from institutions.

- For example, an Owner might upload a photograph of themselves in order to share that digital likeness with other parties. A trusted institution could provide assurance that the image is indeed a likeness of the individual with a digital signature. Additional digital signatures would increase the apparent assurance of the image as the user asked more institutions to sign.[10]

[8] https://sovrin.org/
[9] For example, in the Sovrin system each combination of verified and verifiable claim is given its own agent to manage the data transfer.
[10] Digital likenesses are an interesting case. As people age or as their appearance changes then these images become less good likenesses. A suitably featureful solution could allow automated expiry of these signatures.

Qualified data can be imported in a format which facilitates compartmentalised, selective disclosure of information.

- For example, a driving licence issued by a licencing authority (e.g. DVLA) contains multiple pieces of data about the licence holder. It may be advantageous to break these individual parts up to facilitate zero-knowledge-proof claims.

The question of who is allowed to input what data, and to what level of assurance, may be hard-baked into the blockchain-based solution. Alternatively, this could be handled more democratically, whereby all users could enter any data and verify anything whatsoever (with these claims and verifications all being captured on the blockchain). The balance between control over the system and such flexibility will need to be considered prior to implementation, given the use case.

Integration with existing processes

Blockchain-based identity management systems can also be integrated with existing systems, databases and infrastructure.

- For example, blockchain-based identity frameworks such as the the Sovrin Network are able to operate alongside and in concert with legacy systems for managing online identity verification. This capacity for systems integration ensures that blockchain-based solutions can be rolled out smoothly and without causing significant disruption.
- Blockchain-based solutions can also make reference to existing databases used to store private information, rather than replacing them in their entirety. In this case, the blockchain is providing an immutable 'official' record of verified claims. If data is changed locally without verification via the blockchain, the system will not recognise that data as valid.
- The blockchain can also integrate with physical infrastructure (e.g. gates, doors and biometric sensors such as facial recognition or thumbprint scanners). This could enable airside access infrastructure to act as a Verifier, authenticating claims about an Owner's access rights or biometric markers and allowing secure access to restricted zones.

This ability to integrate with existing processes is a key advantage of blockchain-based solutions. It allows organisations to introduce such a solution gradually, replacing existing processes and apparatus on a piecemeal basis and avoiding wholesale transformation and disruption to business-as-usual.

Figure 4 - Integration with biometric sensors is possible with TrustChain (taken from The National, www.thenational.ae)

Level of centralisation

Blockchain-based systems enable the use of decentralised networks of trust. Cryptocurrencies were one of the first use cases to exploit this feature, with transactions recorded on the blockchain for the entire community to see. Such openness is at the heart of the trust network. However, as stated earlier, blockchain technology does not preclude the possibility of having central, trusted authorities such as government agencies within your network.

- For example, in the context of identity management, the fact that the Passport Office has verified a particular claim would be visible on the blockchain to all users.[11]

The level of centralisation within the system also determines how the blockchain is governed and incentivised. For a single, agreed upon version of the blockchain to exist, there needs to be a consensus process for deciding the composition of each new block. In the AIC use case, each block would relate to a number of verifiable claims; this would determine the authoritative view of the blockchain as it evolved. This process is underpinned by a consensus algorithm, tailored to represent governance constructs that are either:

- *centralised*, e.g. a 'Proof of Authority' system (whereby a given authority decides the composition of the next block); or

[11] However, the exact details of the personal information they were verifying would be indecipherable until the User permitted a Verifier to access the information through a verifying protocol.

- *decentralised*, e.g.in a 'Proof of Work' system (where a community is involved in an arbitrary competition, incentivised by a winner's fee, for the right to 'place' the next block).

Other governance constructs include:

- 'Proof of Stake', where the creator of the next block is chosen via various combinations of random selection and wealth or age; and
- 'Proof of Capacity', where individuals bid for the rights to decide the next block's composition, using storage capacity as the bidding resource. The more storage capacity a user stakes, the greater the probability of winning the rights.[12]

Multiple approaches can be used in parallel to add robustness and flexibility. Algorithm selection within a blockchain-based solution is a key engineering decision; it should be informed by the intended purpose of the solution and other constraints such as the desired degree of centralisation.

Further analysis would be required to identity the most appropriate approach (or blend of approaches) for an AIC system. Of course, the exact governance construct chosen for a TrustChain solution will incur costs for computation, storage and communications. In general, the more decentralised the approach, the more expensive the running costs will be; however, this does not factor in the external costs of administering a central authority.

[12] See Jenks, T (2018) Pros and Cons of Different Blockchain Consensus Protocols https://www.verypossible.com/blog/pros-and-cons-of-different-blockchain-consensus-protocols and Vasa (2018) ConsensusPedia: An Encyclopedia of 30+ Consensus Algorithms https://hackernoon.com/consensuspedia-an-encyclopedia-of-29-consensus-algorithms-e9c4b4b7d08f for more detail on other constructs.

The benefits of blockchain: security and efficiency

The features of blockchain technology offer several distinct advantages over traditional identity management systems. In short, blockchain gives organisations the opportunity to deliver significant improvements in both the security and efficiency of their AIC systems. These benefits - including, critically, a more robust underpinning of continuous vetting and increased assurance against the insider threat - are summarised below.

Decentralisation increases resilience and efficiency

The decentralised structure of most blockchains increases the resilience of a blockchain-based AIC solution and reduces the administrative burden on centralised authorities.

- Each Owner's identity data is individually encrypted with a key pair, unique to the piece of data and the individual with whom it is shared. Any malicious actor would only be able to decrypt one person's verifiable claim at a time.
- Further, the atomised nature of verifiable claims means that the malicious actor would only ever be able to obtain small packets of information. By contrast, unauthorised access to a traditional spreadsheet holding multiple passholders' data is far more damaging, enabling such actors to change any data point for any individual therein.

Blockchain's consensus approach to trust would also ensure that, once claims had been verified and represented on the blockchain, the system itself would continue to provide the source of trust for identity properties. Such a system would not need to rely solely on trusted authorities repeatedly checking Owners' identity properties (e.g. gathering scanned copies of passports, or proofs of address).

- For example, an AIC applicant may have a verified claim regarding their DOB, verified by an approved Issuer. This could be referred to by anyone requiring this data in future, with its authenticity reliably underpinned by the blockchain.

Some models of implementation also allow for the decentralisation of system running costs - e.g. where the cost of verifying claims can be based on the number of claims accessed by a user, or where users are charged based on the amount of storage their usage of the system requires. This potentially presents a fairer, more equitable pricing model for system users.

Immutability of data helps to mitigate insider threat

The structure of a blockchain means the data record it represents is immutable, given that each new block contains a hashed representation of the entire preceding chain embedded within itself. In order to change data within one block, anyone trying to alter the blockchain would need to simultaneously alter the data in the target block and *all subsequent blocks* in the chain - all before the next block is laid down. In real terms this is impossible. This tenet sits at the heart of blockchain's immutability.[13]

[13] It should also be noted that multiple identical copies of the blockchain are held by different nodes within the community. Counterfeiting the entirety of the blockchain is thus rendered even more difficult.

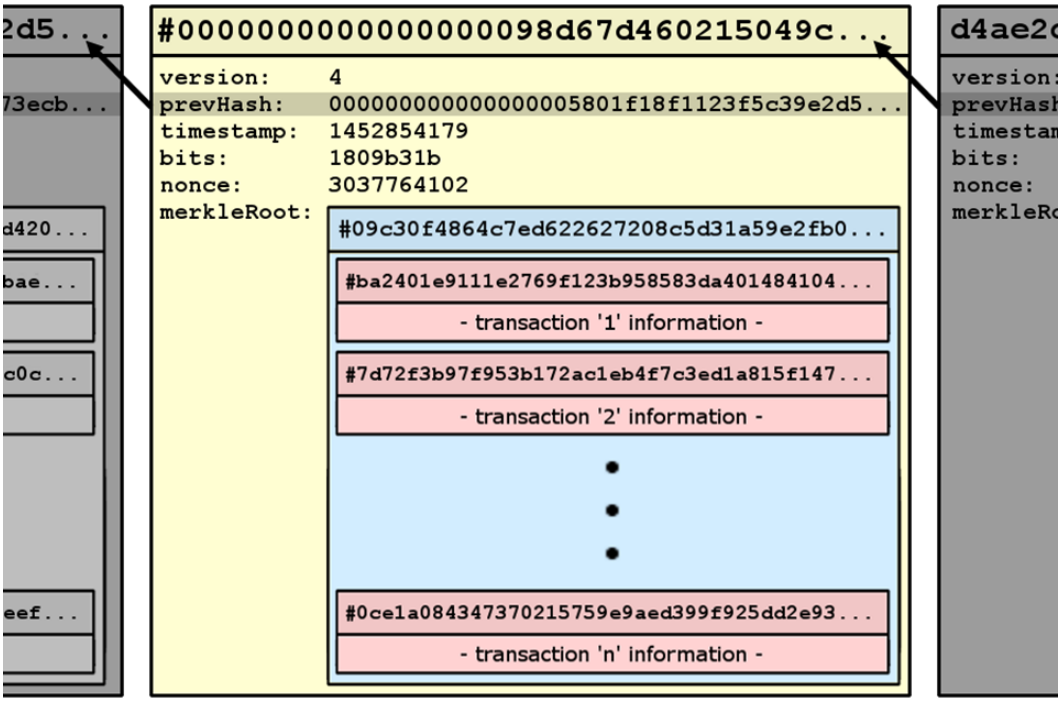

Figure 5 - Each block in the chain references the previous block (taken from https://blog.scottlogic.com)

The advantage this confers in the context of an AIC system is that verified claims cannot be altered. Consequently, while it might be relatively easy for an unauthorised user to alter the photograph of a pass holder on a local airport security database, this photograph would no longer match the photograph referenced within the blockchain's hashed record. The new photograph would therefore be identified as invalid within the system.

Instantaneous updates support continuous vetting

Within a blockchain-based system, records pertaining to an Owner's identity properties are linked to the blockchain in real-time. This means that business rules could be encoded within a blockchain-based AIC system to deliver instantaneous changes to access control. Any changes to the blockchain would immediately be recorded on all parts of the system. This supports the goal of continuous vetting within AIC systems.

- For example, if a verified claim from the appropriate authority recorded that a passholder had acquired a criminal conviction, this could create a new verifiable claim that superseded the previous claim. This would invalidate any claims dependent on it, trigger an alert and enable a pass to be revoked automatically, with immediate effect.

Furthermore, verified claims about critical identity properties (such as the example above regarding a criminal record) can be recorded in perpetuity. The system can be designed so that important records will remain on the system when an Owner disengages from it, in such a way that it is no longer visible to users. Should the Owner then re-engage with the system, these records would still exist within the blockchain, indelibly linked to the pass applicant. Such continuity offers efficiency and brings clear benefits from a security perspective.

Transparency reduces the risk of system manipulation

Blockchain-based technology provides transparency for all data therein, operating on the principle of an open-source code base. This means that any changes to the status of verified claims and any changes to the code are open to scrutiny by the user community. Such transparency increases trust and heightens the difficulty of manipulating data or the wider system, and makes such manipulation easier to detect.

It also means that trust in Issuers can be easily accounted for, and even adjusted. All blockchain users can see the source of verification for given claims and use their own criteria to determine what might constitute a trusted source of verification for any given claim within a given context.

- For example, an employer's verification of identity properties may be sufficiently robust for a temporary AIC pass, which only grants escorted access to airside zones. By contrast, details supporting a permanent unescorted pass might require more rigorous verification by a government agency.

Similarly, a blockchain-based system would help Verifiers (e.g. pass managers) to respond to situations where a given Issuer (e.g. a particular employer) is no longer trusted. The blockchain could require all pass holders whose claims had been verified by the untrusted Issuer to re-apply. This transparency would facilitate better audit and analysis of Issuer behaviour.

'Self-sovereign identity' complies with new standards of data protection

Most blockchain-based identity frameworks are clearly designed to be compliant with data privacy and handling legislation (including GDPR 2018, IPA 2016, DPA 2018 and FOIA). These frameworks define themselves as consistent with 'self-sovereign identity' - a concept relating to the Owner's sovereignty over the use and storage of their own personal data.

In this context, genuine ownership of one's data is seen as a worthy aspiration, allowing an individual to control access to that data. Self-sovereign identity frameworks aim to support various libertarian principles that can be mapped across to GDPR legislation. These principles comprise:

- Control and assurance over personal data access - An SSI system can provide granular control over what data are being shared, together with revocation mechanisms.[14,15] Some blockchain frameworks support smart contracts, which could be used to enforce the user's consent automatically. For example, they might be obliged to sign a smart contract which consents to share their data with a specific organisation for the duration of their use of an AIC pass.

- Minimal disclosure by default - SSI operates on the basis of providing only the minimum amount of information required to satisfy a given criteria, using zero-knowledge-proofs where appropriate. This principle acts as an in-built constraint on the proliferation of personal data exposure and storage.

[14] Maesa, D.D.F., Ricci, L. and Mori, P., 2017. Distributed access control through blockchain technology. *Blockchain Engineering*, p.31.
[15] Maesa, D.D.F., Mori, P. and Ricci, L., 2017, June. Blockchain based access control. In *IFIP International Conference on Distributed Applications and Interoperable Systems* (pp. 206-220). Springer, Cham.

- The right to erasure - As described in GDPR in relation to EU citizens, the right to erasure - also known popularly as 'the right to be forgotten' - allows people to request the deletion of personal data. In an SSI system, an Owner has full ownership of their identity data and may simply withdraw the right for anyone else to access this data - in effect deleting it from the system. This is possible because the personal data itself is stored 'off-chain' rather than on the blockchain, with a unique encrypted identifier used to reference the data. Any changes to the data itself will invalidate the link between the data value and the record on the blockchain. Access relies on the Owner's consent and is enforced by SSI consent mechanisms, which also enable the revocation of any data accesses granted previously (if required).

- Anonymisation - References on the blockchain are pseudonymous and cannot easily be linked to individuals. In SSI systems, identifiers are cryptographically generated and cannot be linked to a specific person. Furthermore, a new identifier is created on a pairwise basis for every piece of data and its recipient. As a result, even if one identifier is attributed to an individual it will not compromise any other records.

- Data portability - GDPR seeks to protect an Owner's right to transfer their personal data from one place to another. The SSI system supports this right by combining different technologies that enable data portability, such as the distributed ledger, with standardised data exchange formats such as eXtensible Data Interchange (XDI).

- Audit of data use - The design of SSI systems enables the monitoring of verification protocols, where Verifiers seek to confirm particular identity properties related to specific Owners. This facilitates the easy auditing of any accessing of personal data, helping to monitor organisations and hold them to account for their use of that data.

SSI is a popular, rapidly emerging concept, very much in sync with public expectations and the legislative direction of travel regarding personal data use. It also enjoys the sponsorship of a number of major tech companies such as IBM[16] and Microsoft.[17] However, some aspects of its principles may not, at least on initial inspection, seem wholly compliant with the goals of an AIC system. For example, the 'right to erasure' could be seen to limit the ability of security services to monitor individuals who have previously held AIC passes.

It is possible, though, to address these concerns through a combination of both the technology itself and the use of proper consent procedures. Regarding the right to erasure, for example, the record of a reference to an Owner's AIC pass would remain on the blockchain, but would be indecipherable without the Owner's consent.

- One solution might be to incorporate an agreement within the pass application that the Owner would allow this information to remain visible to a particular government agency for a defined period of time.

[16] Gunter A (2018) Collaboration: Unlocking decentralized, digital identity management through blockchain. https://www.ibm.com/blogs/blockchain/2018/04/collaboration-unlocking-decentralized-digital-identity-management-through-blockchain/
[17] Outlier Ventures (2018) Microsoft announces compatibility with Sovrin and decentralized identifiers. https://outlierventures.io/microsoft-announces-sovrin-partnership/

- An alternative might be to consider the information regarding who has or has not held a pass as 'owned' by the pass-issuing authority, rather than the passholder themselves.

There are therefore a number of ways these kinds of discrepancies can be reconciled with the SSI concept.

In summary, SSI should not be viewed as an absolute set of conditions, but rather as a segment within a spectrum of data ownership models, championing the individual Owner as the primary guardian of their own personal data. Blockchain-based solutions (such as TrustChain) can be designed to reflect these SSI principles, and therefore represent a secure, efficient and c*ompliant* means through which to address the identity management challenges facing airports and other organisations today.

Examples of blockchain in use today

Blockchain-based identity management systems are already being implemented in a number of settings worldwide.

- Estonia was the first country to implement a blockchain-based digital identity solution as part of their e-Citizenship programme. Beyond conferring proof of identity, the sophisticated scheme facilitates online authentication, digital signatures and electronic voting. It also links to medical records/prescription services, tax records and benefits claims.[18]

Figure 6 - The Estonian Digital Identity Card (taken from www.leapin.eu/articles/e-residency)

- The government of Dubai has partnered with the UK startup company ObjectTech to provide enhanced airport security using blockchain-based solutions. Work is in train to develop digital passports that could eliminate the need for manual checks at Dubai International Airport. The system will combine biometric verification and blockchain-based identity management, and is being designed to verify people through images as they move around the airport. In doing so, Dubai aims to improve security while simultaneously reducing inconvenience to passengers. The solution will include a number of SSI features designed to give the Owner greater control over their own personal data.[19]
- There are other national and provincial governments with active research programmes in this area, including in India, Singapore, Australia and the State of Illinois.

[18] https://e-estonia.com/solutions/e-identity/id-card/
[19] D'Cunha (2017) Dubai Sets Its Sights On Becoming The World's First Blockchain-Powered Government. Forbes https://www.forbes.com/sites/suparnadutt/2017/12/18/dubai-sets-sights-on-becoming-the-worlds-first-blockchain-powered-government/

- In addition, many initiatives by charities and NGOs are seeking to leverage blockchain-based solutions to provide vulnerable people such as refugees or homeless people with digital identities, in the hope of combating human trafficking and modern slavery.[20]
- The ID2020 Alliance is a network of charities and tech companies which are exploring, among other things, the potential for blockchain-based identity management systems to enhance people's lives in the developing world.[21, 22]
- Some industry-specific blockchain-based identity management initiatives are also in use, such as the Mobility Open Blockchain Initiative.[23] This programme was founded by the automotive industry to consider the applications of blockchain-based identity management for drivers and their use of vehicles, promoting greener, safer and more efficient mobility.

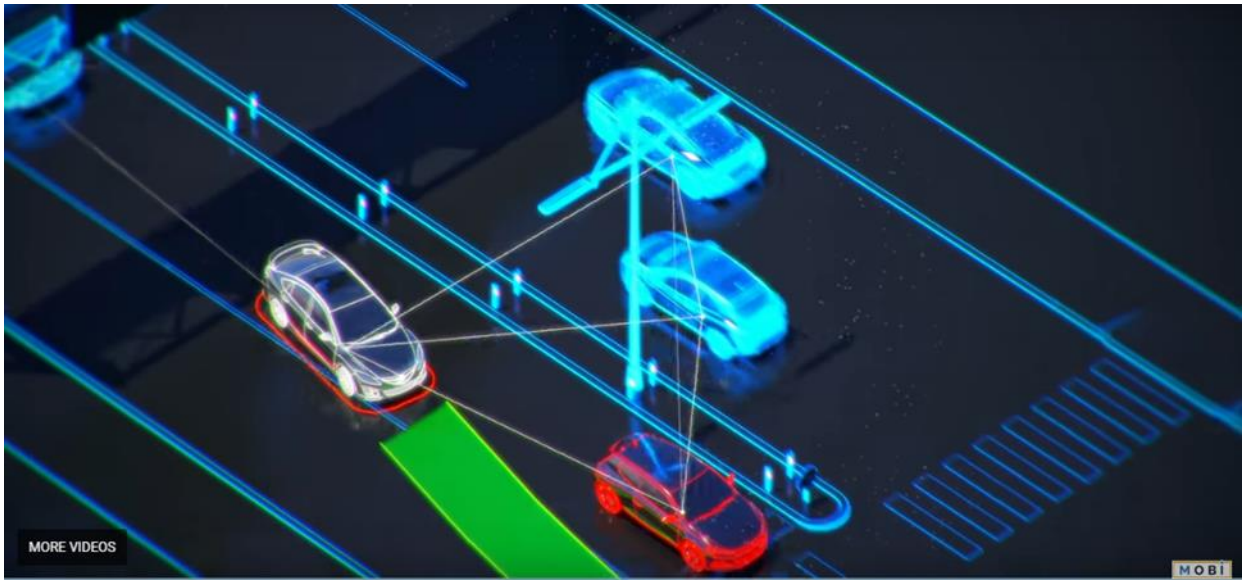

Figure 7 - MOBI uses blockchain technology to identify vehicles and drivers (taken from https://dlt.mobi/)

- Technology companies and foundations have also been involved in developing frameworks to support blockchain-based identity management systems. The Sovrin Trust Framework[24] is one of the most prominent of these. It uses a public permissioned distributed ledger that provides public access for identity owners, while permitting only trusted, vetted entities to serve as nodes. The Sovrin Foundation is a leading proponent of the SSI philosophy.
- A number of development platforms are also enabling developers to create decentralised applications for multiple purposes, including identity management systems. One of the

[20] Humenansky, J. (2018) The Impact of Digital Identity. Blockchain at Berkeley. https://blockchainatberkeley.blog/the-impact-of-digital-identity-9eed5b0c3016
[21] https://id2020.org/digital-identity-1/
[22] Bindi, T. (2017) Microsoft and Accenture develop blockchain ID system for refugees. ZDNet. https://www.zdnet.com/article/microsoft-and-accenture-develop-blockchain-id-system-for-refugees/
[23] https://dlt.mobi/
[24] https://sovrin.org/library/sovrin-trust-framework/

most widely used such platforms is Ethereum,[25] which is open-source and community-maintained.

In summary, there are a wide range of potential blockchain solutions in use today, all of which were designed with particular use cases in mind. It is unlikely that any single 'off-the-shelf' system will directly meet all the requirements for aTrustChain AIC system at this stage. Such a solution will require a blend of existing technologies and bespoke elements. Our conclusion below highlights some key considerations in designing such a system.

[25] https://github.com/ethereum/wiki/wiki/Ethereum-introduction#about-ethereum

Conclusion

This paper has made the case for the potential application of blockchain technology (in the form of TrustChain) as an AIC management solution. The concept demonstrator we have built for this project, summarised in the accompanying Concept Demonstrator Report, demonstrates that such a solution can deliver some of the fundamental benefits outlined above.

Blockchain technologies are becoming more widely adopted and applied to the challenges of identity management in a digital world. The EU's Joint Research Centre has predicted the imminent demise of paper certificates as proof of identification in the near future,[26] and a number of foreign governments have already begun experimenting with blockchain-based solutions. Given the amount of time new conceptual systems can take to be approved, designed, developed, integrated, assured and deployed, it would be prudent to explore how blockchain-based solutions can be leveraged to enhance AIC systems in greater detail.

Blockchain technology offers a wide range of potential benefits for the AIC use case - notably its ability to facilitate continuous vetting, mitigate insider threats and enable compliance with data protection and privacy legislation. However, as a caveat, we note that some issues remain outstanding and will need to be addressed. These include:

- defining the legal requirements for such a system;
- establishing the economic model under which it operates; and
- managing its integration with existing systems.

Our research to date has established some broad parameters regarding the likely shape of a blockchain-based AIC solution.

- For example, it will probably require higher levels of centralisation than many blockchain systems, with trusted agents (e.g. government agencies) operating within the system.
- Additionally, the level of self-sovereignty granted to Owners is likely to be partially restricted to some degree.

However, we have also established that there does not appear to be an existing model which could be easily applied to the AIC use case. The technical and organisational challenges of implementing such a system will need to be fully scoped before any design decisions are finalised.

In conclusion, we propose a more detailed study which will test an adapted, bespoke version of our TrustChain concept demonstrator within a live (but controlled) operational setting. The study should assemble more robust evidence regarding the effectiveness of this model, as well as pinpointing some of the real-world barriers to implementation. This work would then enable stakeholders to consider associated costs and benefits, in order to determine the feasibility and timeframe for delivering the TrustChain solution in the context of AIC identity management.

[26] Grech, A. & Camilleri, A. (2017) Blockchain in Education. JRC Science for Policy Report. European Commission. http://publications.jrc.ec.europa.eu/repository/bitstream/JRC108255/jrc108255_blockchain_in_education(1).pdf