Mamoru – Protect what you love

Blockchain SAAS solution for the Identity of Things

Preface

In a 21st-century world, we define ourselves increasingly by the products we own. From items such as laptops and smartphones which enable the smooth running of our lives, through the cars and bicycles which power our journeys from A to B, to the branded handbags and watches that enhance our lives with their aesthetic appeal and collectability, we are surrounded by possessions that make our lives better in every possible way.

However, in an increasingly connected and borderless world, it has never been easier for bad actors to steal high-value portable assets, to fake authenticity or to alter log books.

Bicycles are stolen in Berlin and are sold on in Amsterdam or Lille; luxury fashion accessories are counterfeited; classic cars are written off and then resurface with new bodywork and a fresh coat of paint.

While this is inconvenient for consumers, it can be even more damaging for manufacturers, resellers and insurance companies. National and local registries exist for some asset classes, while some manufacturers or stores keep records (in many cases on paper). But there is no universal oracle maintained by a neutral authority whose data cannot be tampered with or lost.

Much work is being done in the area of KYC and IAM as financial institutions and digital service providers attempt to map digital identities to living human individuals. But less work has been done in the area of mapping real-world assets to their digital identities, particularly in cases where the asset class is not one that is necessarily permanently connected to a network.

Of course, these systems exist, but they are usually proprietary walled gardens. Burberry makes use of RFID to display more information about some of their clothes on smart mirrors in store, when the shopper tries them on. But once the shopper leaves the store, they lose access to the information contained within their item.

Now imagine a world where this information is not only permanently available, but can be updated with details such as resale, theft, insurance claim or even maintenance records.

The ability to link an item's digital identity with the digital identity of the owner, and then update this record and make it accessible to anyone in the world, is key to our service solution. Below, we outline the technology behind our system, which provides a digital identity for any asset throughout its entire lifecycle, irrefutably proving ownership and recording key events such as ownership transfer and alteration.

This ability to offer updates in a physical object's digital record provides the universal, dynamic element that is missing from existing asset identity systems.

> **"Existing identity data and policy planning give IAM leaders and technology service providers (TSPs) a narrow view of entities leading to a static approach that does not consider the dynamic relationships between them" –** ***Earl Perkins, research vice president at Gartner***

Blockchain technology: transparency and immutability

In its simplest definition, a blockchain is a cryptographic tool that is used to build an immutable and unalterable time-stamped data record, without the need for a trust relationship between the parties involved in the transaction.

The first – and best known – use of blockchain technology is Bitcoin, the digital currency that allows individuals to make financial transactions with minimal cost across national boundaries. All records are fully decentralised, distributed across a network of thousands of computers in many different countries. By most standards, Bitcoin has been a resounding success: launched in 2009, it has proved itself a resilient and seemingly unhackable network for transferring wealth and storing value, while remaining totally public and transparent.

However, it soon became apparent that this type of decentralised, immutable, timestamped ledger had many uses other than cryptoeconomic transfer.

It is possible to use the Bitcoin blockchain to tokenise digital assets, but the landscape changed in 2015, with the launch of the Ethereum blockchain. This worldwide peer-to-peer network (aka the Ethereum Virtual Machine) allows more complex contracts to be executed and stored, and thus is suitable for registries of ownership, sale or any other change of state.

Mamoru is effective a service layer above the blockchain, allowing a broad range of interactions through a range of user interfaces, from sector-specific apps to administrative dashboards, thus allowing both product owners and producers to access information stored within the blockchain and update these records.

Proof of ownership

It is the universality of public blockchains such as Bitcoin and Ethereum that make them such an attractive proposition. If a consumer buys an item from a store, they will have a receipt with a record of the transaction, which may (or may not, depending on the item) connect the transaction (and possibly their personal identity) with some unique identifying feature on the asset they have bought.

They may be able to use this receipt as proof of purchase for insurance purposes or for showing a prospective purchaser if they transfer ownership, but both these circumstances require a high degree of trust. Especially if the receipt was issued by a reseller, there is no link back to the original provenance of the item. And even in the case of a newly purchased asset, there needs to be a degree of trust that the originating manufacturer or point of sale will remain in business long enough for records of sale to be persisted.

For a typical asset such as a bicycle, the owner's ability to prove ownership conclusively is problematic unless they are the original buyer. And even in this case, the new owner is required to place their trust in a paper receipt matched to a frame number, or in a registry held by a third party such as a police force, art register or industry body. The latter is likely to be (a) very localised and (b) inconvenient to verify.

The Mamoru solution is simple: once an asset has been given its own digital identity on a public blockchain, it may be transacted with, and these transactions may be publicly viewed by anyone using a blockchain explorer. As with any transaction on Ethereum, the identity of the individual is always anonymous. The mobile app allows the owner of the protected item to read back the details of their asset, or to make changes in state, but there is no way for a third party who does not have the contract ID to view the transaction.

The asset is linked to its digital counterpart by means of a smart tag. Specific hardware options will be discussed below, but the asset identity program is based on the NFC and BLE technology available in all modern smartphones. The ubiquity of mobile phones means that most people will have within their pocket the facility to scan and ascertain the ownership of anything covered by the Mamoru solution.

Thus the flow of asset ownership registration happens in three steps:

1. The item is fitted at the point of manufacture or sale with a chip bearing an identity (in the form of a hash) that has already been written to the blockchain
2. After sale, the new owner downloads the Mamoru app and creates an account
3. The owner uses the app to scan the asset and link their own account to the tag ID of the asset by means of a smart contract executed by and stored within the blockchain

Proof of possession

The distinction between ownership and possession may initially appear to be a matter of semantics, but in fact, the two are totally different concepts. Is every asset you own constantly in your possession? The Mamoru solution can also be used to log change events such as rental contracts, so that any change of state (a loan to a friend, or a commercial rental agreement) can be written to the blockchain and later read back.

While proof of ownership requires only a bearer token to represent on the blockchain the link between the individual and the asset, proof of possession is something more. As well as providing information about the status of the owned item, it is possible to write more complex information into the contract.

Proof of authenticity

The owner wishes to protect their asset by proving their ownership and being able to recover it if it is stolen. However, the manufacturer has, in their view, something more important to protect: the reputation of their product. The SaaS offering from Mamoru provides full identification of an asset, through its entire lifecycle of purchase, resale and maintenance.

Producers of counterfeits have become ever more sophisticated, and it can be difficult for an uninformed buyer to make a decision about whether a product is genuine or not. Many are made with a copy of a real serial number, and takes authentication by an expert to decide which is the real item. These problems disappear when one object is mapped to one identity within an immutable data structure like a blockchain, which is unforgeable and unhackable.

In the case of a bicycle which may have had its gears replaced with cheaper ones, or in the case of a collectable watch which has been maintained by someone who is not an expert, it is possible to track the entire history, showing maintenance events by licensed operatives and demonstrating the entire provenance of an asset through its chain of ownership and resale.

Location monitoring

The recovery of an asset (virtually an impossibility with existing property registers) can be viewed in two different ways: first, passively, where a stolen asset is discovered and identified by a third party; and, second, actively, where the owner chooses to track the location of a possession in real time.

In the case where there is a critical mass of individuals who have downloaded the free Mamoru app, reporting the discovery of a bike which has been scanned and found to be stolen, is as simple as tapping a button in the app and (optionally) adding a message. The location is sent to the bike's owner automatically, using the location of the phone.

For certain high-value items, it may be desirable to trace them using an app, by means of a GPS module which constantly broadcasts its location. The Mamoru solution offers the optional facility to see, in, real time, the location of your possession. As GPS modules consume a small amount of power, they are easiest to embed in something that already has some kind of power-generating capacity – an electric bicycle, for example. This has the added advantage of allowing us to provide aggregated data reporting. To alleviate privacy concerns, it should be remembered that the asset owner always retains the freedom to decide how much of their own identity to reveal.

Once registered, the ability to know beyond any doubt the exact location of an item is a crucially useful tool in its recovery. As GPS modules reduce in cost, size and energy consumption, we envisage a world where more and more personal assets will be come effectively theft-proof.

Logging and maintenance

The service layer offered by Mamoru, however, can do far more than simply provide tokenised proof of ownership and aid recovery of stolen assets.

This blockchain-based SaaS entity can act as a fully functioning database and administration console for manufacturers and resellers, and allowing a wide variety of assets to have their state and any events throughout their life cycle logged in the same way an automobile has a dealer-certified log book.

Once written, data in the Ethereum blockchain is free to access, which means that records of maintenance appointments, where relevant, and verified evidence that any repairs or interventions have been carried out by a qualified operative, add value to the product and make life easy for manufacturers who do not then have to maintain their own databases.

The global nature of the blockchain, along with its 100 per cent availability, means that customer data records can be shared across office locations in different towns, states or even countries.

Technology choice

Ethereum

Our primary concern when choosing a blockchain was to ensure it is a public blockchain. One of the reasons for this is our commitment to ensuring that the end user always has access to their data, regardless of whether they use a Mamoru app.

While we have carefully evaluated the possibilities offered by the Bitcoin blockchain, using the improved Colored Coin implementation, we decided that Ethereum, with its baked-in support for smart contracts, is the best choice despite the controversial hard fork.

NodeJS

The Mamoru back end is as minimal as possible. Business logic is kept in the blockchain, where it will be accessible in perpetuity, regardless of the existence of Mamoru. We designed our API to be simple and easy to maintain. We chose Node because of its ease of integration and the fact that it is a forward-looking technology with an active and numerous developer community.

Hardware
Mamoru is hardware-agnostic. We chose NFC initially as it is widely available and cheap, allowing us to be fast to market. But we are designing our app to work with any short-range communication technology available on mobile phones. Adopting BLE would allow iPhones to use the scanning feature of the Mamoru app, and there doubtless will be other technologies available in future which can be leveraged to extend Mamoru functionality.

B2B and wholesale insurance

As an ongoing record, the blockchain also has the potential to red flag multiple claims and other suspicious activity. Where the end user has chosen to link their real-world identity to their blockchain identity, KYC becomes possible for insurers and it is possible to build a pattern of behaviour based on the data which the individual user is happy to make public. Insurance companies traditionally demand a high degree of proof that insured items are authentic, demanding extra work from both the insurer and the owner of the insured item. Blockchain-based proof of ownership and authenticity automates this process and remediates the need for extra valuations and paper receipts and other documentation.

Open standard and privacy

Mamoru does not provide a proof of identity for human individuals. Other companies are working on these solutions, and we envisage a future where someone using the app may choose to use one of these third-party services to link their digital identity to their physical selves. Or they may choose not to do this, simply giving away as much data as they are comfortable with.

We categorically believe in the transformative power of blockchain technology as a force for transparency and self-determination. Because our back end is simply a proxy, and our contracts are stored in a public blockchain, the information is accessible regardless of Mamoru's existence.

What does this mean? The primary benefit is that data is persisted, whether or not the user decides to take advantage of the Mamoru service layer and applications. We make it easy for end users, manufacturers and resellers to make sense of the audit trail and identity possessed by a physical entity in the real world.

References

Gartner on the Identity of Things: http://www.gartner.com/newsroom/id/2985717

Ethereum White Paper: https://github.com/ethereum/wiki/wiki/White-Paper

IBM ADEPT: http://www-935.ibm.com/services/multimedia/GBE03662USEN.pdf