tomorrow's transactions

Home > Thought Leaders > Blog > **Putting "identity" on the "blockchain". Part 1: Find a problem**

Filed Under: Identity, Shared Ledger

Putting "identity" on the "blockchain". Part 1: Find a problem

6th June 2016 by Dave Birch

I have to give a presentation about putting identity on the blockchain, even though no-one seems entirely clear what "identity" means or, for that matter, what "blockchain" means. So I thought I'd try and experiment in thinking out loud this week, using your feedback to try and finish the week with some consistent model of a solution that will solve a known and understood problem. A tall order. But there's lots of work being done in this area and I've been reading some very interesting papers and posts. I think it's a worthwhile experiment in the week of the Cloud Identity Summit and I'm hoping that colleagues and friends in New Orleans will be coming up with some new ideas in this area too.

OK.

There has been a lot of discussion recently about the idea of using the blockchain to "do something" about identity, so I thought I'd put together a few blog posts with some of our thoughts on the topic, gathered from a few of the different projects that we are involved with. Lots of people seem to think that putting identity on the blockchain is a good thing to. But, as many other people have pointed out, in order to come up with some kind of idea as to what exactly the blockchain is going to do is first necessary to come up with some idea about what the identity problem is and then come up with some more specific ideas about how exactly a blockchain (or, more generally, any other form of shared ledger) might solve them.

The idea for this blog post began when my colleagues were putting together some ideas to present at the Open Identity eXchange (OIX) meeting in London few weeks ago. I thought it might be useful to contribute some of our thoughts around that presentation, in their incomplete form, to structure further discussion around this topic. First, the identity problem. Actually there are lots of different identity problems so I thought I'd choose a specific one I've been working with recently. As the chair of the techUK payments group (techUK is the trade association for the British technology industry), I've been taking part in the Financial Services Passport Working Group that started discussing the issue a couple of years ago. This is a good example of a very specific identity problem and a community that is looking for solution.

Let me illustrate what the problem is with a personal example. I've been a customer of Barclays since 1977 and they know absolutely everything about me and my financial history. My salary has always been paid into the same Barclays current account. My mortgage is currently with Barclays and were I to have any savings they would probably be with Barclays to, since I'm extremely lazy. Now suppose I go to open account with the NatWest. The fact that I've had an account with Barclays the 40 odd years will count for absolutely nothing and they will treat me as if I'd just arrived as a refugee. I have to produce some form of identity documentation (which they might well be incapable of verifying: I have literally no idea how the counter staff at NatWest go about checking whether a Romanian passport is real or not) as well have some proof of address, which normally comes down to that well-known high security fundamentally British identification document, a gas bill.

Now suppose I go to get some pensions advice from a financial adviser or look into changing my mortgage to get a better deal or decide to open one of those ridiculous Individual Savings Accounts (ISAs) that the Chancellor of the Exchequer has created so that rich people can salt away tax-free money for their children and thus drive up house prices even further to no general economic benefit to the nation. In any of these cases I would be faced with the necessity to provide my financial identity all over again. So what can be done about this? It's hardly a new problem.

> "An adviser to a new charitable incorporated organisation that spent more than a year trying to open a bank account has blasted Barclays for its onerous demands and disproportionate due diligence."
>
> Barclays slated after CIO takes a year to open a bank account

Thought Leaders

We help our clients bridge the gap betwe
business and technology by providing
practical, impartial advice at all stages in
project life cycle from the conceptual pha
through to completion. We help
organisations evaluate, prototype and
design new business concepts, develop
new products and services and test and
certify complex systems using advanced
techniques and fully-automated robotic t
management.

SEARCH THE BLOG

Search for:

SHARE

Facebook

Tweet

LinkedIn

Pinterest

RSS FEEDS

Posts

Comments

POST CATEGORIES

- Banking and Finance (171)
- Blooks & Media (6)
- Cash and cash replacement (163)
- Chyp events and notices (100)
- Crime & Fraud (121)
- Cryptocurrency (6)
- Finance and Banking (48)
- History and future (55)
- Identification and Authentication (243)
- Identity (45)
- Inclusion (8)
- Markets (8)
- Markets (445)
- Mobile money (14)
- Mobile Payments (5)
- Money (69)
- Money (425)
- Payment Cards (3)
- Payment systems (208)
- Payments (76)
- People (426)
- Podcasts (1)
- Political, legal and regulatory (68)

Well suppose when you open your first bank account and the bank goes through all of its complex know your customer (KYC), anti-money-laundering (AML), counter-terrorist financing (CTF), politically exposed person (PEP) checking and credit referencing and then decides to give you an account. Suppose at that point the bank gave you some kind of financial passport (put to one side what this actually is or what data it contains or where that data might be stored) that you could use to open accounts at the NatWest, change mortgages, open a savings account or obtain financial advice simply by proving that it is **your** financial passport. Then it becomes a simple problem of authentication and we have a variety of strong authentication mechanisms available to us (even without some proper National Entitlement Infrastructure as I have long called for). The cost savings to the industry from not having to continually repeat identification procedures would be substantial and the convenience afforded to the consumer notable.

So why doesn't this happen? Well, that's a good question. We started to look at it a generation ago and the assumption was, at that time, that we would use public key infrastructure (PKI) to solve the problem. I know, I know, people have been going on about this sort of thing for years (here, for example). So, I open a bank account and the bank generates a key pair. The private key is kept in tamper-resistant hardware (at the bank, so that I can't lose it) and the public key is used to form a variety of public key certificates (PKCs) or what I prefer to call "virtual identities". Each of these identities contains a number of different attributes that are attested to by whoever signed the certificate.

Now I wander into the NatWest and present my Barclays virtual identity, perhaps by using my mobile phone or smart card, and all NatWest have to do is to validate that I am rightful owner of the private key associated with the public key in the certificate. They can do this in a variety of ways, but let's say for sake of argument they send a message to my phone that is encrypted using the public key in my Barclays virtual identity and my Barclays app on the phone demands strong authentication and gets it and reports back. NatWest would also have to check that the public key certificate I'm presenting to them hasn't been revoked so this means they have to query the Barclays Certificate Revocation List (CRL) in some way either as part of the challenge to the app or in a separate step.

Problem solved.

Or a least it might have been, had anybody ever implemented any of this stuff. Identrust gave it a go in the corporate space, defining a complete set of standards and more importantly the business rules that go around them, but nothing ever happened in the customer space. I did think for a while that, because the cryptography used to support chip and PIN is the same as the cryptography needed to support this kind of PKI, it would be efficient to add something along the lines of the financial passport to the debit cards in widespread use. I have a vague memory of being involved in some discussions around this with one of the UK banks a decade or so ago and as I recall (and my memory may well be imperfect) the reason for not doing it was that debit card production was outsourced to one particular supplier and they had no interest in raising the cost of the cards issued by a couple of pence in order to save the bank a ton of money in the branches or to combat fraud. I shouldn't think things have changed much by now. And persons of a suspicious nature may well want to believe that banks don't want to make identification easy and portable because they see it as a way of locking in customers, but I am sure that they would not engage in this kind of behaviour.

So if we're not going to implement the financial services passport that way then how can we implement it? In the techUK working group that's been looking at this we were really focusing on a couple of obvious architectures that all simplify down to the centralised architecture and the federated architecture. In the centralised architecture, the banks will all chip in to build a central database somewhere, perhaps run by BACS or some other industry body, and that would hold the details of the identity, the identity verification processes that had been completed and the relevant keys and certificates. So I go into NatWest to open accounts and I authenticate myself to the financial services passport database and Bob's your uncle. This would have course require some coordination between banks and everybody else, and it would have to be pretty reliable otherwise it would turn into a honeypot for criminals and fraudsters, but it's a plausible hypothesis.

Another way of doing it would be a federated solution where each bank holds its own database of the financial passports that it has issued and other banks can query that database using the normal protocols of federation in order to gain access to the data under controlled circumstances. I used to think that this would be the best of way of moving forward, decoupling the banks in this way, despite what it meant in terms of having to sort out liability agreements. I remember a survey for VocaLink a couple of years ago in which some two-thirds of respondents said that they saw value in the establishment of that centralised KYC utility, and I was sure they were wrong. There's no need for a central KYC utility, I thought, when we could have a federated identity linked to verified attributes infrastructure (i.e., a reputation infrastructure).

There would be no need for NatWest to actually store my Barclays financial services passport, they would just need to store a pointer to with the records showing that they had checked. Then if I subsequently get arrested for fraud or Barclays closes my account

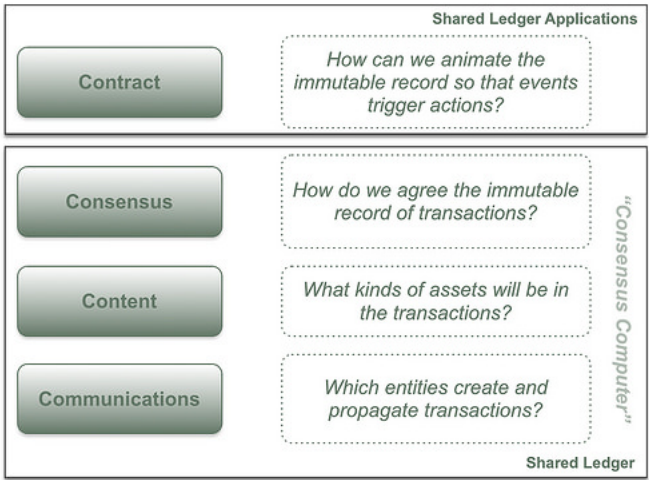
Privacy and security (100)
Public Sector and NGO (35)
Public Sector and NGOs (9)
Retail (130)
Retail and Transit (25)
Shared Ledger (9)
Skills (3)
Social Media and Organisations (21)
Telecoms and Media (172)
Telecoms and Technology (12)
Ticketing (14)
Transit and Travel (53)
Uncategorized (322)

because I turn out to be associated with money-laundering, we need some mechanism for informing all the other people who are depending on that passport that it is no longer but I’m sure it’s not beyond the wit of humanity to come up with some sort of semantic federation that could take care of this.

In recent times, however, a new possibility has wandered into the discussion. Yes, the blockchain. Well, a blockchain. Or to be more precise, some form of Shared Ledger Technology (SLT).

What if we could use shared ledger technology to build this record of financial services passports but but in such a way that no institution owned it, that it had no central system to go down, that it could resist intrusion or attempts at fraud from compromised members of the network, and that it could provide a platform for new products and services that we can’t really imagine at the moment? Personally, I think the shared ledger may well a plausible solution to this problem and having chaired a discussion on identity and personal security as well as a superb panel on identity at Consenus 2016 in New York I’ve been thinking harder about what shared ledger technology could do for organisations in this field. If we take our layer-based model (the “consensus computer” and the applications that we are going to run on it) and begin to think what kinds of identity-related content might be useful, I think we can get somewhere.

Let’s start building the models that we need to think this stuff through clearly. I think we should start with our model of the Shared Ledger that we are going to use to store “identity”. I think Consult Hyperion’s “4x4” model works very well, so we’ll use that.



How can we animate the immutable record so that events trigger actions?

How do we agree the immutable record of transactions?

What kinds of assets will be in the transactions?

Which entities create and propagate transactions?

So in this emerging paradigm, our thought processes then drift on toward the content of this ledger. I saw some interesting demos at Consensus. Deloitte and others had started to build blockchains with defined content assets and these were interesting. But let’s say for sake of argument that a ledger is a record of transactions. The ledger isn’t simply a write-only file containing copies of driving licences and passports and whatever else, it’s a record of transactions that link entities identified at the communications layer with a variety of identity attributes through transactions, developing a reputation associated with that identity. This, I think, is the kind of architecture that Cambridge Blockchain explained to me when I bumped in them last year and it seems a reasonable starting point, congruent with our ideas about the kinds of transactions that might be entered into a shared ledger.

> “
>
> Thus, a blockchain can act as a provenance protocol for data across disparate semi-trusting organizations.
>
> From Will Provenance Be the Blockchain’s Break Out Use Case in 2016? – CoinDesk

We have to be careful with what we are putting in the Content layer, naturally. We don’t want to turn the shared ledger into a resource for despots and confidence tricksters. Hence it is reasonable to ask whether anyone should be able to look at my financial services passport or whether it should be encrypted in some way so that only “authorised” entities can decrypt it. My first thought is that we may want to go for something like this, which is why I prefer to call the Content Layer of our model translucent rather than transparent.

> “
>
> A distributed and irreversible system for trust management, which stores personal data, could offer a hotbed for doxing and identity theft – and even undermine an individual’s right to be forgotten.
>
> From What Airbnb’s blockchain proposal means for privacy

Indeed it could, which is why it should not store personal data in the clear. So, to end this problem statement of our thought experiment, let’s recap: what we will be storing in the shared ledger is not identity itself but some kind of identity transaction and when you come and present your financial services passport to a bank, you will do it by proving that you have control of the private key that corresponds with the public key that is linked to the relevant identity transactions (e.g., Barclays KYCd Dave Birch).

Reasonable starting point? Your thoughts?

0 thoughts on “Putting “identity” on the “blockchain”. Part 1: Find a problem”

Pingback: Putting “identity” on the “blockchain”. Part 2: Create an identity model | Consult Hyperion

Pingback: Putting “identity” on the “blockchain”. Part 3: Define the transactions | Consult Hyperion

Pingback: Putting “identity” on the “blockchain”. Part 3: Define the transactions | Consult Hyperion | FintechLab

Pingback: Putting “identity” on the “blockchain”. Part 4: Create a ledger of transactions | Consult Hyperion

Pingback: Putting “identity” on the “blockchain”. Part 4: Create a ledger of transactions | Consult Hyperion | FintechLab

Tags: identity, kyc, shared ledger

← Card market reform means non-card opportunities
Putting “identity” on the “blockchain”. Part 2: Create an identity model →