Peer Attestation of Identity in the Real World

Submitted by Dr Shaun Conway & Lohan Spies

Context

In most of the developing world people tend to have poor documentary evidence to prove their identity and to access their entitlements.

Regulations might allow for identity credentials to be attested by a trusted third-party such as a solicitor, priest or village chieftain. But these attestations are typically low-fidelity paperware affidavits, with wet signatures. They are easy to fake and have limited utility or credibility - particularly as the basis for proving identity in digital applications.

This has led us to research potential methods to digitise and democratise peer attestations so that any individual can have their identity assertions validated and enriched.

> A practical use-case example comes from our work in South Africa where we are implementing a proof of concept digital identity registration application for children, using the blockchain.
>
> This will enable eligible children to receive a small daily subsidy for attending pre-school classes. The current government subsidy scheme is paper-based, costly to administer, plagued by fraud and excludes children who cannot prove their identity or entitlements. It yields very little useful information about service-delivery or development outcomes.
>
> A successful ‘KYC for Kids’ solution should hopefully establish greater trust, truth and transparency in how social benefits are administered to identified beneficiaries, together with proof of service delivery and valuable meta-data. This could also start generating more effective ways for children to access other services and future social and economic opportunities, through real digital inclusion.

Our paper briefly presents a few of the technical problems we have encountered in designing a peer attestation mechanism for this context, with some initial ideas for possible technical solutions that we hope will stimulate further discussion.

The Proof Problem

Digital identity attributes must provide credible proof that a person is who they claim to be, as well as evidence of other related facts, for instance about where they live and what benefits they are entitled to receive.

Credible oracles of truth must be found who will attest to these facts. Using authenticated digital signatures, attestations can be encoded as software proofs.

Through this method, knowledge-based claims, such as “I know that the person who looks like this photo is Akash” can be used to verify identity attributes and turn these into proven credentials. Artifactual claims can also be attested, such as: “this identity photo is a true representation of Akash and has not been tampered with”.

Some proofs can be executed by computational oracles (for instance, using biometric matching algorithms), which is an area of rapid technological progress. But for practical purposes, most identity attribute attestations require third-parties, such as trust authorities, to go on the record as having verified specific facts, from what they can reasonably be expected to know.

This works when credible trust authorities are available, cooperative, accessible and have the facts on record. In other cases, Peer Attestation could potentially provide an alternative. The Blockstack Peer Attestation Schema provides an example of how such a mechanism could be implemented with software proofs using cryptographic signatures.

However, we feel that this promising method needs to be further developed before it can be formalised as a systematic and reliable operating model for identity proofing.

The Trust Problem

The general limitations of centralised trust authorities have been well described and in developing countries this is further exacerbated by non-existent or poorly-performing trust authorities that are unreliable or not trustworthy because of technology or people failures. Distributed Trust Authority (DTA) models provide a compelling alternative that could reduce dependency on central authorities, eliminate selective exclusion and lower the risks of a single point of failure or fraud.

A DTA must have explicit rules about who gets to participate, how voting takes place, processes to resolve disputes, execution of mandates, the scope of decisions, and so on.
For Peer Attestation to function as a DTA mechanism, participants must implicitly trust their peers and Relying Parties must explicitly trust the mechanism, or they will not use it.
Mechanisms are needed to encode and reliably execute these rules.
Recent developments in computational consensus protocols could potentially offer a technical solution.

For instance, the idea of modified Federated Byzantine Agreement (FBA), as described by David Mazières for the Stellar Consensus Protocol, could possibly be adapted for Peer Attestation. In this model, trust can be enforced by peers reaching consensus through Quorum Slices (conceptually, slices bind the system together in much the same way as the Internet is unified through network peering and transit decisions).
The key innovation in FBA is that each node gets to choose its own quorum slice.

This is an appealing way to address the complexities, limitations and unpredictability of real human peer networks, where participants are unlikely to constantly remain available and willing to provide reliable attestations over time. In this consensus protocol, dynamic groupings of peers would exchange messages to assert signed statements about another person's identity attribute.

Participants could be selected from peers that are expected to know the individual or to know something about them, whilst still offering some freedom to choose which combinations of other participants to trust. For practical purposes, this might include a combination of their personal contacts and the institutions that hold account information about them (selected from their personal data records).
Once a sufficient number of peers has asserted a statement the quorum is considered to have reached consensus and the attribute is considered verified.

Our assumption is that participating peers are less likely to defraud their assertions if they can be fully identified as the owner of the public key they use to digitally sign each message. As with any DTA/consensus mechanism, there are disincentives for any one participant to be dishonest, as this reduces their trust status in the network and could result in them being progressively excluded.

If quorum slices are selected using a relatively unpredictable (random or possibly even opportunistic) consensus algorithm, this could minimise the opportunity for peer collusion within a group of dishonest nodes.

The protocol waits for a threshold number or combination of participants to agree (for instance 51% or more, including one approved Trust Authority), before considering the credential to have been validated. This can be achieved asynchronously over any period of time (at least in theory).

The protocol could be implemented with open membership to promote organic network growth. It benefits from low barriers to entry and has modest computational requirements that could be executed on smartphones.

The Validity Problem

Identity proofing through peer attestation will have to provide itself to be a statistically valid mechanism with an acceptable level of predictive specificity for any given identity attribute to be true and also sensitive enough to exclude false positives.

Whether this is possible can only be empirically determined by measuring how peer attestation systems perform over time when implemented in real-world settings.

For now, Relying Parties could choose their own validity criteria for levels of identity assurance - for instance, an attestation might need to include one recognised institution as a source of peer attestation for a credential to be considered valid.

The idea of flexible distributed trust seems compelling as relying parties have the freedom to trust any combination of parties they see fit. For example, a small non-profit, such as a local Pre-School service, could play a key role in attesting the identity of a child (and the fact that they attend the service).

The Incentive Problem

Peer attestation systems pose queries to the network itself, rather than to a centralised indexes, which means that peers are expected to perform work. To operationalise this so that it reaches a scale of participation that makes the system useful to everyone, people will have to have enough incentives to freely participate.

Designing mobile user interfaces that simplify and gamify attestation as an integral part of user journeys for getting other more important jobs done -- such as when making a financial transaction -- might help. But networks of peers are often heterogeneous and have all types of participants - including friends, professionals and services, so it is unlikely that everyone will be equally incentivised by the intrinsic benefits of participation. We also have to factor in the disincentive of the personal and organisational liability that is inherent to this type of accountable peer attestation mechanism.

A potential solution is to trade digital assets for work done, or in exchange for information being provided. Digital currencies are ideally suited for this as they provide transparent and efficient ways of transacting and accounting and could also be used as proxy measures of reputation and trust.

An incentive mechanisms could be modelled on a Prediction Market encoded in a smart contract that requires all participants to deposit a stake when they make an attestation. Losers of a consensus round have their deposit split between the winning nodes and they are effectively left with fewer trust points. These incentive pay-offs could be configured to encourage participation by different types of peers - including commercial entities.

Safety and Privacy Problems

Peer attestation requires an attesting peer to act in the role of a trust authority, which we believe should not be an arbitrary claim, as this could compromise the safety of the mechanism and open it up to abuses or negligence. We therefore suggest that to qualify as a trusted node, an attesting peer must at least have achieved a high level of identity assurance for accountability — essentially ‘legal identity’ with certified credentials that accredit them to a standard of KYC compliance that would generally be accepted by a bank. This could be further strengthened by a reputation score.

To reach consensus, the initiating node would message all available peers but only those that can demonstrate the credentials to meet the pre-defined criteria for identity assurance and/or reputation would be entitled to make assertions.

If this scheme worked, it could potentially rapidly scale through both social network and data network effects, to create distributed trust networks of individuals who have been identified by their peers. This could be achieved through consensus dynamically emerging from the linkages between network slices.

Quorum slices could be privacy-preserving, as long as software encrypts all personal data attributes and these can only be selectively seen by trusted peers within a given slice that links back to the referenced individual.

The Agency Problem

In a Peer attestation network all peers are not really equal peers. The most obvious example is children relying on attestations by adults - most of whom they will not actually ‘know’ (as trusted others). This introduces the problem of who should have the right to assert information about other people - especially when they are themselves unable to contest this information, or to consent to how this information will get used by third parties.

It might be possible to resolve by having an accountable public record of attestations and by only allowing individuals with certain credentials (that have been attested by trusted others) to perform an agency role. But this raises questions about who should take on the custodian responsibility for making these political decisions.

Regardless of how this plays out, we feel that any agents who provide digital identity registration services for children should have the strong ethical obligation to ensure that these identities are self-sovereign.