Credit-based Reputations for Identity Management with Blockchain and Flow Networks

Whitepaper proposal for the 04/2017 'Rebooting Web of Trust' Design Workshop

11 April 2017

Tobias Mayer, Omar Hasan, Lionel Brunie

Institut National des Sciences Appliquées (INSA) de Lyon, Laboratoire LIRIS

{ tobias.mayer // omar.hasan // lionel.brunie} @insa-lyon.fr

ABSTRACT

A secure management of digital identities is an obvious requirement for digital technologies and applications (digital payment, online shops, insurances, etc.). It is typically achieved by pre-defined certificate-based trust. However, pre-defined trust on centralized instances is not always possible or wanted for trust management and the "web-of-trust" emerged as a decentralized alternative. It determines a trust value by aggregating reputations issued by other entities, where the reputations represent a subjective evaluation of the user satisfaction. This mechanism is also suitable for the identity management when using reputations to indicate (the subjective impression of) an identity's trustworthiness. However, such traditional reputation-based web-of-trust approaches suffer from Sybil attacks, where an identity can increase the own trust value by creating synthetic identities issuing reputations.

We propose a trust management mechanism for the decentralized reputation-based web-of-trust approach, which operates among two avenues. First, issuing reputations imposes spending some credits, which are received through reputations and the total amount being limited in the system. In order to prevent Sybil attacks, circular reputations are not allowed, which is determined by applying flow network concepts to verify reputation validity. Second, identities and reputations are stored in a blockchain where and identity's trust value can be determined by traversing the stored blocks and aggregating related values accordingly. The proposed mechanism is fully decentralized, able to prevent threats such as Sybil attacks or reputation flooding, offers secure and immutable storage characteristics, where any action can be cryptographically verified.

CONTEXT

Identity management with a web-of-trust (WoT) cannot rely on pre-defined trust as provided by certificate authorities in public key infrastructures (PKI). To this end, WoT aggregates reputation values in a distributed manner. However, we cannot draw conclusions among off- and on-line identities such that any trust value is fully determined by activities and reputation values provided on-line. Malicious nodes can exploit this aspect, e.g. by creating additional identities to increase the own trust values through synthetic reputations. Moreover, reputation integrity and accountability need to be ensured. The blockchain theory has recently revolutionized the concept of electronic cash by eliminating the requirement of trusted third parties and by providing true decentralization. Its secure immutable distributed data storage is therefore crucial for reliable reputation-based trust management.

We consider therefore the problems (1) that the pure aggregation of reputations is not sufficient and we require mechanisms to prevent reputation misuse or colluding parties; and (2) that a blockchain model shall be able to support and maintain trust & reputation information.

PROPOSED APPROACH

We propose a new identity management approach based on reputation and flow networks. Reputations are provided by spending some credits where the total amount of credits is limited in the system. This prevents misuse such as Sybil attacks through the imposed value and credit limitations. The economic mechanics serve thus as trust generator in addition to the absence of centralized pre-defined trust.

We consider a system, where identities are represented by self-contained data (public key, unique id, etc.) and are able to provide reputations to other identities. A reputation is considered as a positive feedback for the receiving identity. The amount of received reputations represent the amount of available credits to spend and reputations can be provided as long as the issuing identity has sufficient credits. However, we require that circular reputations are not possible to prevent misuse (i.e. identity B cannot provide a reputation to identity A if B has received on by A beforehand).

We leverage flow networks to determined circular dependencies and total credits available per identity as illustrated in Figure 1. Blockchain will be used to store provided reputations. Trust management aspects are integrated into the blockchain architectural design and the consensus algorithm (see section implementation possibilities).

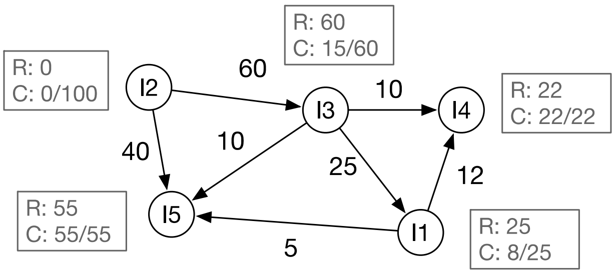


Figure 1: The reputation (R) of each identity is determined by the amount of incoming reputation values that serve as credits (C) for issuing reputations. Here with a limit of 100 credits in the system and I2 being the first node in the system and thus initially owning some credits.

OPEN QUESTIONS

- **What is an identity?** A self-contained identity profile is an intuitive approach. However, a distributed approach may be beneficial where a “core identity” (name, address, etc.) is extended by distributed domain- or application-specific identity information.
- **How to ensure privacy-preserving trust management?** WoT reveals relationships between nodes and flow networks reveal the amount of trust/credit that a user A assigns to user B. Therefore, reputations shall not be linkable to an identity and it shall not be possible to determine the amount of available credits for other identities. Several mechanisms have been proposed that enable operations over encrypted data (e.g. fully/partial homomorphic encryption or multi-party computation).
- **How to ensure traceability of user actions?** Any action must be securely traceable in a time-ordered manner to enable accountability (e.g. to detect and handle misbehaviours), verifiability, accounting of identity management features etc.
- **What are limits & characteristics of the credit based trust management?** The proposed mechanisms may have unknown limits & characteristics. For example, the subjective value of reputations may differ through availability of credits or the limitation/value of credits lead to users to save their credits. This should be further assessed by an evaluation study.
- **How to ensure verifiability?** The correctness of reputation and available credits must be verifiable, particularly when operation on encrypted data. This requires a sound definition of verifiability, while a realization may integrate existing mechanisms (e.g. zero-knowledge proofs).

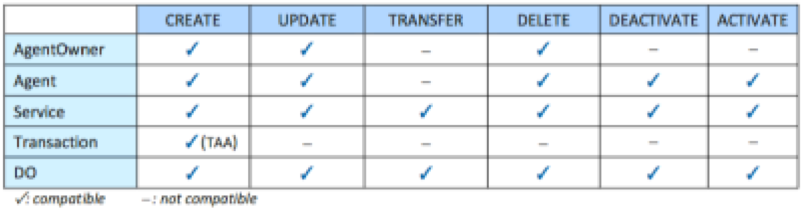
- **How to securely store and maintain trust management data?** We need to specify the identity and reputation data models and an architectural integration concept that allows additional logic (trust value calculation, flow network operations etc.). An example is a stack oriented approach with each layer encapsulating distinct features.

- **How to make the identities & reputations usable in applications & business logic?** The identities and reputation values shall accessible by third party platforms and applications such as accessing an insurance profile or negotiating deals in e-commerce. What are therefore the requirements for technical interoperability enabling the access of identity & trust data, traceability of interactions and respect of privacy. Other requirements may be discovered by further discussions.

IMPLEMENTATION WITH THE DATACOPP PLATFORM

"DataCOPP" is an incubating project developed by T. Mayer at the INSA de Lyon with the aim to develop a high-performance hybrid blockchain as distributed platform for privacy-preserving data processing. Some of its architectural design concepts can be beneficial for the realization of credit-based reputation approach as outlined in the following:

- **High extendibility through a layered architecture with nested payloads**. Architectural layers enclose distinct functionalities with each layer's data being stored as payload in the underlying layer. Trust management can be achieved as one or multiple additional layers (e.g. flow network, trust model).
- **Hybrid blockchain for high adaptability, scalability & performance**. The blockchain federation consensus consists of a voting on block validity enabling high throughput performance and flexibility regarding parameters. An underlying database (Apache Cassandra in case of DataCOPP) enables linear scalability and adjustable data replication. This enables scalable performance & data storage suitable for the integration of application related data into the blockchain storage system.
- **Blockchain asset management for trust management operations**. The DataCOPP asset management offers multiple asset management operations as shown and maintains identities to some degree (for example, Bitcoin offers CREATE and TRANSFER). This concept can be adapted to support reputation management of (e.g. maintenance of credits).



	CREATE	UPDATE	TRANSFER	DELETE	DEACTIVATE	ACTIVATE
AgentOwner	✓	✓	–	✓	–	–
Agent	✓	✓	–	✓	✓	✓
Service	✓	✓	✓	✓	✓	✓
Transaction	✓ (TAA)	–	–	–	–	–
DO	✓	✓	✓	✓	✓	✓

✓: compatible –: not compatible

Figure 2: DataCOPP asset management operations for the entities of a traceability layer.

- **Trust management integration into "deep validation" routines**. During the storage process, the deep validation logic performs block validation checks of invalidity conditions on all architectural layers. This may be extended by trust management conditions to prevent storage of illegal reputations (e.g. no storage of circular reputations, spending to many credits than available).
- **Privacy-preserving multi-party computation**. A Master thesis aims in integrating privacy-preserving computation features into the DataCOPP platform by relying on the Shamir's Shared Secret scheme (using the SEPIA library[1]). It will store an arbitrary data set, e.g. an identity profile, in an encrypted and distributed way over participating nodes and enable operations over the encrypted data (e.g. average, sum). The Master student has started in March 2017 and will provide a proof-of-concept by September 2017. This proof-of-concept may be extended by reputation & trust features.

[1] http://sepia.ee.ethz.ch