- 1. Abstract Introduction We propose a decentralized reputation system that can replace the word-of-mouth, stars- and review-based systems. The basic idea is that a member A trusts her friends with a certain value (with a 1/2 multisig), thus risking to lose their value. When A wants to transfer value V to a (maybe previously unknown) member B, A asks the system if she trusts B enough to transfer this value to B. The system will search throughout the network for trust paths that begin from A and reach B and add up to V and will answer whether the proposed transaction is within the trust capabilities of A towards B. If the answer is positive, it means that transferring value V to B will not raise the risk for A to lose their value. Note: we use Bitcoin terminology.
- 2. Related Work
- 3. Key points

Definitions

- Direct trust from A to B, $DTr_{A\to B}$ Total amount of value that exists in 1/{A,B} multisigs in the utxo, where the money is deposited by A
- B steals x from A B steals value x from A when B reduces the $DTr_{A\to B}$ by x. This makes sense when $x \leq DTr_{A\to B}$.
- Honest (passive) strategy
 A member A is said to follow the honest (passive) strategy if for any value x that is stolen from her, she substitutes it by stealing from others that trust her:

$$\begin{cases} x \text{ if } \sum_{B \in members} DTr_{B \to A} \ge x \\ \sum_{B \in members} DTr_{B \to A} \text{ if } \sum_{B \in members} DTr_{B \to A} < x \end{cases}$$

or simply $min(x, \sum_{B \in members} DTr_{B \to A})$.

• Indirect trust from A to B $Tr_{A \to B}$ Value that A will lose if B steals the maximum amount she can steal (all her incoming trust) and everyone else follows the honest (passive) strategy.

Theorems

- $Tr_{A\to B} = MaxFlow_{A\to B}$ (Treating trusts as capacities)
 - (a) $Tr_{A \to B} \geq MaxFlow_{A \to B}$ because by the definition of $Tr_{A \to B}$, B leaves taking with him all the incoming trust, so there is no trust flowing towards him after leaving. $Tr_{A \to B} < MaxFlow_{A \to B}$ would imply that after B left, there would still remain trust flowing from A to B.
 - (b) $Tr_{A \to B} \leq MaxFlow_{A \to B}$ Suppose that $Tr_{A \to B} > MaxFlow_{A \to B}$ (1). Then, using the min cut - max flow theorem we see that there is a set of capacities $C = \{c_1, ..., c_n\}$ with flows $X = \{x_1, ..., x_n\}$ such that $\sum_{i=1}^n x_i = MaxFlow_{A \to B}$ and, if severed $(c_i' = 0 \ \forall i \in \{1, ..., n\})$ the flow from A to B would be 0, or, put differently, there would be no directed trust path from A to B. No strategy followed by B could reduce the value of A, so our supposition (1) cannot be true.

Combining the two results, we see that $Tr_{A\to B} = MaxFlow_{A\to B}$.

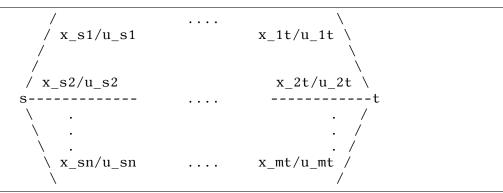
• Trust transfer theorem (flow terminology) Let s source, t sink, $X_s = \{x_{s \to 1},...,x_{s \to n}\}$ outgoing flows from s, $X_t = \{x_{1 \to t},...,x_{m \to t}\}$ incoming flows to t,

 $U_s = \{u_{s \to 1}, ..., u_{s \to n}\}$ outgoing capacities from s, $U_t = \{u_{1 \to t}, ..., u_{m \to t}\}$ incoming capacities to t,

V the value to be transferred.

Nodes apart from s, t cannot create or consume flow.

Obviously $maxFlow = F = \sum_{i=1}^{n} x_{t \to i}$.



We create a new graph where

(a)
$$\sum_i u'_{s \to i} = F - V$$

(b)
$$u'_{s \to i} \le x_{s \to i}$$

We will now prove that maxFlow' = F' = F - V.

(a) It is impossible to have
$$F' > F - V$$
 because $F' \le \sum u'_{s \to i} = F - V$.

(b) It is impossible to have F' < F - V.

Let i be a node such that $x_{s \to i} > 0$ and $I = \{(i,j) \in E\}$ the set of direct trusts outgoing from i. In the initial graph we have $x_{s \to i} = \sum_j x_{i \to j}, F = \sum_i x_{s \to i}$ and in the new graph we have $x'_{s \to i} = u'_{s \to i} \leq x_{s \to i}, F' = \sum_i x'_{s \to i}, x_{i \to j} \leq u_{i \to j} = u'_{i \to j} \forall j, i$. We can construct a set $X'_i = \{x'_{i \to j}\}$ of flows such that $x'_{i \to j} \leq x_{i \to j}$ and $\sum_j x'_{i \to j} = x'_{s \to i}$. This shows that there is a possible flow such that F' = F - V, so the maxFlow algorithm will not return a flow less than F - V.

Example construction:

$$x'_{i o j} = x_{i o j} \forall j \in \{1,...,k\}$$
 with k such that

i.
$$\sum_{j=1}^k x_{i\to j} \le x'_{s\to i}$$
 and

ii.
$$\sum_{j=1}^{k+1} x_{i \to j} > x'_{s \to i}$$

$$x'_{i\to(k+1)} = x'_{s\to i} - \sum_{j=1}^{k} x'_{i\to j} x'_{i\to j} = 0 \forall j \in \{k+2, ..., |X'_i|\}$$

- 4. Further Research
- 5. References
- 6. Tags/Keywords decentralized, trust, reputation, web-of-trust, bitcoin, multisig, line-of-credit, trust-as-risk, flow