Blockchain based Decentralized Reputation Model and General Trust Framework

Student: Sujata Tamang
Supervisor: Jonatan H. Bergquist
Reviewer: Björn Victor
Department of Information Technology, Uppsala University

Background

Online identities are an essential element in the process of digital interaction and requires unknown entities to trust each other based on reputation system of the platform in use. Let us take a simple scenario to present the context. Alice wants to buy a pair of headphones. To achieve this, she browses the webshop, Dbay which is a buy/sell platform. She then finds a relevant ad placed by Bob who has good reviews. Alice picks up her credit card, submits required details and waits for her desired product to be delivered as promised. In this interaction, trustworthiness of Bob is fully reliant on Dbay. The entity claiming to be Bob could be Eve who found a way to bypass Dbay's security and inflate his reputation on the system. Eve could delete the ad and associated account when the payment is complete or she could gather Alice's personal details to misuse it later. Any malformed decision on trustworthiness of an entity could be expensive and deal severe damage to the user. A centrally governed system is more prone to directed attacks. One successful attack on Dbay can leave all its users vulnerable. Thus, a central point of authority is the single point of failure.

On the other hand information distributed over decentralized network would require simultaneous attacks on numerous accounts to achieve the same effect. Added layer of cryptographic security on this network would hugely raise the difficulty level of attack. In 2008, a solution was proposed as Bitcoin, a peer-to-peer electronic cash system [5] that eliminated the need for trusted central authority. The underlying technology, namely blockchain is a public ledger that allows anyone on the network to audit blockchains state changes and prove with mathematical certainity that transactions were made according to the specified blockchain rule. [4] It comes with a computationally expensive proof of work for nodes to maintain and update the blockchain database. Thus, blockchain ensures fault tolerance, zero downtime, tamper-resistant data. Leveraging this technology for implementing reputation system could be an ideal solution. The use of right reputation algorithm integrated with Blockchain can ensure trustworthiness of online identities with high degree of certainity.

Task

The goal of this thesis is to use blockchain technology and smart contracts to model a reputation system with graph theory and relevant reputation algorithms in use. It aims to have a trust framework that can assist decision making to either carry out the transaction or not. A reference network will be created where nodes and their relationships will be studied to identify honest or malicious participants. The method to calculate reputation score and infer trust value of associated identity will be discussed and applied. Generalization of this reference network to other transactional network to serve various other use cases will also be discussed.

Research questions that this project aims to address are :

1. *Reputation Model:* How can graph properties and similar algorithms be used to formulate reputation model such that malicious nodes are detected and trust transitivity is preserved for infering the trust value for each nodes in the network? Definition of the endorsement network, edges, direction, weight, vertices.

2. *Blockchain:* What are the requirements for storing trust values and linking them to associated identities stored off blockchain network? How will the blockchain architecture look like for endorsing known and unknown entities to serve decision making process before two parties

engage in any transaction? How can blockchain application be built to define a general trust framework for a transactional network? What should the overall system architecture look like?

3. *UseCases:* How can the discussed endorsement network ensure trustworthiness while also preserving users anonymity and how can it be generalized to other transactional network or added on top of it to serve other usecases such as content filtering, E-Commerce etc?

Main goal of the thesis project: The Main goal is to prove that discussed trust framework works to evaluate trustworthiness of participating entities via Proof of Concept.

Objective to support the main goal:

- *Definition:* Identify relevant concepts, Current reputation models, EigenTrust, Network flow convergence Algorithm.
- *Analysis:* Evolution of blockchains, types, consensus algorithms, other relevant blockchain concepts.
- *Requirement Analysis:* Pre-requisite for test setup, User stories, Determine user types, functions, functional and non functional requirement for the system, identities, storage.
- *Solution Design:* Formulate reputation as network flow problem, use graph properties, EigenTrust.
- *Implementation:* Write smartcontracts, deploy on ethereum test network.
- *Result:* Measure, analyze, evaluate reputation scores and trust accuracy.
- *Documentation:* Write Report throughout the project timeline.

Method

Solidity, [7] contract oriented programming language will be used for writing contracts that define transactions and their exchange methods on the peer-to-peer network of Ethereum. [6] Test and deployment will be performed on Ethereum test network. Cloud services(e.g.docker) may be used to test the validator nodes that follows discussed consensus. For frontend to communicate with the contracts, web3.js can be used. Git will be used as version control for the codes.

Relevant Literature

Some existing works carried out in relation to decentralized reputation based on graph theories and various trust metrics are provided in References section as: [1] [2] [3]

Relevant Courses

The relevant courses that the student has undertaken at Uppsala University, are listed below. They are ordered based on their relevance to the project.

1. Cryptology, 5c
2. Secure Computer Systems, 5c
3. Applied Cloud Computing, 10c
4. Advanced Software Design, 5c
5. Programming Theory, 10c
6. Algorithms and Data Structures II, 5c

Delimitations

Given the time constraints, implementation will be limited to PoC for endorsement network. Discussion on several usecases will be presented but will not be experimented or tested with. Results will attempt to show accuracy, failure probability but they will not be experimentally compared to the existing systems for lack of time to search for appropriate datasets. If time permits, frontend may be developed such that contracts can be interacted with from the web interface directly.

Time Schedule

Week	**Description**
5 - 6	Identify Relevant concepts: EigenTrust, Flow convergence
7 - 8	Evolution of blockchains, consensus algorithms
9 - 10	Model Network flow using graph properties
11 - 13	Setup test network, Write smartcontract code.
12	Midterm meeting
14 - 16	Results: Measure, Analyze
17 - 18	Write analysis of results
19 - 20	Write conclusion, futurework, complete final draft for feedback
21 - 22	Prepare presentation, refactor code and documentation for prototype
23	Backup time
24	Update with feedback, finalize paper, and present orally

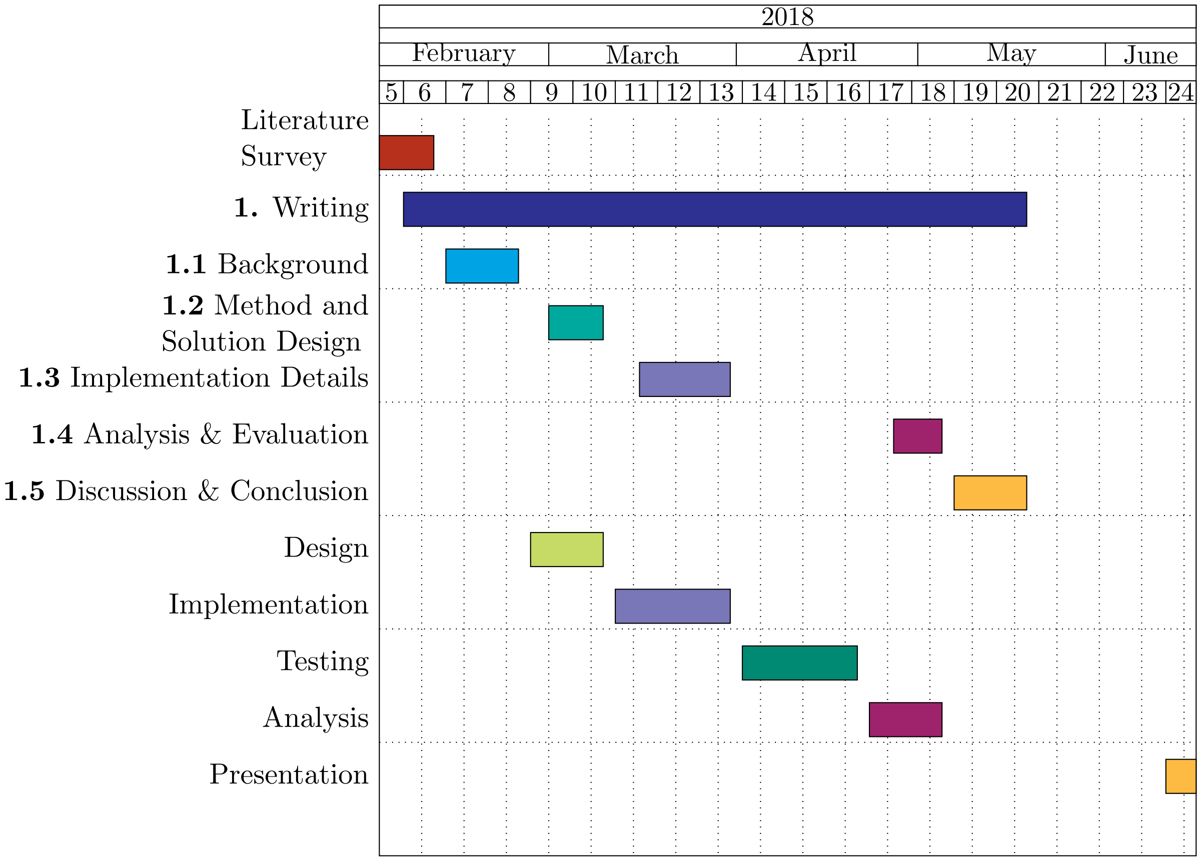

Figure 1: Time Plan

References

[1] Matthew B. Buechler, Manosai Eerabathini, Christopher Hockenbrocht, and D. Wan. Decentralized reputation system for transaction networks. 2015.

[2] Dimitra Gkorou. Exploiting graph properties for decentralized reputation systems. 2014.

[3] Sepandar D. Kamvar, Mario T. Schlosser, and Hector Garcia-Molina. The eigentrust algorithm for reputation management in p2p networks. Working Paper 2002-56, Stanford InfoLab, 2002.

[4] Goldin Mike. Just enough bitcoin for ethereum. Consensys, Oct 12, 2015. Accessed 23 Dec 2017, [Online]. Available: `https://media.consensys.net/time-sure-does-fly-ed4518792679`.

[5] Nakamoto Satoshi. Bitcoin: A peer-to-peer electronic cash system. Bitcoin, Oct 31, 2008. Accessed 23 Dec 2017, [Online]. Available: `https://bitcoin.org/bitcoin.pdf`.

[6] Open Source. Ethereum whitepaper. Accessed 23 Dec 2017, [Online]. Available: `https://github.com/ethereum/wiki/wiki/White-Paper`.

[7] Read the docs. Solidity. Ethereum whitepaper. Accessed 15 Jan 2018, [Online]. Available: `https://solidity.readthedocs.io/en/develop/`.