Blockchain based Decentralized Reputation Model and General Trust Framework

Student: Sujata Tamang
Supervisor: Jonatan 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 the reputation system of platform in use. The reputation systems that are widely used in today's online systems are application specific and each service provider has their own rating system whereby users can leave rating/feedback for a good or bad experience encountered. These models have various limitations and fail to provide a precise accuracy range of user's trustworthiness. [4] Any malformed decision on the trustworthiness of an entity could be expensive and deal severe damage to the user. A centrally governed system is more prone to directed attacks as it has a single point of failure.

On the other hand, information distributed over a decentralized network would require simultaneous attacks on numerous accounts to achieve the same effect. In 2008, a solution was proposed called Bitcoin, a peer-to-peer electronic cash system [8] 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 certainty that transactions were made according to the specified blockchain rule. [6] Different blockchain comes with various consensus algorithms based on the application and use cases to maintain and update the blockchain database. Blockchain ensures fault tolerance, zero downtime, and tamper resistant data to be stored on its network. 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 a high degree of certainty.

Previous work that has been done in context of reputation management for online systems can be seen in [1][3] [12]. EigenTrust [5] is a reputation managemen algorithm that is based on the notion of transitive trust(i.e. If a peer i trusts a peer j then it implies that i trusts all other peers trusted by j) and can be used on P2P network. Bayesian network based trust model has been studied by [11] to build reputation based on recommendations in P2P networks. Similarly, TrustDavis [2] presents an interesting method for non-exploitable online reputation system by defining important characteristics of honest and malicious participants and provides an incentive for accurate ratings of trust.

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 transaction or not. An endorsement network will be simulated where participants can endorse each other based on physical or digital acquaintance. The 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 endorsement network to other transactional networks to serve various other use cases will also be discussed.

Research questions that this project aims to address are :

1. *Reputation Model:* Definition of nodes, edges, direction, weight, vertices in the endorsement network. How can graph theories and relevant reputation algorithms be used to model the interaction between entities and detect/identify honest or malicious nodes?

2. *Blockchain:* What are the requirements for storing trust values and linking them to associated identities stored off a blockchain network? How can a blockchain application be built to define a general trust framework for a transactional network? How could the overall system architecture look like?

3. *Use Cases:* 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 use cases such as content filtering, E-Commerce etc?

Main goal of the thesis project: The main goal is to design a PoC to simulate an endorsement network that can compute reputation score and identify trustworthiness of interacting entities using smart contract based decentralized reputation model.

Method

The methodology for this project will follow an incremental approach that will start with definition of problem supported by literature review and followed by solution design and implementation. The steps can be broken down into:

- *Definition:* Identify relevant concepts, algorithms, current reputation models, evolution of blockchains, consensus algorithms, other relevant blockchain concepts.
- *Analysis:* pre-requisite for test setup, user stories, determine user types, functions, functional and nonfunctional requirements for the system, identities, on chain vs. off-chain storage.
- *Solution Design:* Formulate reputation model using graph properties, methods to quantify reputation score, trust values.
- *Implementation:* Write smart contract code, deploy on the test network.
- *Result:* Measure, analyze, evaluate reputation scores and trust accuracy range.
- *Documentation:* Write report throughout the project timeline.

Solidity, [10] a 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. [9] Test and deployment will be performed on Ethereum test network. Cloud services such as docker may be used to test the validator nodes that follow discussed consensus. Neo4j can be used for graph simulation. node.js can be used as a javascript run time and web3.js API may be used to build a web application that can communicate with the smart contract. Solc will be used to compile solidity code and Git will be used as version control for the codes.

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 a PoC for endorsement network. Discussion on several use cases will be presented but will not be experimented or tested with. Results will attempt to show reputation accuracy and failure probability but 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

The week column in the time table corresponds to the respective week shown in figure 1.

Week	Description
1 - 2	Literature survey: Reputation algorithms, Identify relevant concepts, Refine specification
3 - 4	Background: Evolution of blockchains, Consensus algorithms
5 - 6	Method & Design: Model network using graph properties
7 - 10	Implementation: Setup test network, Write smart contract code.
10	Midterm meeting
11 - 12	Testing: Measure, Analyze, evaluate
13 - 14	Analysis: Write analysis of results
15 - 16	Discussion & Conclusion: Write conclusion, futurework, complete final draft for feedback
17 - 18	Refactor code, documentation, prepare presentation
19	Backup time
20	Presentation: Update with feedback, finalize paper, and present orally

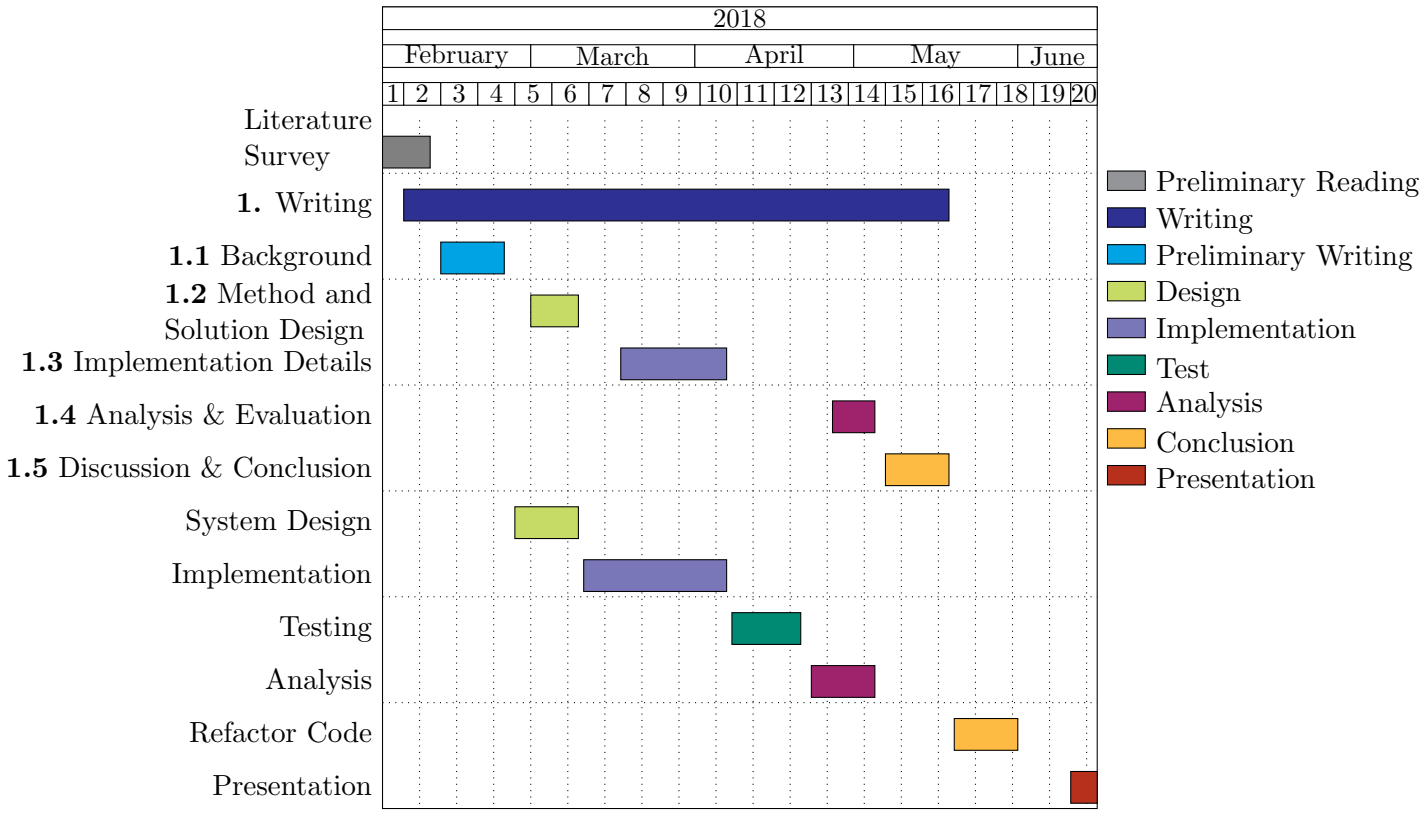

Figure 1: Time Plan

References

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

[2] Dimitri do B. DeFigueiredo and Earl T. Barr. Trustdavis: A non-exploitable online reputation system. TrustDavis. Accessed 11 Feb 2017, [Online]. Available: `http://earlbarr.com/publications/trustdavis.pdf`.

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

[4] Audun Jøsang, Roslan Ismail, and Colin Boyd. A survey of trust and reputation systems for online service provision. *Decis. Support Syst.*, 43(2):618–644, March 2007.

[5] 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.

[6] 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`.

[7] Jordi Sabater and Carles Sierra. Review on computational trust and reputation models. *Artificial Intelligence Review*, 24(1):33–60, Sep 2005.

[8] 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`.

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

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

[11] Y. Wang and J. Vassileva. Trust and reputation model in peer-to-peer networks. In *Proceedings Third International Conference on Peer-to-Peer Computing (P2P2003)*, pages 150–157, Sept 2003.

[12] Bin Yu and Munindar P. Singh. Distributed reputation management for electronic commerce. *Computational Intelligence*, 18(4):535–549, 2002.