Distributed Academic Grading System Using Smart Contracts

Shikhar Mahajan
Supervisor: Prof. Arnab Bhattarcharya

Indian Institute of Technology, Kanpur
Undergraduate Project Presentation

smahajan@iitk.ac.in

November 13, 2017

Overview

Introduction

Introduction

The prominent feature of blockchain development is commonly understood as the decentralization of financial systems. The main reason behind this is the mechanism of incentivising the block miners for preserving the trust and robustness in public blockchains at the cost of their computation power and storage. Private blockchains, on the other hand are not open to public mining estranging the direct monetary influence. This opens up the scope of this technology to all sectors where data mutability is an existing issue.

Blockchain Under the Hood

Existing Technologies:

- Concurrency Control
- Multiversion Concurrency Control
- Distributed Multiversion Concurrency Control

At the core, blockchains offer just another mechanism for the synchronization of distributed databases, but is not limited to it.

Blockchain Under the Hood

- A block is defined as a collection of hashed transactions floated in the network at a particular instant of time.
- The blocks are chained by storing the hash of the previously linked block address in the freshly created one.
- The chain follows the time-stamped manner of recording each modification to the database
- The identity hooked to these transactions follows the concept of asymmetric keys.

At the core, blockchains offer just another mechanism for the synchronization of distributed databases, but is not limited to it.

Non-fiscal disruptions by Blockchains

Industries widely affected:

- Real estate
- Healthcare
- Music Recording Industry
- Voting
- Internet of Things (IoT)

Blockchain-The Solution!?

Characteristics of the Problem

- Distributed database: Any modification to the database entries are only entertained through transactions accepted by mining nodes.
- Multiple writers: As the database is distributed and open for mining, multiple people can write to it at once.
- Mistrust among the writers: The concept of consensus is relevant only when there are multiple writers present with conflicting goals/records.

Characteristics of the Problem

- Interactive transactions: Deleting and creating entries in a collective bilateral fashion accounts to modifying the database linking each transaction that involves a particular entry.
- Disintermediation: This is a fundamental fracture point of many projects aiming to exploit blockchains. It leads to delays in acceptance of transactions and involves the cost of applied computation power and storage of all the verifiers involved.

Characteristics of the Problem

- Permissioned miners: The provision of permissions in blockchains opens up its scope to many fields. This is a primary pointer to the development of private blockchains where an authority in control of the blockchain permits some particular nodes to mine blocks. This margins the protocols adopted by private banks with a public protocol like Bitcoin.

Important Note

Two most important differences between blockchains and centralized databases can be characterized as follows:

- Disintermediation: Blockchains enable multiple parties who do not fully trust each other to safely and directly share a single database without requiring a trusted intermediary.
- Confidentiality: All participants in a blockchain see all of the transactions taking place.

Blockchains represent a trade-off in which disintermediation is gained at the cost of confidentiality.

Potential Use-cases

- Lightweight financial systems: Loyalty points, giftcards, credits
- Provenance tracking: Supply chain multijurisdictional processes
- Multiparty aggregation: Interorganizational record keeping, transaction data, news feed

Smart Contracts in Ethereum

Smart Contracts in Ethereum

- People started embedding metadata in bitcoin transactions to serve purposes like digital assets and document notarization.
- As a result, many next-generation public blockchains were developed such as Nxt, Bitshares, Ripple and Stellar.
- Ethereum, the programmable blockchain has 2 type of accounts: user accounts and contracts.
- A contract is a computer program with an associated miniature database, which can only be modified by the program that owns it.

Smart Contracts in Ethereum

Constituents of a smart contract:

- Expressing business logic as computer programs.
- Representing the events which trigger that logic as messages to the programs.
- Using digital signatures to prove who sent the messages.
- Putting the programs, messages and signatures on a blockchain.
- Executing every program for every message on every node.

Distributed Academic Grading System (DAGS)

Constraints:

- Each course is identified by an unique course ID like CS395.
- The instructor of the course and maximum number of students that can get enrolled in the course is set by the chairperson primarily.
- The instructor is allowed to add students in the course via their public addresses. These public addresses of students are also needed in order to obtain a their past grade sheet.

Constraints:

- A student cannot fake his/her identity to get enrolled in the course twice.
- A grade can only be assigned by the professor and once assigned, cannot be changed by him/her at any later point of time. In case of any discrepancies, the chairperson is the only authority who can alter the grade.

Constraints:

- Each student has the permission to view his/her own grade but not someone elses.
- Everyone in the network can do statistics on the course grading scheme such as percentage of students getting an A grade, failing the course etc.
- Professor is able to justify the grading scheme if questioned later(Off-chain data).

Demonstration

Future Work

- Scale the current distributed model to accommodate many courses instead of one in a single blockchain.
- Modifying the current model such that a student gets an unique ID among all students which is consistent in all courses that he/she gets enrolled in.
- Introduce off-chain data to include hashes of the soft-copies of all the answer scripts.
- Migrate the application completely to the Truffle framework from browser based Remix IDE to make the system adaptability easier.

Thank You

Questions?