Distributed Trust and Blockchains Date: *29.08.2019*

Instructor: *Sujit Prakash Gujar* Scribes: Zubair Abid
Akshay Kharbanda

Lecture 3: Distributed Consensus, and Cryptographic Puzzles

1 Recap

1.1 Quiz Review

1.2 Last Class

1. MyCoin (Goofy Coin)
   How does MyCoin work?

   (a) Coins are sent to a public key

   (b) Coins are sent by the sender signing them

   (c) When the next person sends it, they also sign it and add it to the hash pointer

   (d) It just needs digital identity, and relies on the statement that signatures cannot be forged.

   Challenges: The system does not provide a mechanism agains double spending of coins.

2. TrustMe Coin (Scrooge Coin)
   How does TrustMe Coin work?

   (a) A public ledger is maintained that can e verified

   (b) The hash pointer is always signed and publicly known.

   (c) There is pseudo-anonymity: public key will e disclosed, but not the real world identity.

   Challenges: Getting consensus in such a system, for distributed system. If a single party controls it the advantages of digital currency as envisioned by distributed system enthusiasts are lost.

2 Distributed Consensus

2.1 How does distributed consensus work for blockchain?

For distributed consensus to work in a blockchain,

1. As the protocol terminates, all honest nodes must agree on the same value.

2. The value must be given by an honest node.

2.2 Fischer-Lynch-Paterson impossibility

The FLP impossibility shows that in an asynchronous distributed system (under certain conditions), it is not possible for any distributed algorithm to solve the consensus problem even if a single node is being dishonest.

Paxos: Paxos is a solution that largely works in practice, but is possible to come up with theoretical test cases where the algorithm gets stuck, calculating for infinite time and thus not getting any result.

What is Bitcoin doing differently?
The specific set of cases under which the FLP Impossibility holds are altered in this new setting. Namely, alongside all else there is also a reward (bitcoins) given for maintaining the database correctly, and a penalty for being dishonest.

2.3 How is Consensus achieved for blockchain?

In a blockchain, the consensus happens in a specific manner:

1. Broadcast the transaction to all nodes.
2. Each node collects new transactions into a block.
3. A random node gets a chance to write to the ledger (blockchain). It broadcasts the block and the other nodes accept the block if all the transactions are valid (unspent, valid signatures).
4. Nodes express their acceptance by including its hash in the next block they create.

2.4 Challenges of the process

1. Choosing the node should not take too long.
2. The random node should not be faulty.
3. ”Randomising” the node in real life is not an easy task.

3 Figuring out how to select a random node

We are motivated by the idea that selecting a node at random is not an easy task. Random number generators that exist are pseudorandom, using a seed value. We could try to therefore implement pseudorandom with a completely random seed, or discard the approach entirely in favour of another one.
In general, there are two ways we consider of selecting a random node.

1. Noise
2. Solving a puzzle

3.1 Using noise to select the random node

Noise is used as the pseudorandom generator seed.
It needs to be accessible to all the nodes, however.
One idea suggested: At each round, the protocol generates a certain random string and we pick a node with identity having the same bit string in its identity.
Challenges to this idea

1. This is prone to Sybil attacks. One dishonest user can create multiple accounts, increasing their own probability for mining the next block, leading to centralisation.

   Say dishonest user creates 1 Million blocks, and 10,000 other users have 1 block each. This user writes the next block with

   $$\textsc{Probability} = \frac{1,000,000}{1,010,000} = 1(almost)$$

2. We also know in which order the following people will be writing the next block. This opens up space for human harm.

3.2 Puzzle approach

Another approach is to use a cryptographic puzzle, and the one who solves it first will be appending to the ledger next.
An obvious concern is that machines with higher computational power will solve the challenges faster, and can again control the system if that much compute is available to them. So the difficulty of the challenge is adjusted proportional to capacity power.

3.3 How much damage can a malicious node do?

1. *Stealing others' bitcoins:* is not particularly a possibility, as digital signatures cannot be forged.
2. *Denial of Service to certain people*
3. *Double Spending:* TODO WRITE

4 Cryptographic Puzzles

4.1 What is a Puzzle?

4.2 Proof of Work and Incentive Engineering

5 Introduction

In your scribes make proper sections, subsections. The following general instructions should be followed.

1. Do not use all CAPS in titles.
2. Use notation used in the class. (vectors, variables are in small letters, matrices, sets are in capital letters).
3. All variables must be in math mode. That is $ $. For example, we write n-dimensional and not n-dimensional. Typically while writing scientific technical reports, all the variables are used in italics like x, n etc.
4. All Figures/Tables must be centered. If you are using any pictures, try to use \begin{center} \end{center} around it.
5. Proof read once before submitting. (There should not be ? in pdfs I receive).
6. Make sure there are no spelling mistakes and grammar mistakes.
7. Use \begin{definition} \end{definition} or theorem environments appropriately.
8. Note that all important equations should be numbered and not important equations should not be numbered.

   \begin{equation}\label{eq:use_suitable_name}\end{equation}

   will do in latex.
9. You can use

   \ref{eq:use_suitable_name}

   for referencing it any where in the document. References to equations/tables/figures should be Fig. no Eq. (no) and Table no etc.

10. Do not use boldface to emphasize anything. Use command emph provided by latex.

11. Go through Section 2 of MS Thesis Submission guidelines for more on general guidelines for writing reports.

12. As far as possible create your own examples/figures. If any figure is downloaded from internet, please mention appropriate image credits.

13. Do not create images from textbook and paste them. You will get zero marks.

14. Any case of plagiarism will get zero marks.

15. If you are new to latex, you might find the following link useful

    https://en.wikibooks.org/wiki/LaTeX/Mathematics

    I personally use overleaf, which is cloud based latex tool. Overleaf and Shareltex (another popular cloud based latex tool) have joined together to offer cloud based latex service.

    There are many latex tools and editors available for offline use. You can choose any one based on your comfort.

16. However, it should be noted that you must submit Overleaf/Sharelatex link to TA for first scrutiny.

17. **While Submitting** You must use subject line as ‘DBTM18: Lecture X scribes’ where X is replaced by your lecture number. The file should be named as: DBT18_Lecture_X_yourname.zip The zip file must contain all the required resources.

18. You must submit overleaf link of the project to TAs within 7days from the lecture. For example, if the lecture you are scribing happens to be on Tuesday, you must submit before coming to the class on next Tuesday.

19. Note that this is 3 people working for 5% of evaluation. Put your efforts in making scribes best. considerable amount of effort is expected.

20. Do not remove any of

    ```
    \usepackage{}
    ```

    commands at top. If you add any package that is clashing with the above packages, remove them.

Definition 1 (def)**.** *Any important definitions will go here*

Theorem 1. *Theorems should go in this enviroment*