PhD 1^{st} semester Bi-annual Report

XING Yidi

May 10, 2019

Doctoral project background

Title of thesis - Privacy and Security in Blockchain: Transaction confidentiality, and Proof-of-Reputation based consensus

Tutorship - Co-tutorship by the collaboration of laboratory LIRIS, INSA Lyon, France and the University of Passau, Germany

List of supervisors - Lionel BRUNIE, Harald KOSCH, Sonia BEN MOKHTAR, Omar HASAN

Start date of the PhD - 01/10/2018

Doctoral School - Ecole Doctorale InfoMaths

Team and Laboratory - Equipe DRIM, LIRIS

Period of report - from 1st October 2018 to 30th Juin 2019

1 Introduction

This report is an attempt to consolidate and document all the research related activities, tasks carried out under the supervision, guidance and continued support of the research supervisors during the scholars first year of study from 1^{st} October 2018 - 30^{th} Juin 2019.

(All the communications(mails/letters/documents) pertaining to research study have been presented in this report for analysis of the efforts taken, progress made by the scholar since registration and for future reference.)(????)

I extend my sincere gratitude and profound thanks to my research Guide and Supervisor, **Omar Hasan, Sonia Ben Mokhtar, Harald Kosch and Lionel Brunie.**

2 Tentative Research Topic Statement

In the recent years, the blockchain field has received great attention from different and diverse domains. The blockchain technology itself has undergone tremendous evolution, improvement and progress.

Since the successful advent of Bitcoin in 2009, a large number of alternative cryptocurrencies came out nowadays, such as Litecoin, EOS, Stellar, each has its original advanced features; also numerous general-purpose blockchain platforms such as, "Ethereum" that provide smart contract enforcement, "Hyperledger Fabric" that got participation by IBM, Microsoft, major bank organizations, etc.

Generally, a blockchain system has features like distributed, decentralized, autonomy and a certain degree of openess, and thus are principally based on p2p netowrks, in order to organized the scattered nodes to participate to data validation and ledger updating in the global scale. Within a p2p network, the nodes connect and interact with each other in a flat topology. They all have an equivalent status: each node takes charges independently of being a network router, validate transactions and transaction blocks, broadcast data, discover and communicate with newly joined nodes, and so on.

The blockchain systems - through their specific economic incentive mechanism - guarantee a strong motivation for all the nodes to participate to the generation and validation of new transaction blocks. During this step, a critical action is to elect a special node to be responsible to add - for the first time - the next block into the blockchain ledger. Here, we need a specific algorithm to complete the selection, that is called a consensus algorithm.

Consensus problem

What is the definition and the utility of a such consensus algorithm? To answer that question, a clarification about "what is consensus problem" is helpful.

The main research of "consensus problem" is to provide a solution about how to form a consensus probability distribution when a group of individuals has their own subjective distribution regarding a specific probability space.

Before the "age of blockchain", the consensus researches in IT field focused on distributed consistency, that is, to make sure that every node within a distributed systems cluster having exactly the same data and could make global consensus regarding each specific proposal (to the system). It is a basic problem in distributed computing.

Difference between "consistency research" and "consensus research"

Although the words "consensus" and "consistency" have similar significations in the literal sense, we need to clarify their delicate difference in this topic statement section: the "consistency problem researches" emphasizes on the the final and stable status that the ndoes made after the consensus process; as for the "consensus problem researches", it focuses on the process itself and the algorithm used to allow the distributed nodes achieve consensus with each other.

BFT problem with consistency research

In early consistency researches,

3 Expected Scientific Objectives