شبكة المعلومات الجامعية
التوثيق الإلكتروني والميكروفيلم

جامعة عين شمس

التوثيق الإلكتروني والميكروفيلم

قسم

نقسم بالله العظيم أن المادة التي تم توثيقها وتسجيلها
علي هذه الأقراص المدمجة قد أعدت دون أية تغيرات

يجب أن

تحفظ هذه الأقراص المدمجة بعيدا عن الغبار

MONA MAGHRABY

AIN SHAMS UNIVERSITY
FACULTY OF ENGINEERING
Computer and Systems Engineering

Different Consensus Algorithms Protocols used for Blockchain Technology and Smart Contract

A Thesis submitted in partial fulfilment of the requirements of
Master of Science in Electrical Engineering
(Computer and Systems Engineering)

by

Sherif Mohamed Samir Fth-Alla Shebl

Bachelor of Science in Electrical Engineering
Communication and Electronics Section
Faculty of Engineering (at Shoubra), Zagazig University, 2003

Supervised By

Prof. Dr. Hoda Korashy Mohamed

Dr. Hazem Said Ahmed Mohamed

Cairo - (2020)

AIN SHAMS UNIVERSITY
FACULTY OF ENGINEERING
Computer and Systems Engineering

Different Consensus Algorithms Protocols used for Blockchain Technology and Smart Contract

by

Eng. Sherif Mohamed Samir Fth-Alla

Bachelor of Science in Electrical Engineering
(Communication and Electronics) Department
Faculty of Engineering (at Shoubra), Zagazig University, 2003

Examiners’ Committee

Name and Affiliation	**Signature**
Prof. Mostafa Mahmoud Aref	
Head of computer science Dept., Computer and Information sciences, Ain Shams University	....
Prof. Mohamed Mahmoud Ahmed Taher	....
Computer and Systems, Ain Shams University	
Prof. Hoda Korashy Mohamed	....
Computer and Systems, Ain Shams University	

Date: 22 December 2020

Statement

This thesis is submitted as a partial fulfilment of Master of Science in Electrical Engineering, Faculty of Engineering, Ain shams University.

The author carried out the work included in this thesis, and no part of it has been submitted for a degree or a qualification at any other scientific entity.

Sherif Mohamed Samir Fth-Alla Shebl

Sherif M. Samir

……………………………………………………………………….

Date: 22 December 2020

Researcher Data

Name	: Sherif Mohamed Samir Fth-Alla Shebl
Date of Birth	: 22/06/1979
Place of Birth	: Cairo, Egypt
Last academic degree :	Diploma of Science in Electrical Engineering.
Field of specialization	: Computer Engineering and Systems.
University issued the degree	: Faculty of Engineering, Ain Shams University
Date of issued degree	: 2014
Current job	: Senior Software Development Engineer.

Abstract

Secret key and public key are fundamental building blocks in cryptography that are used in numerous protocols. A trusted party is obligated to protect its secret key from any unfaithful party and spread its public key through secure communication channels to all other parties, this notation is called public key encryption.

Node resources scale sub linearly in all respects (storage, disk IO, computation, and bandwidth). So a need for a deeper concept arises. Our goal is to implement a stateless consensus architecture, which means that all blocks can be fully validated without any access to state. The motivation is that this will allow validators to not keep any main chain state, lowering validator hardware requirements and making it more accessible. One of the difficulties with this is that the witness sizes required for this can be very substantial. We can reduce this by using polynomial commitments, in which any number of data elements can be proven using just a single group element as a witness. One such scheme relying on sorted key-value lists. However, it introduces significant complexity in the form of several layers of caching and needing permutation arguments to merge those separate commitments.

This thesis aim is to address these two fundamental issues. First, we scale threshold cryptosystems, which protect secret keys by dividing them up across many parties. We discuss threshold signatures, verifiable secret sharing and distributed key generation protocols that can scale to millions of participants. Our protocols reduce execution time, depending on the scale. For example, at large scales, we reduce time from tens of hours to tens of seconds. At the core of most of our contributions lie new techniques for computing evaluation proofs in constant-sized polynomial commitments. Specifically, we describe how to decrease the time to calculate n proofs for a degree bound n polynomial from $\Theta(n^2)$ to $\Theta(n\ log\ n)$, at the cost of increasing proof size from $\Theta(1)$ to $\Theta(log\ n)$.

Acknowledgment

First and above all, I sincerely appreciate the almighty God for His graces, strength, sustenance and above all, His faithfulness and love for my life. His benevolence has made me excel and successful in all my academic pursuits. I thank him for providing me this opportunity and granting me the capability to proceed successfully. I am grateful for his provision of joys, challenges and grace for grace that have been bestowed upon me during this research work, and indeed, throughout my life.

There are so many people I want to thank, it would be understandable if you get tired of reading this…

I would like to place on records my heartfelt and sincere thanks to my supervisor, Prof. Hoda Korashy Mohamed, for supporting and guiding me during these years. For the freedom to explore any topic I was interested in. For her guidance when I did not know what to do with that freedom. This thesis may not exist without her valuable advice and useful comments. And my thanks to my thesis committee, Dr. Hazem Said Ahmed Mohamed, for his invaluable Feedback. I appreciate their contribution of time and ideas to make my work productive and stimulating. Their valuable suggestions, comments and guidance encouraged me to learn more day by day. Their deep insights helped me at various stages of my research. Big thanks once again go to them for without them this work would never see the light as it is today.

I would like to take this opportunity to thank my family, for a loving home.

My mother, for all her sacrifices. For raising us. For letting us go. For never doubting us. For teaching us independence and responsibility through her faith in us. For being a role model. For her boundless love.

My wife Rana, for her love, understanding, and support to finish my academic degree.

Without their help, this thesis would not have been completed. I dedicate all my success to them.

Finally, A Heartfelt thanks to my supportive wonderful family and friends for supporting and encouraging me to keep me motivated to work valuable and harder in all life moments. You have a constant source of strength and inspiration to me especially at the moment when there was no one to answer my queries.

Sherif Mohamed Samir Fth-Alla Shebl
Computer and Systems Engineering
Faculty of Engineering
Ain Shams University
Cairo, Egypt
December 2020

Table of Contents

List of Figures