# ANALISA KEMUNGKINAN ALGORITMA SHA256 & ALGORITMA SCRYPT DALAM MENEMUKAN BLOK BARU PADA TEKNOLOGI BLOCKCHAIN

Novan Ageng Mulyadi[1], YB. Dwi Setianto[2]

[1,2]Program Studi Teknik Informatika, Fakultas Ilmu Komputer, Universitas Katolik Soegijapranata

[1]14k10074@student.unika.ac.id, [2]setianto@unika.ac.id

## Abstract

*In cryptocurrency, a block is a record of new transactions that could mean the location of cryptocurrency, medical data, or even voting records. Once each block is completed it's added to the chain, creating a chain of blocks: a blockchain. Because cryptocurrencies are encrypted, processing any transactions means solving complicated math problems using specified algorithm like SHA256 and Scrypt. People who solve these equations are rewarded with cryptocurrency in a process called mining. In this study the authors will find out the comparison of SHA256 and Scrypt to work on the blockchain. To find out the comparison between SHA256 and Scrypt some test will be done in this research. The test were given to both algorithm on some test System to observe which algorithm that has highest probability in finding new block. the results of the tests done in this paper show that Scrypt is much slower to hash than SHA256 but the Scrypt algorithm has greater chance to find a new block.*

**Keywords:** *SHA256, Scrypt, Proof-of-Work, Blockchain, Comparison*

## Pendahuluan

Penelitian ini membandingkan probabilitas untuk menemukan blok baru antara Algoritma SHA256 dan Algoritma Scrypt yang terdiri dari enam bab. Bab pertama adalah tentang latar belakang yang membandingkan SHA256 dan Scrypt secara umum, bab kedua berisi tentang referensi penelitian seperti proses publikasi elektronik dan dokumentasi, bab ketiga akan menjelaskan Metodologi secara umum seperti platform yang digunakan, eksperimen yang akan diuji dan bagian yang diamati untuk mengumpulkan data, bab keempat akan menggambarkan sistem pengujian dan program yang akan digunakan untuk mengamati, di bab kelima berisi hasil eksperimen yang telah dilakukan dan bab keenam terakhir berisi hasil kesimpulan dari penelitian ini.

## Landasan Teori

Menurut Ittay Eyal, Adem Efe Gencer, Emin Gün Sirer, Robbert van Renesse, Bitcoin adalah mata uang kripto terdesentralisasi terdesentralisasi yang secara implisit mendefinisikan dan menerapkan konsensus [1]. Bitcoin menggunakan protokol blockchain untuk membuat serial transaksi mata uang Bitcoin di antara penggunanya. Mesin negara direplikasi mempertahankan saldo dari pengguna yang berbeda, dan transisinya adalah transaksi yang memindahkan dana di antara mereka. Mesin negara ini dikelola oleh node-node sistem, yang disebut penambang.

Menurut Roman Beck, Jacob Stenum Czepluch, Nikolaj Lollike, Simon Malone, Blok A berisi data semua transaksi dalam jangka waktu tertentu, dan referensi ke blok sebelumnya [2]. Kriptografi yang digunakan untuk membuat blok berbeda tergantung pada protokol blockchain yang digunakan, tetapi pada dasarnya kita dapat melintasi seluruh blockchain dan menemukan setiap transaksi yang pernah dilakukan, semua jalan kembali ke blok pertama, yang disebut blok genesis. Algoritma Hashing digunakan untuk memastikan bahwa semua blok terbentuk dengan baik dan tidak dirusak, dan dengan demikian blockchain membuat dirinya aman dan hampir tidak bisa dipecahkan. Blockchain tidak disediakan dari satu server, tetapi dijalankan pada jaringan komputer yang tersebar luas sebagai buku besar yang didistribusikan. Semua peserta jaringan menyimpan semua data di blockchain, dan semuanya bekerja sama dalam mengembangkannya. Komputer-komputer ini sering disebut penambang. Tergantung pada protokol blockchain, ini akan bersaing untuk membentuk blok baru yang kemudian ditambahkan ke blockchain ketika dipilih melalui skema konsensus.

Menurut Arthur Gervaisy, Ghassan O. Karamez, Damian Gruber, Srdjan Capkun, ketentuan privasi karena integrasi filter Bloom di klien SPV [3]. Tunjukkan bahwa filter Bloom menyebabkan kebocoran privasi yang serius dalam implementasi klien SPV yang ada. Lebih khusus lagi, bahwa sejumlah besar alamat pengguna klien SPV yang memiliki sejumlah kecil alamat Bitcoin (misalnya, <20) bocor oleh satu filter Bloom. Selain itu, sejumlah besar alamat pengguna bocor jika musuh dapat mengumpulkan dua filter Bloom berbeda yang dikeluarkan oleh node yang sama, terlepas dari target false positive rate dari filter, dan jumlah alamat yang dimiliki oleh pengguna. Mengingat kebocoran informasi seperti itu dapat sangat merusak privasi pengguna.

Menurut Arthur Gervaisy, Hubert Ritzdorfy, Ghassan O. Karamez and Srdjan Capkun, perbedaan antara jumlah input dan output dari suatu transaksi dikumpulkan dalam bentuk biaya oleh penambang Bitcoin [4]. Penambang adalah rekan, yang berpartisipasi dalam pembuatan blok Bitcoin. Blok-blok ini dihasilkan dengan menyelesaikan skema proof-of-work (PoW) berbasiskan hash, para penambang harus menemukan nilai nonce yang, ketika di-hash dengan field tambahan, hasilnya di bawah nilai target yang diberikan. Jika seperti itu ditemukan, penambang kemudian memasukkannya ke dalam blok baru sehingga memungkinkan setiap entitas untuk memverifikasi PoW. Karena setiap blok terhubung ke blok yang dihasilkan sebelumnya, blockchain Bitcoin tumbuh pada generasi blok baru di jaringan.

Menurut Arthur Gervais, Vasileios Glykantzis, Ghassan O. Karame, Hubert Ritzdorf, Karl Wüst, Srdjan Capkun, mekanisme konsensus bukti kerja (PoW) adalah mekanisme konsensus terluas yang terluas dalam blockchain yang ada [4]. PoW diperkenalkan oleh Bitcoin dan mengasumsikan bahwa setiap rekan menilainya dengan "kekuatan komputasi" nya dengan memecahkan bukti contoh kerja dan membangun blok yang sesuai. Bitcoin, misalnya, menggunakan PoW berbasis hash yang memerlukan pencarian nilai nonce, sehingga ketika di-hash dengan parameter blok tambahan, nilai hash harus lebih kecil dari nilai target saat ini. Ketika seperti itu ditemukan, penambang menciptakan blok dan meneruskannya pada lapisan jaringan.

Menurut Jo¨el Alwen, Binyi Chen, Krzysztof Pietrzak, Leonid Reyzin, Stefano Tessaro, Scrypt adalah calon MHF sederhana yang dirancang oleh Percival, dan dijelaskan dalam RFC 7914 [5]. Telah digunakan dalam sejumlah cryptocurrency dan telah menjadi inspirasi bagi Argon2d, salah satu pemenang dari kata sandi baru-baru ini kompetisi-hashing. Meskipun popularitasnya, tidak ada batas bawah yang ketat pada kompleksitas memorinya yang diketahui.

Menurut Levent Ertaul, Manpreet Kaur, Venkata Arun Kumar R Gudise, Scrypt adalah hashing algorithm yang memanfaatkan fungsi derivasi kunci berdasarkan sandi [6]. Ini menghasilkan vektor besar string bit pseudorandom. Dibutuhkan banyak memori dan biaya CPU. Banyak nomor pseudorandom dihasilkan dalam seluruh proses yang disimpan dalam memori akses acak sehingga menempati ruang memori yang sangat besar. Ini dianggap sebagai algoritma yang mahal karena setiap elemen yang dihasilkan selama waktu hashing membutuhkan lebih banyak memori dan komputasi. Ini sangat aman karena sangat sulit bagi penyerang untuk memecahkan pesan berciri ini karena kurangnya sumber daya dan memori.

## Metodologi Penelitian

Langkah pertama dalam melakukan penelitian ini adalah mencari jurnal-jurnal dan dokumentasi maupun publikasi elektronik yang berkaitan dengan topik SHA256, Scrypt dan juga Blockchain kemudian dari sumber-sumber referensi tersebut dilakukan penyusunan design program untuk membuktikan hipotesa yang dibuat yang nantinya dilakukan testing dan dilakukan Analisa terhadap data yang didapatkan.

Proyek ini akan membandingkan kemungkinan Algoritma SHA256 dan Scrypt Algoritma untuk menemukan blok baru. Program sumber yang digunakan untuk menjalankan tes adalah Bitcoin Core pada SHA256 dan Litecoin Core pada Scrypt. Untuk menyelesaikan tes, Penulis menggunakan 4 CPU yang berbeda untuk menjalankan tes.

Untuk membandingkan SHA256 dan Scrypt, Penulis akan mencoba untuk menguji dalam beberapa kondisi yang berbeda seperti:

1. Waktu Hashing: proses hashing akan dilakukan 3 kali untuk setiap algoritma dengan waktu hashing yang berbeda, yang pertama adalah 10 jam hashing, yang kedua adalah 3 jam hashing, dan yang terakhir adalah 1 jam hashing.
2. Test System: proses hashing akan dilakukan pada 4 CPU yang berbeda, yang pertama adalah Intel Pentium G4560, yang kedua adalah AMD Ryzen 3 1300X, yang ketiga adalah Intel Core i5-4200H, dan yang terakhir adalah AMD Ryzen 7 1800X.

Dari pengujian tersebut, Penulis akan mencatat berapa banyak percobaan pada setiap pengujian yang menggunakan pengukur hash dan berapa banyak blok baru yang ditemukan selama pengujian dengan menggunakan bahasa pemrograman awk dan akan digunakan untuk menghitung kemungkinan menemukan blok baru.

## Hasil dan Pembahasan

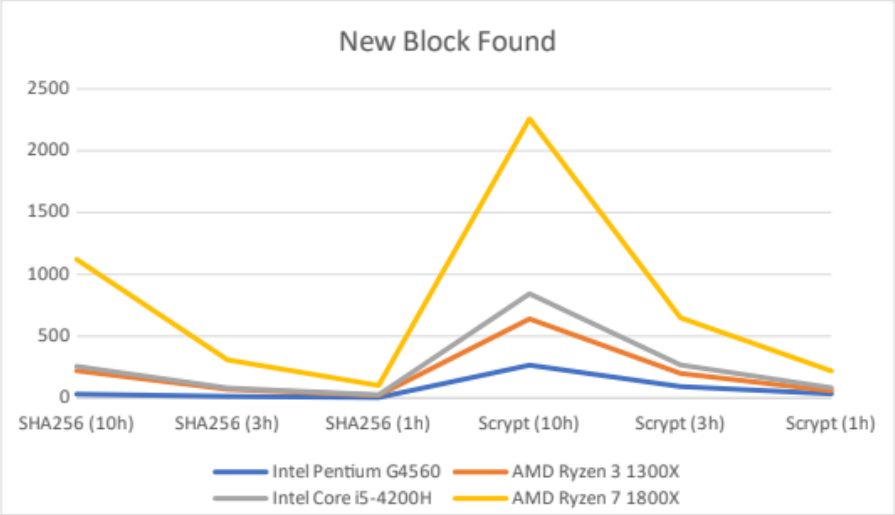
Penulis menjalankan pengujian pada 4 Sistem Tes yang berbeda untuk membandingkan kemungkinan menemukan blok baru pada setiap algoritma, semua tes direkam dengan simplescreenrecorder pada Linux Ubuntu 16.04 dan masuk ke file `debug.log`. Dari setiap file log, Penulis menggunakan awk untuk mengumpulkan informasi dari semua file log.

Dari file debug penulis tahu bahwa penemuan blok baru ditandai dengan 'proof-of-work found', dan upaya dapat dihitung dengan pengukur hash dalam kh / s. Dan kemudian Pengarang mengumpulkan data ini:

Tabel blok baru yang ditemukan selama pengujian, direkam menggunakan debug.log dan diproses menggunakan utilitas awk pada sistem Linux:

Tabel 1: Tabel blok baru

| CPU | New Block on SHA256 in 10 hours | New Block on SHA256 in 3 hours | New Block on SHA256 in 1 hours | New Block on Scrypt in 10 hours | New Block on Scrypt in 3 hours | New Block on Scrypt in 1 hours |
|---|---|---|---|---|---|---|
| G4560 | 31 | 13 | 4 | 265 | 92 | 34 |
| i5 4200H | 35 | 10 | 4 | 203 | 68 | 26 |
| R3 1300X | 190 | 58 | 17 | 375 | 107 | 23 |
| R7 1800X | 864 | 227 | 76 | 1414 | 382 | 136 |



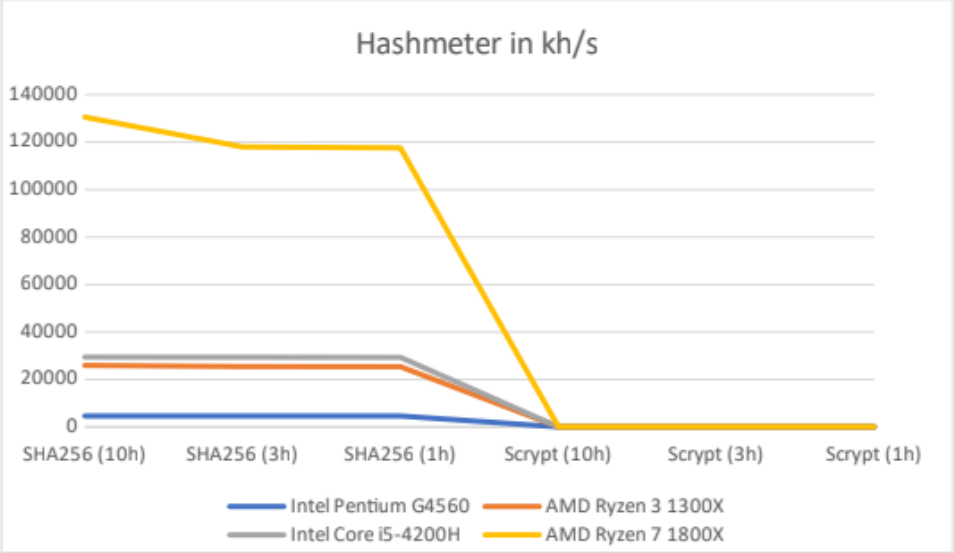

Gambar 1: Grafik blok baru

Dari data di atas meja Anda dapat melihat perbedaan besar antara dua algoritma dalam 24 skenario pengujian yang berbeda, algoritma Scrypt dapat menemukan lebih banyak blok baru daripada algoritma SHA256 di setiap tes. Dari analisis saya itu terjadi karena algoritma Scrypt memiliki banyak parameter biaya yang telah ditetapkan dan itu membuat algoritma scrypt memiliki target hashing lebih spesifik daripada SHA256.

Tabel hash meter yang direkam selama tes, dikumpulkan dari debug.log dan diproses menggunakan utilitas awk pada sistem Linux:

Tabel 2: Table hashmeter

| CPU | Hashmeter on SHA256 in kh/s | Hashmeter on SHA256 in kh/s | Hashmeter on SHA256 in kh/s | Hashmeter on Scrypt in kh/s | Hashmeter on Scrypt in kh/s | Hashmeter on Scrypt in kh/s |
|---|---|---|---|---|---|---|
| G4560 | 4619 | 4614 | 4619 | 9 | 9 | 9 |
| i5 4200H | 3516 | 3910 | 3905 | 6.55 | 6.5 | 6.7 |
| R3 1300X | 21305 | 20809 | 20753 | 10 | 10 | 10 |
| R7 1800X | 101111 | 88624 | 88271 | 41 | 36 | 36 |



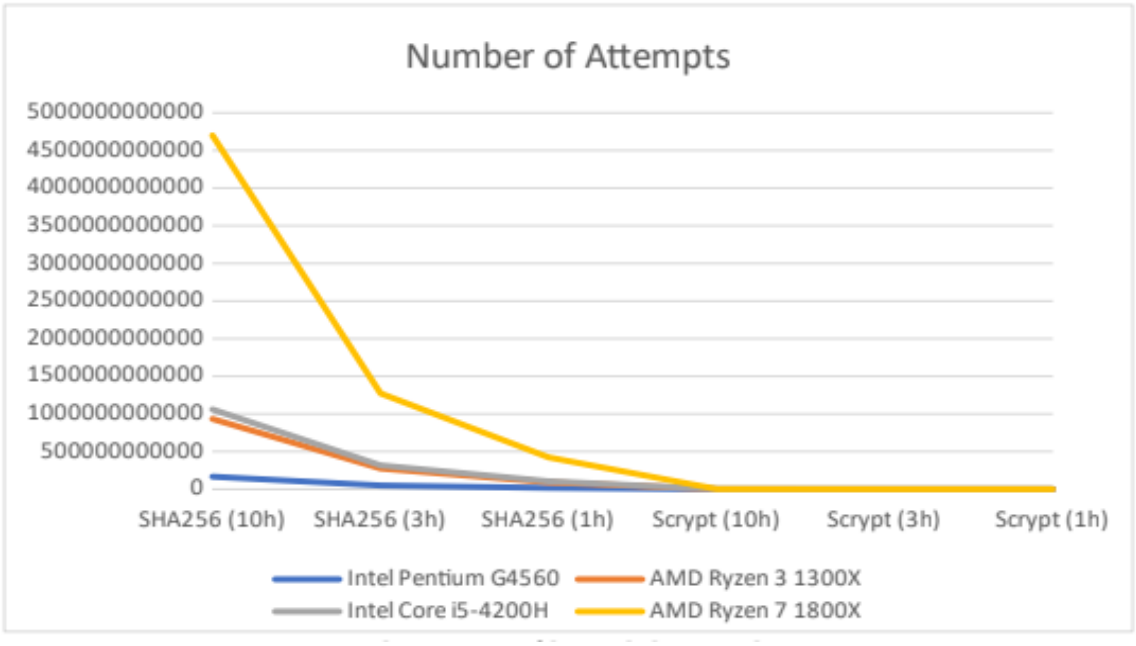

Gambar 2: Grafik hashmeter

Dari data Anda hampir tidak dapat melihat kesenjangan besar antara dua algoritma, sistem pengujian dapat memiliki lebih banyak blok pada SHA256 daripada algoritma Scrypt di setiap sistem uji. Dari analisis saya itu terjadi karena scrypt memiliki proses yang lebih rumit daripada SHA256, bahkan algoritma Scrypt dapat berisi algoritma hashing lain dalam prosesnya juga. Itu sebabnya itu lebih lambat daripada algoritma Scrypt.

Tabel percobaan yang dihitung dengan mengalikan hashmeter dan jumlah detik dalam setiap skenario pengujian yang berjalan selama pengujian, diproses menggunakan utilitas awk pada sistem Linux:

Tabel 3: Tabel jumlah percobaan

| CPU | Attempt on SHA256 in 10 hours | Attempt on SHA256 in 3 hours | Attempt on SHA256 in 1 hours | Attempt on Scrypt in 10 hours | Attempt on Scrypt in 3 hours | Attempt on Scrypt in 1 hours |
|---|---|---|---|---|---|---|
| G4560 | 1.66E+11 | 49831200000 | 16628400000 | 324000000 | 97200000 | 32400000 |
| i5 4200H | 126576000000 | 42228000000 | 14058000000 | 235800000 | 70200000 | 24120000 |
| R3 1300X | 766980000000 | 224737000000 | 747108000000 | 360000000 | 108000000 | 36000000 |
| R7 1800X | 3640000000000 | 957139000000 | 317776000000 | 1476000000 | 388800000 | 129600000 |



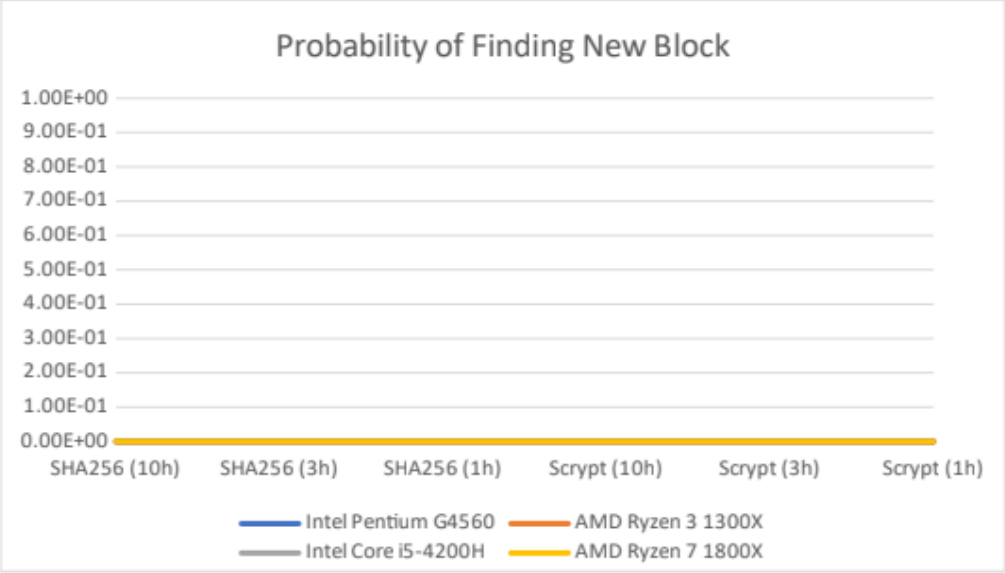

Gambar 3: Grafik jumlah percobaan

Dari data yang Anda ketahui bahwa upaya pada SHA256 jauh lebih banyak daripada pada algoritme Scrypt, itu terjadi karena pengukur hash pada SHA256 jauh lebih cepat daripada algoritma Scrypt dan itu berarti SHA256 dapat melakukan lebih banyak upaya daripada algoritma Scrypt. Bentuk analisis saya, hanya dengan melihat hash meter Anda tahu bahwa itu terjadi karena SHA256 memiliki proses hashing lebih cepat daripada algoritma Scrypt.

Tabel probabilitas yang dihitung dari semua data yang dikumpulkan dari tes dan diproses menggunakan LibreOffice Calc pada sistem Linux:

Tabel 4: Tabel probabilitas ditemukannya blok baru

| CPU | SHA256 Probability in 10 hours | SHA256 Probability in 3 hours | SHA256 Probability in 1 hours | Scrypt Probability in 10 hours | Scrypt Probability in 3 hours | Scrypt Probability in 1 hours |
|---|---|---|---|---|---|---|
| G4560 | 0 | 0 | 0 | 8.17901E-05 | 0 | 0 |
| i5 4200H | 0 | 0 | 0 | 0 | 0 | 0 |
| R3 1300X | 0 | 0 | 0 | 0 | 0 | 0 |
| R7 1800X | 0 | 0 | 0 | 0 | 0 | 0 |




Gambar 4: Grafik probabilitas ditemukannya blok baru

Dari data pada tabel ini Anda tahu bahwa algoritma Scrypt memiliki probabilitas yang sedikit lebih tinggi daripada algoritma SHA256 di setiap skenario pengujian. Dari analisis saya itu semua terjadi karena algoritma Scrypt memiliki parameter yang lebih standar seperti parameter biaya CPU, parameter biaya memori, parameter Paralelisasi, panjang Output dll yang membuatnya memiliki proses hashing lebih spesifik dan mencegah algoritma membuang sumber dayanya.

## Kesimpulan

Dari semua tes yang dilakukan, dapat disimpulkan bahwa algoritma Scrypt dapat menemukan lebih banyak blok baru daripada algoritma SHA256 meskipun SHA256 dapat melakukan lebih banyak upaya di detik tetapi jumlah blok baru yang ditemukan kurang dari algoritma Scrypt. Oleh karena itu, penulis menyimpulkan bahwa Scrypt memiliki probabilitas yang lebih tinggi dalam menemukan blok baru daripada algoritma SHA256 pada teknologi Blockchain.

Bagaimanapun, penulis menyarankan untuk penelitian berikutnya untuk melakukan penelitian dalam hal keamanan pada algoritma yang terkandung dalam teknologi blockchain. Jadi, dapat dipastikan bahwa algoritma tidak hanya memiliki probabilitas

tinggi untuk menemukan blok baru, tetapi juga menyediakan keamanan data dalam teknologi Blockchain.

## Daftar Pustaka


[1] I. Eyal, A. E. Gencer, E. G. Sirer, and R. van Renesse, "Bitcoin-NG: A Scalable Blockchain Protocol," *CoRR*, vol. abs/1510.02037, 2015, [Online]. Available: http://arxiv.org/abs/1510.02037.

[2] R. Beck, J. S. Czepluch, N. Lollike, and S. Malone, "BLOCKCHAIN – THE GATEWAY TO TRUST-FREE CRYPTOGRAPHIC TRANSACTIONS," *Research Papers*, May 2016, [Online]. Available: https://aisel.aisnet.org/ecis2016_rp/153.

[3] A. Gervais, S. Capkun, G. O. Karame, and D. Gruber, "On the Privacy Provisions of Bloom Filters in Lightweight Bitcoin Clients," in *Proceedings of the 30th Annual Computer Security Applications Conference*, New York, NY, USA, 2014, pp. 326–335, doi: 10.1145/2664243.2664267.

[4] A. Gervais, G. O. Karame, K. Wüst, V. Glykantzis, H. Ritzdorf, and S. Capkun, "On the Security and Performance of Proof of Work Blockchains," in *Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security*, New York, NY, USA, 2016, pp. 3–16, doi: 10.1145/2976749.2978341.

[5] J. Alwen, B. Chen, K. Pietrzak, L. Reyzin, and S. Tessaro, "Scrypt Is Maximally Memory-Hard," in *Advances in Cryptology – EUROCRYPT 2017*, Cham, 2017, pp. 33–62.

[6] L. Ertaul and M. Kaur, "Implementation and Performance Analysis of PBKDF 2, Bcrypt, Scrypt Algorithms varunkrg."