BAB II
TINJAUAN PUSTAKA

2.1. Penelitian terdahulu

Berdasarkan judul penelitian, terdapat beberapa penelitian yang berkaitan dan dapat mendukung penelitian yang sekarang serta dapat diajukan bahan acuan, antara lain :

Penelitian tahun 2018 yang berjudul "*Verus Proof of Power, A provable Hybrid Solution to 51% Hash Attacks"* oleh M. J. Toutonghi dan M. F. Toutonghi. *Verus Proof of Power (PoP)* merupakan sebuah algoritma konsensus hybrid yang menggabungkan *Proof of Work (PoW)* dan *Proof of Stake (PoS)* digunakan untuk memvalidasi setiap blok. Kita ketahui bahwa Verus coin adalah project komunitas open source yang memanfaatkan kemajuan terbaru dalam privasi dan keamanan *blockchain*. Keamanan yang dijelaskan disini dan terbukti tahan terhadap 51% atau bahkan 99% serangan hash *PoW*. Selain itu penerapan *Crypto* conditions yang unik dan disempurnakan juga memungkinkan verus coin juga memberikan solusi untuk masalah PoS dari apa saja yang dipertaruhkan.

Penelitian tahun 2018 yang berjudul "*zk-SNARK Privacy and a Holistic Approach to ASICs"* oleh M. J. Toutonghi yang dimana dikatakan dalam penelitian nya bahwa saat ini verushash belum di implementasikan untuk perangkat GPU, sehingga jika diterapkan pada GPU mungkin akan menjadi lebih lambat daripada perangakat CPU. Inti Haraka512 didasarkan pada standar enkripsi AES, hal ini membuat verushash sangat cepat pada CPU modern dan karena didasarkan pada operasi AES standar, dapat menawarkan jaminan keamanan yang kuat.

Penelitian tahun 2018 yang berjudul "*GPU and CPU Accelerated Mining of Cryptocurrencies and their Financial Analysis"* oleh Iyer, S. G., dan Dipakumar Pawar, A. yang dimana mengatakan bahwa hashrate merupakan fungsi penting dalam melakukan penambangan cryptocurrency,

dalam melakukan penambangan semakin tinggi tingkat hash yang dihasilkan maka semakin tinggi hasil yang di dapatkan.

Penelitian tahun 2018 yang berjudul "*APPLICATIONS OF DATA MINING IN FINANCE"* oleh N. K. Hariharan dimana dalam bisnis keuangan, penambangan data sangat penting atau berharga. Hingga saat ini, penambangan data terlah terbukti menjadi solusi yang layak untuk mendeteksi dinamika keterkaitan data keuangan.

Penelitian tahun 2018 yang berjudul "Teknologi Blockchain Cryptocurrency Di Era Revolusi Digital" oleh Bhiantara, Ida Bagus Prayoga dimana dalam penelitian tersebut mengatakan bahwa cryptocurrency merupakan sebuah teknologi menggunakan basis blockchain. Untuk dapat menggunakan mata uang crypto ini harus ada kesepakatan untuk menggunakan nya tanpa menggunakan pihak ketiga. Setiap proses transaksi yang dilakukan akan disimpan dan dicatat pada setiap folder anggotanya. Catatan ini tidak dapat dirubah ataupun di hapus, namun hanya dapat ditambah pada saat melakukan transaksi.

Tabel 2. 1 Penelitian terdahulu berkaitan dengan penelitian sekarang

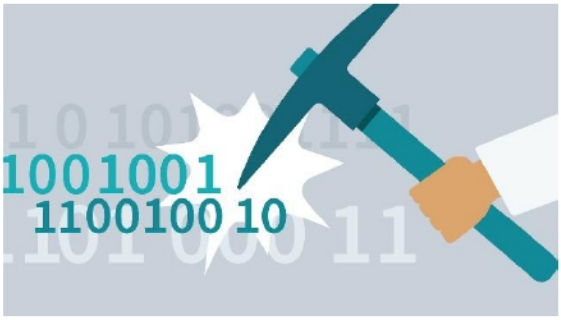
Peneliti	**Pendekatan Metode**	**Hasil**
M. J. Toutonghi and M. F. Toutonghi (2018)	Metode Pos hash dan Pos Nonce Costruction pada VerusPoP	Sebuah solusi keamanan yang terbukti dengan 51% dari serangan hash [4].
M. J. Toutonghi, (2018)	Menggunakan Metode verushash dengan algoritma Haraka512 V2	Penambangan verus dengan algoritma verus hash menggunakan Haraka512 V2 dapat memaksimalkan kinerja CPU modern

		sehingga dapat bersaing dengan GPU dan ASIC[3].
Iyer, S. G., & Dipakumar Pawar, A. (2018).	Metode umum dalam pengaturan lingkungan penambangan untuk mendapatkan hash yang tepat	Tingkat hash adalah tulang punggung penambangan cryptocurrency. Semakin tinggi tingkat hash, semakin tinggi hasilnya. Sebagai jumlah orang di seluruh dunia terlibat dalam bisnis penambangan cryptocurrency, yang telah secara signifikan meningkatkan jumlah perangkat keras standar non-kustom penambang[11].
N. K. Hariharan (2018)	Metode penerapan penambangan data dalam keuangan	Penambagan data dapat diterapkan di berbagai aplikasi keuangan seperti analisis resiko pinjaman, dan prediksi pembayaran[12].
Bhiantara, Ida Bagus Prayoga (2018)	Metode Blokchain pada Cryptocurrency	Cryptocurrency merupakan mata uang digital yang menggunakan teknologi blockchain. Penggunaan cryptocurrency memerlukan kontrak untuk menggunakan cryptocurrency tanpa menggunakan pihak ketiga lainnya[13].

Penelitian-penelitian di atas memberikan gambaran tentang Verus Coin, algoritma konsensus yang digunakan, keamanan yang dihadirkan, penggunaan CPU versus GPU dalam penambangan, peran hashrate dalam penambangan cryptocurrency, serta pentingnya penambangan data dalam konteks keuangan. Informasi ini akan menjadi dasar penting untuk menganalisis keuntungan penambangan Verus Coin pada CPU dengan memperhatikan perbandingan hashrate yang dihasilkan.

2.2. Dasar Teori

2.2.1 Crypto Mining



Gambar 2. 1 Crypto Mining[14]

Crypto mining, atau yang lebih dikenal sebagai penambangan kripto, merupakan proses yang melibatkan penggunaan perangkat keras komputer untuk menghasilkan koin baru dan mengonfirmasi transaksi dalam mata uang kripto. Dalam penambangan kripto, diperlukan penggunaan berbagai jenis perangkat keras khusus yang dirancang untuk melakukan tugas-tugas matematika yang kompleks. Alat-alat ini digunakan untuk memvalidasi transaksi kripto dan juga untuk menyelesaikan blok-blok dalam blockchain.

Proses penambangan kripto melibatkan komputer atau perangkat khusus yang disebut sebagai "penambang" (miners). Penambang ini bertugas untuk menyelesaikan serangkaian perhitungan matematika yang rumit untuk memverifikasi dan memvalidasi transaksi yang terjadi dalam jaringan kripto. Setelah sejumlah transaksi terverifikasi, blok baru akan ditambahkan ke blockchain.

Perangkat keras yang digunakan dalam penambangan kripto biasanya terdiri dari unit pemrosesan grafis (GPU) atau sirkuit terpadu khusus (ASIC), tergantung pada jenis mata uang kripto yang ditambang. GPU umumnya digunakan untuk penambangan mata uang kripto yang berbasis algoritma Proof of Work (PoW), sementara ASIC digunakan untuk mata uang kripto yang menggunakan algoritma khusus.

Selama proses penambangan, penambang akan bersaing satu sama lain untuk menyelesaikan tugas matematika yang kompleks dan memperoleh hadiah dalam bentuk koin kripto. Penambang yang berhasil menyelesaikan tugas tersebut dengan cepat akan memiliki peluang lebih besar untuk memperoleh hadiah dibandingkan dengan penambang lainnya.

Selain perangkat keras, perangkat lunak penambangan kripto juga diperlukan. Perangkat lunak ini membantu mengontrol operasi penambangan, menghubungkan penambang dengan jaringan kripto, dan menyediakan data dan informasi yang diperlukan.

Penambangan kripto memainkan peran penting dalam menjaga keamanan dan integritas jaringan blockchain. Dengan melakukan tugas verifikasi transaksi dan memvalidasi blok baru, penambang membantu mencegah kecurangan dan serangan terhadap jaringan kripto. Selain itu, penambangan juga merupakan cara untuk menghasilkan koin kripto baru yang bisa digunakan untuk berbagai tujuan, termasuk perdagangan dan investasi [1].

2.2.2 Cryptocurrency

Gambar 2. 2 Cryptocurrency[15]

Cryptocurrency adalah sebuah bentuk aset digital yang dikenal sebagai mata uang kripto, yang mengandalkan kriptografi yang kuat untuk menjaga keamanan dan validitas setiap transaksi keuangan. Selain itu, cryptocurrency juga memiliki sistem yang mengatur proses pembuatan unit baru untuk menghindari inflasi yang berlebihan. Sebagai media pertukaran,

cryptocurrency berfungsi sebagai alat untuk memverifikasi dan merekam transfer aset secara transparan dan terpercaya. [5][6]

2.2.3 Verus Coin

Verus Coin merupakan sebuah mata uang crypto yang dihasilkan dari proses penambangan crypto, penambangan dilakukan menggunakan algoritma verushash. Verus Coin adalah teknologi tanpa pengetahuan, proyek berorientasi privasi yang bekerja untuk menawarkan Public Blockchains as a Service (PBaaS). Verus Coin memperkenalkan algoritma konsensus baru yang disebut Proof of Power, algoritma 50% PoW / 50% PoS, yang bertujuan untuk mengatasi kelemahan pada sistem PoS lainnya [4].

2.2.4 Hash

Hash merupakan kode alfanumerik dengan panjang tetap yang digunakan untuk mewakili kata, pesan, atau data. Hash adalah sidik jari atau abstraksi data digital. Perbedaan antara hashing dan enkripsi adalah enkripsi dua arah, sedangkan hashing adalah enkripsi satu arah. Pada dasarnya, hash memiliki dua properti. a) Input yang sama selalu menghasilkan output yang sama. b) Tidak ada fungsi atau metode untuk mengubah output kembali ke input [16].

2.2.5 Hashrate

Hashrate adalah ukuran yang digunakan untuk menilai seberapa cepat komputer atau mesin penambangan cryptocurrency dapat menyelesaikan operasi perhitungan hash dalam satu detik. Proses hashing ini penting dalam verifikasi dan validasi transaksi dalam jaringan blockchain. Semakin tinggi hashrate, semakin efisien komputer atau mesin penambangan dalam menyelesaikan tugas, yang berarti mereka memiliki peluang lebih tinggi untuk memperoleh reward dalam bentuk cryptocurrency sebagai imbalan atas kontribusi mereka dalam memproses transaksi dan menjaga keamanan jaringan [7].

2.2.6 VerusHash

Gambar 2. 3 Verus Hash [17]

Algoritme hash dirancang untuk menurunkan hambatan penambangan bagi semua orang dan menciptakan jaringan terdistribusi secara alami. Penambangan verus coin dengan algoritma *VerusHash* saat ini merupakan algoritma khusus CPU. Proyek Verus bertujuan untuk membangun keamanan, privasi-sentris, dan keamanan merata pada mata uang kripto [4].

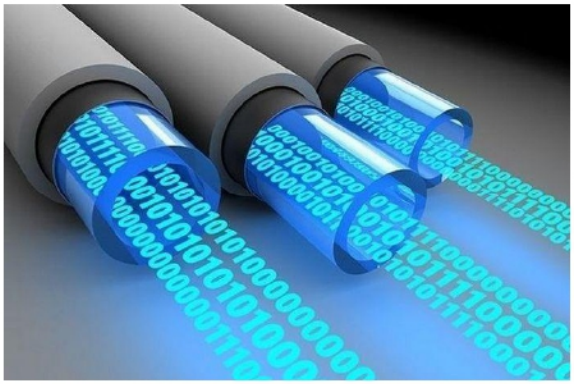
2.2.7 STB

Gambar 2. 4 STB (Set Top Box)[18]

Set Top Box (STB) adalah perangkat yang memiliki fungsi mengonversi sinyal digital menjadi gambar dan suara yang dapat ditampilkan pada televisi analog konvensional [19]. Namun, seiring perkembangan teknologi, STB juga dapat dimanfaatkan sebagai mini komputer seperti Raspberry Pi, yang memungkinkan pengguna untuk

menginstal sistem operasi. Salah satu opsi untuk STB adalah memasang sistem operasi Linux Armbian . Hal ini memungkinkan pengguna untuk menggunakan STB tidak hanya sebagai perangkat untuk menonton televisi, tetapi juga sebagai platform komputasi yang lebih serbaguna dengan berbagai kemungkinan aplikasi dan penggunaan[20].

2.2.8 Bandwidth



Gambar 2. 5 Bandwidth[21]

Bandwidth adalah istilah yang digunakan untuk mengukur jumlah maksimum data yang dapat ditransfer melalui koneksi internet dalam jangka waktu tertentu [22]. Secara sederhana, bandwidth dapat diartikan sebagai kapasitas data yang dapat dikirimkan atau diterima dalam satu waktu. Semakin besar bandwidth, semakin banyak data yang dapat diakses, diunduh, atau diunggah dengan cepat, sementara bandwidth yang lebih kecil dapat membatasi kecepatan dan jumlah data yang dapat diproses dalam waktu tertentu. Kecepatan dan kualitas koneksi internet sering kali tergantung pada seberapa besar bandwidth yang dimiliki oleh penyedia layanan atau infrastruktur jaringan yang digunakan [22].

2.2.9 CPU

Gambar 2. 6 CPU (Central Processing Unit)[23]

CPU (Central Processing Unit) adalah komponen utama dalam sebuah komputer, bertanggung jawab atas pengendalian dan pelaksanaan seluruh operasi yang dijalankan pada komputer. Fungsi utama CPU adalah menerima dan menjalankan perintah dari perangkat lunak (software) serta melakukan operasi matematika dan logika untuk memproses data. CPU bekerja dengan kecepatan tinggi dan berfungsi sebagai otak komputer, mengoordinasikan semua aktivitas dan memungkinkan komputer untuk melakukan berbagai tugas seperti menghitung, menyimpan data, menampilkan grafik, dan menjalankan aplikasi [24]. Tanpa CPU, komputer tidak akan dapat berfungsi dan tidak dapat menjalankan perintah atau melaksanakan tugas apa pun.

2.2.10 Haraka-512

Haraka 512 adalah sebuah fungsi Hash short-input (256 atau 512 bit) yang aman dan effisien, dirancang untuk bekerja sangat cepat pada CPU [2][3]. *Haraka 512* dirancang sebagai Hash Short Input yang dimana secara ekslusif mengkonsumsi satu potongan 512 bit dan menghasilkan 256 bit hasil hash. Memanfaatkan *Haraka 512*, Verushash membutuhkan input berapa saja guna menghasilkan hash 256 bit. Ini membuat verushash 256 bit aman untuk serangan komputasi kelasik dan 128 bit aman melawan komputer kuantum.

2.2.11 GPU

Gambar 2. 7 GPU[25]

Graphics Processing Unit (GPU) adalah prosesor yang terdiri dari banyak inti yang lebih kecil dan lebih khusus. Bekerja bersama, inti memberikan kinerja yang luar biasa karena tugas pemrosesan dapat dibagi dan ditangani di beberapa inti[26]. *GPU* digunakan untuk akelerasi dalam rendering 3D model *graphic*, yang dapat memberikan performa baik dari pada *CPU*.

2.2.12 Application Specific Integrated Circuit (ASIC)

Gambar 2. 8 ASIC[27]

Application Specific Integrated Circuit atau yang kita kenal *ASIC* dibuat khusus untuk melakukan penambangan beberapa jenis mata uang

Cryptocurrency yang dimana salah satu peminat terbanyak nya digunakan untuk menambang Bitcoin. Secara umum *ASIC* dikenal sebagai perangkat yang digunakan untuk melakukan proses penambangan mata uang digital [28]. ASIC terdiri dari beberapa jenis yang popular digunakan sebagai berikut:

- ASIC Antminer S9, Hashrate 14.0 TH/s, dengan daya 1372W
- ASIC Avalonminer 821, Hashrate 11.0 TH/s, dengan daya 1200W
- ASIC Antminer R4, Hashrate 8.4 TH/s, dengan daya 845W

Pada umumnya ASIC digunakan dalam melakukan penambangan Bitcoin [28]. ASIC tidak dapat melakukan penambangan verus coin, untuk saat ini verus coin support CPU,GPU,Mobile phone dan ARM[29].

2.2.13 Virtual Private Server (VPS)

Gambar 2. 9 VPS (Virtual Private Server)[30]

Virtual Private Server (VPS) adalah layanan yang menyediakan virtual computer dengan menerapkan teknologi virtualisasi. Meskipun satu server fisik digunakan oleh banyak pengguna, setiap VPS memiliki sumber daya (private) yang khusus dan terisolasi. Dengan menggunakan VPS, pengguna dapat memiliki kontrol lebih besar atas lingkungan server mereka, menginstal dan mengatur sistem operasi serta aplikasi sesuai kebutuhan mereka tanpa terganggu oleh pengguna lain pada server yang sama [31]. Hal ini membuat VPS menjadi pilihan populer bagi para pengembang, bisnis, dan individu

yang memerlukan fleksibilitas dan skalabilitas dalam mengelola proyek atau situs web mereka tanpa harus mengelola server fisik secara langsung.

2.2.14 Ccminer

CCMiner adalah salah satu perangkat lunak pertambangan cryptocurrency yang dirancang khusus untuk mengekstraksi atau "menambang" berbagai jenis koin kripto. Perangkat lunak ini menggunakan algoritma pemrosesan yang efisien untuk melakukan komputasi yang diperlukan dalam proses penambangan. Dengan CCMiner, para penambang dapat memanfaatkan kekuatan komputasi kartu grafis (GPU) mereka untuk mencari blok baru dan memvalidasi transaksi dalam jaringan blockchain, memungkinkan mereka untuk mendapatkan hadiah koin sebagai imbalan atas kontribusi mereka dalam memelihara keamanan dan konsensus jaringan.

2.2.15 Hellminer

Perangkat lunak penambangan kripto, seperti "Hellminer," merupakan program yang diciptakan khusus untuk melakukan proses penambangan koin kripto dengan memanfaatkan daya komputasi dari perangkat keras, seperti CPU atau kartu grafis (GPU). Program ini berfungsi untuk mengeksekusi algoritma kriptografi yang rumit dan memecahkan teka-teki matematis yang diperlukan dalam proses penambangan blok baru dalam jaringan blockchain. Dengan menggunakan perangkat lunak penambangan, para penambang dapat berkontribusi dalam memproses transaksi, mencari blok baru, dan menjaga keamanan serta konsensus dalam jaringan kripto, yang kemudian akan memberikan imbalan berupa koin kripto sebagai hasil dari upaya penambangan mereka.

2.2.16 Luckpool

Luckpool merupakan salah satu contoh dari banyak "pool" penambangan kripto yang ada. "Pool" penambangan adalah kelompok

penambang kripto yang bekerja bersama untuk menggabungkan daya komputasi mereka dengan tujuan mencari blok baru dan memperoleh imbalan koin yang ditambang. Dalam sebuah "pool," para penambang bekerja secara kolektif untuk memecahkan teka-teki matematis yang diperlukan dalam proses penambangan, dan jika salah satu dari mereka berhasil menemukan blok, imbalan yang diperoleh akan dibagi secara proporsional di antara seluruh anggota "pool." Hal ini memungkinkan para penambang dengan daya komputasi yang lebih kecil untuk tetap berpartisipasi dan mendapatkan penghasilan yang lebih stabil dari penambangan kripto.