Analisis Penerapan Kriptografi pada Masalah Keamanan Bitcoin

Regina Dionne Aurelia Hadiprodjo / 18219030
Program Studi Sistem dan Teknologi Informasi
Sekolah Teknik Elektro dan Informatika
Institut Teknologi Bandung, Jalan Ganesha 10 Bandung
E-mail (gmail): dionne.aurelia@gmail.com

***Abstrak*—Perkembangan teknologi telah membawa banyak perubahan dalam hidup manusia. Salah satu perubahan yang terjadi adalah perubahan dalam melakukan pembayaran atau transaksi. Salah satu jenis transaksi yang banyak diminati oleh masyarakat akhir-akhir ini adalah Bitcoin. Bitcoin merupakan sebuah *cryptocurrency* yang memanfaatkan teknologi *blockchain* dalam pencatatan data transaksinya serta fungsi hash dalam pengelolaan datanya. Fungsi hash yang biasa digunakan pada Bitcoin adalah fungsi SHA-256 dan penerapan fungsi hash dalam Bitcoin ditujukan untuk menjaga keamanan data-data transaksi yang tercatat pada *blockchain*. Meskipun demikian, seluruh aktivitas yang dilakukan secara *online* pastinya memiliki risiko untuk menghadapi serangan dari pihak yang tidak berwenang. Hal tersebut dapat menyebabkan operasional sistem terganggu dan bahkan menyebabkan kerugian secara finansial yang besar. Oleh karena itu, penulis akan membahas terkait keamanan dari Bitcoin serta peran kriptografi dalam mendukung aspek tersebut pada makalah ini.**

Kata Kunci—kriptografi, bitcoin, hash, blockchain, SHA-256

I. PENDAHULUAN

Perkembangan teknologi yang sangat pesat telah membawa berbagai perubahan dalam kehidupan manusia. Penggunaan internet untuk berbagai macam kegiatan telah menjadi hal yang sangat wajar. Salah satu contoh penerapan yang sedang menjadi tren akhir-akhir ini adalah sistem pembayaran dengan menggunakan mata uang digital dan salah satu contohnya adalah Bitcoin. Bitcoin merupakan *cryptocurrency* yang sedang banyak dibicarakan oleh masyarakat. Dengan teknologi tersebut, seseorang dapat melakukan pembayaran untuk transaksi *online*. Selain itu, Bitcoin juga banyak dijadikan sebagai investasi dengan memperjualbelikan Bitcoin.

Crypto-currency, seperti namanya, mengimplementasikan kriptografi untuk membangkitkan mata uang yang digunakan dan memvalidasi transaksi yang terjadi. Salah satu hal yang membedakan Bitcoin dengan *e-payment* lainnya adalah tidak adanya pihak ketiga seperti pada jaringan pembayaran *peer-to-peer* lainnya. Hal tersebut menjadi salah satu daya tarik dari Bitcoin karena biaya operasional menjadi lebih murah dan proses transaksi yang biasanya membutuhkan waktu yang lama akibat pemrosesan secara manual, menjadi lebih cepat. Meskipun demikian, keamanan dari data transaksi tetap terjamin karena seharusnya hanya pihak yang terlibat pada transaksi yang memiliki akses ke data tersebut. Pencatatan data transaksi kemudian dicatat pada sebuah *blockchain* yang merupakan sebuah buku besar yang bersifat terbuka dan terdesentralisasi.

Pembatasan akses hanya bagi *client-server* dari sebuah proses transaksi Bitcoin tidak berarti sistem tersebut benar-benar aman dari serangan *hacker*. Ancaman pembajakan oleh pihak yang tidak berwenang telah menjadi risiko bagi seluruh aktivitas yang dilakukan secara *online* sejak lama. Berdasarkan hasil studi pada tahun 2016, diperkirakan bahwa terdapat hingga 33% dari seluruh transaksi Bitcoin mengalami pembajakan. [1]

Pada makalah ini, akan dibahas terkait ancaman keamanan yang dapat terjadi pada proses transaksi Bitcoin dan metode kriptografi yang digunakan dalam pengamanan proses transaksi tersebut. Pada bagian II terdapat penjelasan definisi dari kriptografi, *blockchain*, fungsi hash, dan fungsi hash SHA-256. Pada bagian III terdapat pembahasan dari serangan yang biasa terjadi pada Bitcoin, implementasi fungsi hash SHA-256 pada Bitcoin, tingkat keamanan fungsi hash tersebut pada transaksi Bitcoin, serta alternatif kriptografi lainnya yang dapat diimplementasikan pada Bitcoin. Pada bagian IV terdapat kesimpulan dari makalah ini.

II. DASAR TEORI

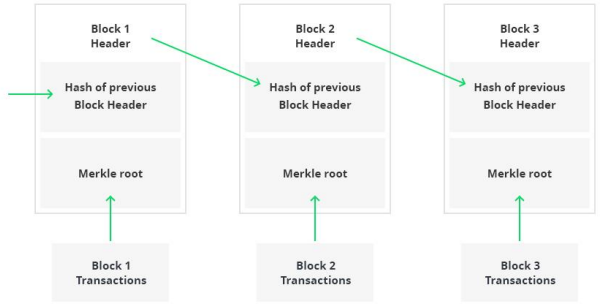
A. Kriptografi

Kriptografi berasal dari Bahasa Yunani "*cryptós*" dan "*gráphein*" yang secara harfiah berarti menulis secara tersembunyi untuk menyampaikan pesan-pesan yang perlu dijaga kerahasiaannya. [2] Dalam kata lain, kriptografi merupakan cabang ilmu pengetahuan yang membahas tentang cara pengubahan pesan agar pesan tersebut tidak dapat dibaca oleh pihak yang tidak berwenang. Terdapat empat layanan yang dapat disediakan oleh kriptografi, yaitu kerahasiaan pesan (*confidentiality*), keaslian pesan (*data integrity*), otentikasi pengirim dan penerima pesan (*authentication*), dan anti penyangkalan (*non repudiation*).

B. *Blockchain*

Blockchain merupakan sebuah buku besar (*ledger*) yang yang terdistribusi dan berfungsi untuk menyimpan data transaksi yang terjadi. [3] Teknologi *blockchain* terdiri dari sekelompok blok yang terhubung menjadi suatu rantai atau

rangkaian dan dihubungkan dengan menyimpan nilai *hash* dari blok sebelumnya.



Gambar 1. Ilustrasi *blockchain*

Sumber: https://mlsdev.com/blog/156-how-to-build-your-own-blockchain-architecture

Salah satu sifat *blockchain* adalah *immutable* yang artinya seluruh blok-blok data yang telah dimasukkan ke dalam *blockchain* sesuai dengan protokol yang ada, tidak dapat diganggu gugat oleh siapapun sehingga tidak mungkin untuk diubah atau dimanipulasi. Dengan demikian, jika terdapat perubahan pada salah satu data di dalam rangkaian blok tersebut, rangkaian tersebut akan terputus. Sifat tersebut menjamin bahwa keaslian data (*data integrity*) akan terjaga.

Sifat *blockchain* lainnya adalah penggunaan sistem desentralisasi. Tanpa adanya sistem terpusat atau *central authority* yang mengelola *blockchain*, validitas data pada sistem tersebut dilakukan secara konsensus dari mayoritas sistem yang ada (*consensus driven*). Pada Bitcoin, proses ini dikenal dengan *mining process*.

C. Fungsi Hash

Fungsi hash adalah fungsi yang mengkompresi pesan dengan ukuran berapapun menjadi suatu nilai yang berukuran pasti. Hasil dari fungsi hash biasa dikenal dengan istilah *message* digest. Sifat dari fungsi ini adalah *irreversible* sehingga pesan yang telah diproses dengan fungsi hash tidak dapat dikembalikan bentuknya seperti semula. Beberapa sifat dari fungsi hash adalah sebagai berikut.

1. *Collision Resistance*

   Sifat ini artinya akan sangat sulit untuk mendapatkan dua input a dan b yang hasil hash-nya adalah H(a) = H(b).

2. *Preimage resistance*

   Sifat ini artinya untuk sebuah output y, akan sulit mendapatkan input a yang hasil hash-nya adalah H(a) = y.

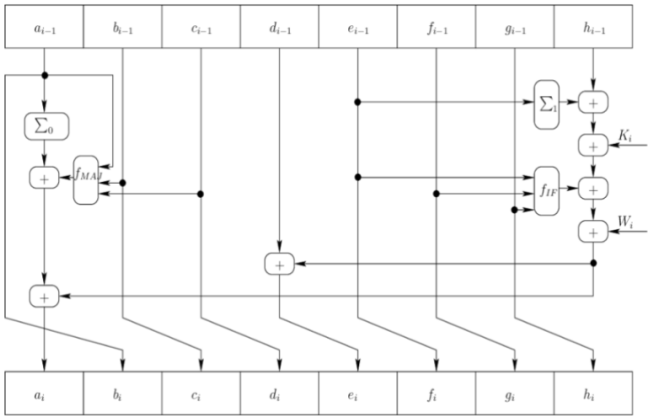
3. *Second preimage resistance*

   Sifat ini artinya jika terdapat output y dengan input a atau H(a) = y, akan sulit mendapatkan sebuah input b sehingga H(b) = y.

Perubahan kecil pada input ke fungsi hash akan menghasilkan nilai *message digest* yang sangat berbeda. Hal tersebut menyebabkan fungsi hash diimplementasikan untuk kriptografi, seperti pada tanda tangan digital.

D. SHA-256

Fungsi hash SHA-256 merupakan salah satu contoh implementasi dari fungsi hash. Fungsi SHA-256 memiliki ukuran *message digest* sepanjang 256 bit. Dasar dari algoritma ini adalah MD4 yang dibuat oleh Ronald L, Rivest dari MIT. Dalam pemrosesannya, terdapat enam operasi pada fungsi SHA-256 yang merupakan kombinasi penggunaan operasi AND, OR, XOR, dan pergeseran bit ke kanan (*shift right*). Berikut adalah ilustrasi dari proses transformasi fungsi SHA-256.



Gambar 2. Pemrosesan Fungsi SHA-256

Sumber: https://journal.unnes.ac.id/nju/index.php/jte/article/view/18628/9320

III. PEMBAHASAN

A. Permasalahan Keamanan pada Bitcoin secara Umum

Beberapa kemungkinan serangan keamanan pada sistem Bitcoin adalah sebagai berikut.

1. 51% *Attack*

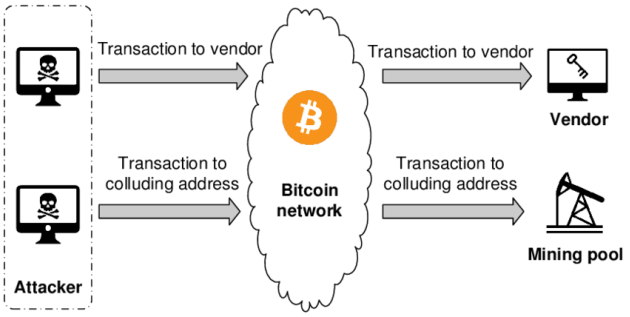
   Serangan ini dilakukan oleh sekelompok *miners* yang mengendalikan lebih dari 50% tingkat hash jaringan atau daya komputasi jaringan. Serangan 51% akan mencegah transaksi baru mendapatkan konfirmasi sehingga aktivitas pembayaran antara pengguna menjadi terhenti.

2. *Double-spending Attack*

   Double-spending adalah sebuah peristiwa saat sebuah *cryptocurrency* dapat digunakan dua kali atau lebih. Hal tersebut akan mengubah informasi yang tersimpan pada *blockchain*. Kondisi tersebut dapat mengakibatkan blok yang dimodifikasi memasuki *blockchain* dan pengguna yang berhasil melakukannya dapat melakukan klaim dari koin pada transaksi tersebut. Umumnya, penyerangan ini terjadi dengan mengirimkan informasi ke pengguna bahwa transaksinya belum terkonfirmasi. Jika pengguna

melakukan konfirmasi pada pesan palsu tersebut, *double-spending attack* terjadi.

Berikut adalah ilustrasi dari *double-spending attack.*



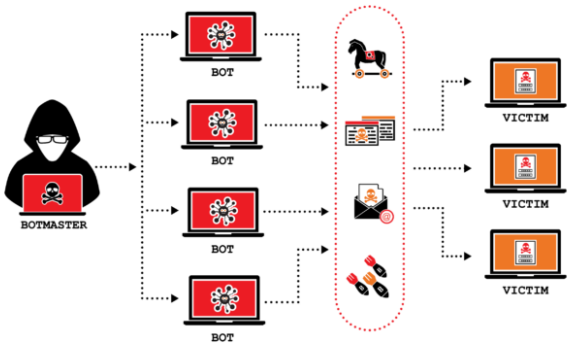
Gambar 3. Ilustrasi *Double-spending Attack*

Sumber: https://twigse.com/stream/what-is-bitcoin-double-spending

3. *Distributed Denial of Service* (DDoS) *Attack*

Serangan ini ditujukan untuk mengeksploitasi layanan dari suatu sistem. Hal tersebut dilakukan dengan mengirimkan *traffic* ke sebuah sistem dari kemampuan sistem tersebut. Dengan demikian, sistem menjadi kewalahan dalam menghadapi permintaan klien. Pada Bitcoin yang menerapkan teknologi *blockchain*, serangan seperti ini terjadi jika terdapat *spam transactions* yang dapat menyebabkan sistem menjadi tidak tersedia bagi pengguna yang benar-benar menggunakan sistem tersebut.

Berikut adalah ilustrasi dari *Distributed Denial of Service* (DDoS) *attack*.



Gambar 4. Ilustrasi *Distributed Denial of Service* (DDoS) *Attack*

Sumber: https://www.thesslstore.com/blog/what-is-a-ddos-attack/

4. *Attacks on the Wallet Software*

Aplikasi pada sisi pengguna seringkali disebut dengan *'wallets'* yang digunakan untuk mengelola Bitcoin yang dimiliki pengguna serta transaksi yang dilakukannya. Terdapat dua cara pengaksesan Bitcoin yang ditawarkan, yaitu melalui *online wallet services* atau aplikasi yang dapat di-*download* oleh pengguna. Secara umum, *online wallet services* lebih rentan terhadap serangan sehingga dibutuhkan proses enkripsi dan di-*back up* secara *offline*.

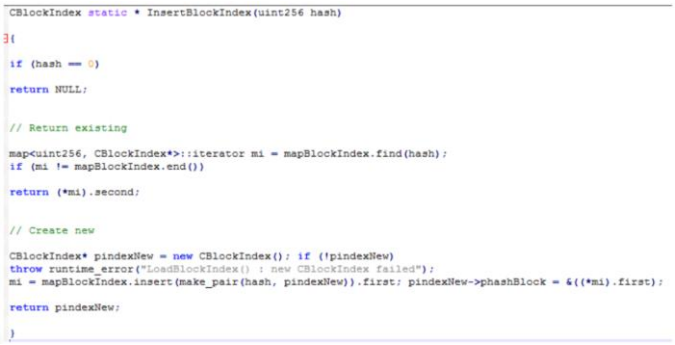
B. Penggunaan Fungsi Hash SHA-256 pada Bitcoin

Proses pembuatan bitcoin atau *bitcoin mining* terjadi jika sistem menemukan sebuah nilai yang panjangnya 32-bit, yang jika dihash bersama dengan data dari transaksi lainnya dengan fungsi hash yang standar akan memberikan hasil hash dengan jumlah angka nol sebanyak 60 atau lebih. Peristiwa ini sangat jarang terjadi sehingga dipercaya bahwa dibutuhkan komputasi yang sangat lama dan mahal. *Miners* atau sistem yang melakukan *mining* biasanya menjalankan *open source software* atau membeli *hardware* untuk melakukan proses tersebut secara efisien.

Hasil dari proses *mining* akan terhubung antar satu sama lain dan membentuk jaringan data-data yang unik. Jaringan data tersebut merupakan sebuah *blockchain* dan seluruh blok akan dipublikasikan melalui internet. Publikasi tersebut dimaksudkan agar *miner* lain tidak mencari blok yang sama sehingga mereka dapat mencari blok lain yang dapat menghasilkan Bitcoin. Proses *hashing* pada sistem *blockchain* yang digunakan oleh Bitcoin dilakukan dengan menggunakan algoritma SHA-256.

Hashing pada Bitcoin umumnya digunakan saat proses ekstraksi dan transaksi. Untuk proses transaksi, pengguna harus memberikan tanda tangan digital pada nilai hash dari transaksi yang bersangkutan untuk mengirimkannya ke pengguna lainnya. Jika seseorang dapat menemukan cara untuk membuat sebuah transaksi yang hasilnya sama dengan nilai hash awal, orang tersebut dapat menambahkan dirinya sebagai penerima koin dan mengambilnya.

Contoh kode yang digunakan untuk menangani transaksi yang terjadi adalah sebagai berikut.



```
CBlockIndex static * InsertBlockIndex(uint256 hash)
{
if (hash == 0)
return NULL;

// Return existing
map<uint256, CBlockIndex*>::iterator mi = mapBlockIndex.find(hash);
if (mi != mapBlockIndex.end())
return (*mi).second;

// Create new
CBlockIndex* pindexNew = new CBlockIndex(); if (!pindexNew)
throw runtime_error("LoadBlockIndex() : new CBlockIndex failed");
mi = mapBlockIndex.insert(make_pair(hash, pindexNew)).first; pindexNew->phashBlock = &((*mi).first);
return pindexNew;
}
```

Gambar 5. Implementasi Penanganan Transaksi Bitcoin dengan SHA-256

Sumber: https://www.icommercecentral.com/open-access/

Saat memproses transaksi dengan fungsi hash SHA-256, jika terdapat dua transaksi dengan nilai hash yang sama dan keduanya merujuk ke transaksi sebelumnya yang sama, maka kejadian tersebut mengindikasikan terjadinya *collision*. Namun, hal tersebut tidak mungkin terjadi karena pada sistem *blockchain* yang digunakan oleh Bitcoin dikarenakan blok-blok data transaksi membentuk rangkaian atau keterhubungan yang bersifat *time-stamped linear*. Setiap blok baru yang yang telah ditemukan pada proses *mining*, akan ditambahkan keterangan *timestamp* pada *header*-nya. Oleh karena itu, blok yang memiliki nilai hash yang sama serta merujuk pada transaksi sebelum yang sama, tidak akan ditambahkan. Proses tersebut diimplementasikan dengan kode sebagai berikut.

```
bool CTxMemPool::accept(CTxDB& txdb, CTransaction &tx, bool fCheckInputs, bool* pfMissingInputs)
{
/---/
//  Do we already have it?
uint256 hash = tx.GetHash();
{
LOCK(cs);
if (mapTx.count(hash)) return false;
}
if (fCheckInputs)
if (txdb.ContainsTx(hash)) return false;
/---/
```

Gambar 6. Implementasi Penanganan Blok Hasil *Mining* Bitcoin dengan SHA-256

Sumber: https://www.icommercecentral.com/open-access/

C. Keamanan Fungsi Hash SHA-256 pada Bitcoin

Beberapa kemungkinan serangan keamanan pada algoritma SHA-256 yang diimplementasikan pada Bitcoin adalah sebagai berikut.

1. *Collision*

   SHA-256 atau algoritma hash secara umum memiliki kemungkinan serangan, yaitu *collision*. Pencarian nilai *collision* untuk fungsi hash SHA-256 melalui *brute force attack* sangat mungkin karena jumlah nilai hash yang dapat dihasilkan terbatas, yaitu sebanyak 2256 hasil. Meskipun demikian, hal tersebut tidak menjadi kekhawatiran dalam implementasi SHA-256 karena dalam pencarian nilai hash untuk *collision* membutuhkan komputasi yang kompleks.

2. *Preimage Attack*

   Serangan ini ditujukan untuk mencari pesan asli dari sebuah nilai hash yang dihasilkan dari suatu fungsi hash. Berdasarkan pendapat Biryukov A. (2011), *preimage attack* yang ditujukan pada SHA-256 baru dapat berhasil pada algoritma SHA-256 yang terdiri dari 41-*step* dan masih aman untuk algoritma yang terdiri dari 64-*step*.

3. *Meet-in-the-middle Attack*

   Serangan ini dilakukan dengan memproses hash dari dua sisi pada saat yang bersamaan. Hal tersebut dilakukan untuk mempersempit nilai pesan asli yang mungkin hingga akhirnya pesan asli yang dihasilkan dari pemrosesan fungsi hash akan ditemukan di tengah. Mencari sebuah *nonce* dengan metode ini bukanlah hal yang sukar sehingga sangat mungkin dilakukan pada Bitcoin.

   Ancaman tersebut tetapi dapat diatasi karena sudah dilakukan implementasi SHA-256 sebanyak dua kali pada Bitcoin. Pada pemrosesan pertama, panjang pesannya tetap dan sepanjang 640 bits yang membutuhkan dua aplikasi untuk melakukan kompresi. Pada pemrosesan kedua, SHA-256 diaplikasikan ke pesan 256 bit. Hal tersebut tentunya menambah tingkat kesulitan dalam melakukan serangan ini.

   Dengan tingkat keamanan dari dua putaran fungsi hash SHA-256, *meet-in-the-middle attack* menjadi sulit dilakukan.

D. Alternatif Algoritma Kriptografi untuk Keamanan Bitcoin

Selain SHA-256, tedapat pula algoritma lain yang dapat digunakan pada Bitcoin, antara lain:

1. *Elliptic Curve Digital Signature Algorithm* (ECDSA)

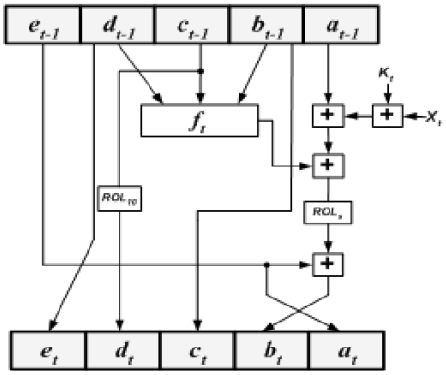
   Elliptic Curve Digital Signature Algorithm (ECDSA) adalah simulasi dari algoritma tanda tangan digital dengan implementasi *Elliptic Curve Cryptography* (ECC). ECC didasarkan pada persamaan $y^2 = x^3 + ax + b \pmod p$, ketika $4a^3 + 27b^2 \neq 0$. Berbeda dengan algoritma lainnya yang biasa tingkat kerumitannya bergantung pada logaritma diskrit biasa dan masalah faktorisasi integer, algoritma perkalian subeksponensial tidak terdapat pada masalah logaritma diskrit kurva elips. Oleh karena itu,

kekuatan per bit kunci algoritma yang menggunakan kurva elips akan lebih kuat secara substansial daripada algoritma biasa.

2. RIPEMD-160

Fungsi hash RIPEMD-160 merupakan turunan dari fungsi hash MD-4 yang telah diperkuat. Awal mulanya, fungsi RIPEMD dibuat dengan menurunkan MD-4 dan diperkuat dengan peningkatan pada pergeseran bit dan urutan karakter pada hasil nilai hash. RIPEMD kemudian dikembangkan lagi menjadi dua jenis, yaitu RIPEMD-128 dan RIPEMD-160.

Berikut adalah ilustrasi dari pemrosesan pesan pada fungsi RIPEMD-160.



Gambar 7. Implementasi Penanganan Blok Hasil *Mining* Bitcoin dengan SHA-256

Sumber: https://www.researchgate.net/figure/RIPEMD-160-operation-block-also-mentioned-as-Round_fig1_221908267

IV. KESIMPULAN DAN SARAN

Bitcoin merupakan *cryptocurrency* yang sedang banyak dibicarakan oleh masyarakat. Dengan teknologi tersebut, seseorang dapat melakukan pembayaran untuk transaksi *online*. *Crypto-currency*, seperti namanya, mengimplementasikan kriptografi untuk membangkitkan mata uang yang digunakan dan memvalidasi transaksi yang terjadi.

Dalam keberjalanan operasionalnya, Bitcoin memiliki ancaman terhadap berbagai jenis serangan oleh pihak yang tidak berwenang. Contoh serangan yang mungkin terjadi adalah 51% *Attack*, *Double-spending Attack*, *Distributed Denial of Service* (DDoS) *Attack*, *dan Attacks on the Wallet Software.*

Metode kriptografi yang sangat umum ditemui dalam implementasi Bitcoin adalah SHA-256. Fungsi hash SHA-256 digunakan untuk mengubah data transaksi sebelum disimpan pada *blockchain* atau buku besar yang berisi seluruh catatan transaksi pada Bitcoin.

Fungsi hash SHA-256 juga rentan terhadap beberapa jenis serangan, seperti *Collision*, *Preimage Attack*, dan *Meet-in-the-middle Attack*. Meskipun demikian, serangan-serangan tersebut membutuhkan komputasi yang kompleks dan mahal untuk dilakukan sehingga fungsi hash SHA-256 dinilai masih cukup aman dalam menjaga keamanan data pada Bitcoin.

Selain fungsi hash SHA-256, terdapat beberapa alternatif metode kriptografi yang dapat diimplementasikan pada Bitcoin, yaitu *Elliptic Curve Digital Signature Algorithm* (ECDSA) dan RIPEMD-160.

Bitcoin pastinya akan terus digunakan karena kemudahan serta keuntungan lain yang ditawarkan. Oleh karena itu, perlu dilakukan pembaharuan dan peningkatan sistem keamanannya secara terus menerus agar dapat beradaptasi untuk menghindari serangan yang pastinya juga terus berkembang variasinya.

UCAPAN TERIMA KASIH

Penulis ingin mengucapkan terima kasih kepada Tuhan Yang Maha Esa atas karunia-Nya sehingga penulis dapat menyelesaikan makalah ini, kepada Pak Rinaldi Munir sebagai dosen pengampu mata kuliah II4031 Kriptografi dan Koding yang mengajarkan penulis berbagai ilmu-ilmu penting yang penulis butuhkan untuk mengerti teori kriptografi, dan kepada teman-teman penulis yang mendukung dalam pembelajaran kriptografi serta pembuatan makalah ini, Leony dan Stella. Selain itu, penulis ingin mengucapkan terima kasih kepada orang-orang yang membahas terkait kriptografi melalui internet dan penulis ambil hasil karyanya sebagai referensi dalam pembuatan makalah ini karena telah membantu penulis dalam menambah wawasan mengenai topik yang penulis bawa di makalah ini.

REFERENCES

[1] Tandel S (2017) *Blockchain: overview, use cases and challenges.*

[2] Choiri, E. (2020). Pengertian Kriptografi, Sejarah & Jenis Algoritmanya. Diakses pada 23 Mei 2022, dari https://qwords.com/blog/pengertian-kriptografi/

[3] Narayanan, Bonneau, Felten, Miller, & Goldfeder (2016)

[4] Behnke, R. (2021). *How Blockchain DDoS Attacks Work*. Diakses pada 24 Mei 2022, dari https://halborn.com/how-blockchain-ddos-attacks-work/

[5] Bosselaers, A. (2012). *The hash function RIPEMD-160*. Diakses pada 23 Mei 2022, dari https://homes.esat.kuleuven.be/~bosselae/ripemd160.html

[6] Courtois N. , Grajek M. , and Naik R. (2014). *The Unreasonable Fundamental Incertitudes Behind Bitcoin Mining*. Diakses pada 23 Mei 2022, dari https://arxiv.org/pdf/1310.7935.pdf

[7] Frankenfield, J. (2022). *Double-Spending.* Diakses pada 23 Mei 2022, dari https://www.investopedia.com/terms/d/doublespending.asp#:~:text=Double%2Dspending%20occurs%20when%20someone,t%20adequately%20protected%20and%20secured

[8] Latifa, E. *Blockchain: Bitcoin Wallet Cryptography Security, Challenges and Countermeasures.* Diakses pada 25 Mei 2022, dari https://www.icommercecentral.com/open-access/blockchain-bitcoin-wallet-cryptography-security-challenges-and-countermeasures.php?aid=86561#29

[9] Nakamoto, S. *Bitcoin: A Peer-to-Peer Electronic Cash System.* Diakses pada 24 Mei 2022, dari https://bitcoin.org/bitcoin.pdf

[10] Vyas, C., Lunagaria, M. (2014). *Security Concerns and Issues for Bitcoin.* Diakses pada 25 Mei 2022, dari https://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.667.5197&rep=rep1&type=pdf

[11] Wang, X. (2019). *Research on ECDSA-Based Signature Algorithm in Blockchain*. Diakses pada 23 Mei 2022, dari https://www.researchgate.net/publication/342660617_Research_on_ECDSA-Based_Signature_Algorithm_in_Blockchain

PERNYATAAN

Dengan ini saya menyatakan bahwa makalah yang saya tulis ini adalah tulisan saya sendiri, bukan saduran, atau terjemahan dari makalah orang lain, dan bukan plagiasi.

Bandung, 25 Mei 2022

Regina Dionne Aurelia Hadiprodjo
18219030