Pemanfaatan *Blockchain* untuk Verifikasi Keaslian *Share* pada Skema Pembagian Data Rahasia

Ahmad Hasan Albana[1]
Program Studi Teknik Informatika
Sekolah Teknik Elektro dan Informatika
Institut Teknologi Bandung, Jl. Ganesha 10 Bandung 40132, Indonesia
[1]*ahmadalbana98@gmail.com,* [1]*13522041@std.stei.itb.ac.id*

***Abstract*—Skema Pembagian Rahasia adalah metode kriptografi untuk mendistribusikan rahasia kepada sekelompok partisipan, di mana rahasia hanya dapat direkonstruksi jika jumlah partisipan yang mencukupi menggabungkan bagian (*share*) mereka. Salah satu kerentanan utama dalam skema ini, seperti pada Shamir's Secret Sharing, adalah ketidakmampuan untuk memverifikasi apakah *share* yang diserahkan oleh partisipan saat fase rekonstruksi adalah asli atau palsu. Partisipan yang tidak jujur dapat menyerahkan *share* palsu untuk mengacaukan hasil rekonstruksi. Makalah ini mengusulkan pemanfaatan teknologi Blockchain sebagai buku besar (ledger) yang tidak dapat diubah (immutable) untuk menyimpan nilai *hash* dari setiap *share* saat fase distribusi. Dengan demikian, sebelum proses rekonstruksi dilakukan, keaslian *share* dapat diverifikasi dengan membandingkan *hash share* yang masuk dengan *hash* yang tersimpan di Blockchain. Pendekatan ini menjamin integritas proses rekonstruksi tanpa perlu mengungkapkan nilai *share* itu sendiri ke publik.**

***Index Terms*—*Blockchain*, *Hash*, Rekonstruksi Rahasia, Skema Pembagian Data Rahasia.**

I. Pendahuluan

Keamanan data merupakan aspek krusial dalam era digital. Salah satu teknik untuk mengamankan data yang sangat sensitif adalah dengan tidak mempercayakannya pada satu entitas saja. Skema Pembagian Data Rahasia, yang diperkenalkan oleh Adi Shamir pada tahun 1979, memungkinkan sebuah rahasia dibagi menjadi n bagian (*shares*), di mana minimal t bagian diperlukan untuk merekonstruksi rahasia tersebut (skema (t, n) threshold) [4].

Namun, skema standar Shamir memiliki kelemahan yang berupa asumsi bahwa setiap kunci yang digunakan untuk rekonstruksi data merupakan kunci yang benar. Dalam skenario nyata, mungkin untuk adanya penggunaan kunci yang salah sehingga akan menyebabkan rahasia gagal direkonstruksi [1].

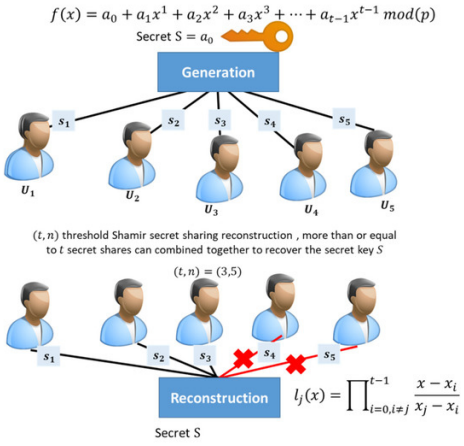
Di sisi lain, Blockchain menawarkan sifat *immutability* dan transparansi. Data yang telah masuk ke dalam blok yang valid sangat sulit untuk diubah [5]. Makalah ini mengusulkan penggunaan Blockchain sebagai media verifikasi publik. Ide dasarnya adalah menyimpan *hash* dari setiap *share* ke dalam Blockchain pada saat fase inisialisasi (pembagian rahasia).

Tujuan dari makalah ini adalah merancang mekanisme verifikasi integritas *share* menggunakan fungsi *hash* kriptografi dan teknologi Blockchain untuk mencegah serangan *share* palsu saat rekonstruksi rahasia.

II. Landasan Teori

A. Skema Ambang Shamir

Skema Ambang Shamir (*t, n*) adalah metode kriptografi untuk membagi sebuah data rahasia (S) menjadi beberapa bagian kunci yang dibagikan kepada sejumlah *n* partisipan sedemikian sehingga sembarang himpunan bagian yang terdiri dari *t* partisipan atau lebih dapat merekonstruksi S, tetapi jika kurang dari *t* maka S tidak dapat direkonstruksi [4]. Skema Ambang Shamir didasarkan pada persoalan Interpolasi Polinomial yang menyatakan bahwa untuk merekonstruksi suatu polinomial berderajat *n*, diperlukan minimal *n+1* buah titik koordinat yang unik.



Source: https://www.mdpi.com/1424-8220/22/1/331

Fig. 1. Skema Ambang Shamir

Skema Ambang Shamir diawali dengan pemilihan suatu angka prima yang lebih dari angka rahasia (S) dan banyak partisipan (*n*) yang digunakan sebagai modulus untuk membatasi operasi dalam bidang terbatas dan memastikan adanya invers untuk sembarang bilangan tidak nol. Untuk skema (*t, n*), akan dibuat suatu persamaan polinom acak berderajat *t-1* dengan S sebagai konstanta. Lalu, akan dibangkitkan *n* buah kunci yang berupa suatu titik unik pada polinom.

Proses rekonstruksi angka rahasia dilakukan dengan cara mensubstitusikan titik (kunci) pada persamaan polinom berderajat t dengan koefisien yang belum diketahui seperti berikut.

$$f(x) \equiv S + a_1 x + a_2 x^2 + \cdots + a_{t-1} x^{t-1} \pmod{p} \quad (1)$$

Lalu akan dicari nilai dari koefisien polinom dengan menggunakan penyelesaian Sistem Persamaan Linear. Adapun angka rahasia merupakan nilai konstanta pada persamaan polinom yang telah direkonstruksi.

Namun, skema standar Shamir memiliki kelemahan yang berupa asumsi bahwa setiap kunci yang digunakan untuk rekonstruksi data merupakan kunci yang benar. Dalam skenario nyata, mungkin untuk adanya penggunaan kunci yang salah sehingga akan menyebabkan rahasia gagal direkonstruksi [1].

B. Fungsi Hash

Fungsi hash kriptografi H adalah algoritma deterministik yang memetakan input data dengan panjang sembarang (*arbitrary length*) ke output data dengan panjang tetap (*fixed length*), yang disebut *digest* atau *hash value*.

$$H : \{0,1\}^* \rightarrow \{0,1\}^n$$

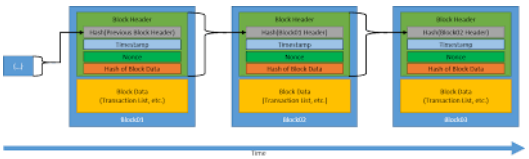
Dalam konteks verifikasi keaslian *share*, fungsi hash harus memenuhi tiga properti keamanan utama [3]:

1) **Pre-image Resistance (One-wayness):** Diberikan nilai hash h, secara komputasi tidak layak (*computationally infeasible*) untuk menemukan input m sedemikian rupa sehingga $H(m) = h$. Sifat ini menjamin bahwa nilai *share* asli tidak dapat dikembalikan dari nilai hash yang disimpan di publik.
2) **Second Pre-image Resistance:** Diberikan input m_1, sulit untuk menemukan input berbeda m_2 ($m_1 \neq m_2$) di mana $H(m_1) = H(m_2)$. Ini mencegah penyerang mengganti *share* asli dengan *share* lain yang memiliki hash sama.
3) **Collision Resistance:** Sulit untuk menemukan dua input sembarang m_1 dan m_2 yang berbeda sehingga $H(m_1) = H(m_2)$.

Algoritma seperti SHA-256 (Secure Hash Algorithm 256-bit) umum digunakan karena memiliki resistensi tabrakan yang kuat dan efek *avalanche*, di mana perubahan satu bit pada input akan mengubah output secara drastis.

C. Blockchain

Blockchain adalah buku besar terdistribusi (*distributed ledger*) yang bersifat terdesentralisasi, transparan, dan *immutable* (tidak dapat diubah) [4]. Struktur data blockchain terdiri dari rangkaian blok yang terurut secara kronologis.



Source: https://www.nist.gov/blockchain

Fig. 2. Visualisasi Blockchain

Setiap blok dalam rantai berisi referensi kriptografis ke blok sebelumnya, yang disebut *Previous Block Hash*.

$$H(Block_i) = H(Header_i + Data_i + H(Block_{i-1}))$$

Keterkaitan ini menyebabkan efek berantai saat dilakukan memodifikasi data pada blok i, menyebabkan hash pada blok berikutnya akan ikut berubah.

D. Smart Contract

Pada platform Blockchain generasi kedua seperti Ethereum, terdapat fitur *Smart Contract*. Ini adalah kode program yang tersimpan di dalam blockchain dan dieksekusi secara otomatis oleh seluruh node dalam jaringan ketika kondisi tertentu terpenuhi [2]. Dalam skema yang diusulkan, *Smart Contract* dapat bertindak sebagai verifikator otonom yang membandingkan hash dari *share* yang diserahkan dengan hash yang telah dicatat sebelumnya, tanpa intervensi pihak ketiga manuasia.

III. Metodologi

A. Fase Distribusi Kunci

Pada fase ini, sebuah entitas tepercaya (*Dealer*) melakukan langkah-langkah berikut:

1) **Pembangkitan Polinomial:** *Dealer* memilih rahasia S dan membentuk polinomial $f(x)$ berderajat $t-1$.
2) **Pembuatan Share:** *Dealer* menghitung n buah *share* (x_i, y_i) untuk $i = 1...n$.
3) **Hashing:** *Dealer* menghitung nilai hash dari setiap komponen y pada *share*:

   $$h_i = H(y_i || salt)$$

   Salt digunakan untuk mencegah serangan *brute-force* atau *rainbow table* karena ruang kunci y_i mungkin terbatas pada field p.
4) **Publikasi ke Blockchain:** Dealer mengirimkan transaksi ke Blockchain yang berisi daftar $\{ID_i, h_i\}$ untuk semua partisipan. Transaksi ini akan ditambang dan menjadi permanen.
5) **Distribusi Aman:** Dealer mengirimkan *share* (x_i, y_i) kepada partisipan i melalui saluran aman.

B. Fase Rekonstruksi Kunci

Ketika k partisipan ingin merekonstruksi rahasia:

1) Setiap partisipan menyerahkan *share* mereka (x_i, y_i') dan $salt$.
2) Mesin rekonstruksi (atau Smart Contract) menghitung hash dari input yang diterima:

   $$h_{calc} = H(y_i' || salt)$$

3) **Verifikasi:** Sistem mengambil nilai hash h_i yang tersimpan di Blockchain untuk ID partisipan tersebut.
4) **Validasi:**
   - Jika $h_{calc} == h_i$, maka *share* dinyatakan **ASLI**.
   - Jika $h_{calc} \neq h_i$, maka *share* dinyatakan **PALSU** dan dibuang dari proses rekonstruksi.
5) Jika jumlah *share* yang valid $\geq k$, maka interpolasi Lagrange dijalankan untuk mendapatkan S.

IV. HASIL DAN PEMBAHASAN

A. Hasil

1) Skenario Pengujian Pembangkitan Share (Dealing Phase): Pada skenario ini, sistem diuji untuk membagi sebuah rahasia (”SUPER_SECRET”) menjadi beberapa bagian (*shares*). Parameter yang digunakan adalah total share ($N = 5$) dan nilai ambang batas atau *threshold* ($K = 3$).

Hasil pengujian pada Gambar 3 menunjukkan bahwa sistem berhasil memproses input rahasia.

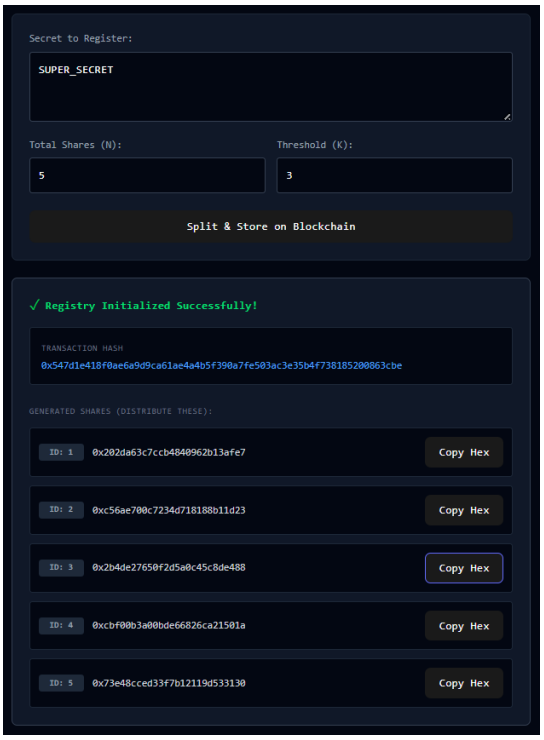


Fig. 3. Tampilan Antarmuka Hasil Pembangkitan Share dan Commit ke Blockchain

Berdasarkan hasil di atas, terdapat dua luaran utama:

1) **Transaction Hash:** Sistem menampilkan *Transaction Hash* (0x547d...) yang menandakan bahwa *commitment* (hash dari setiap share) telah berhasil disimpan ke dalam Smart Contract di jaringan uji Sepolia. Ini menjamin sifat *immutability* data verifikasi.
2) **Generated Shares:** Sistem menghasilkan 5 buah *share* dalam format Heksadesimal yang masing-masing memiliki ID unik (ID 1 hingga 5). Share ini diserahkan kepada partisipan secara *off-chain*.

2) Rekonstruksi dengan Share Mencukupi dan Valid: Pengujian dilakukan dengan memasukkan 3 *share* (sesuai threshold $K = 3$) yang valid, yaitu ID 1, ID 2, dan ID 3.

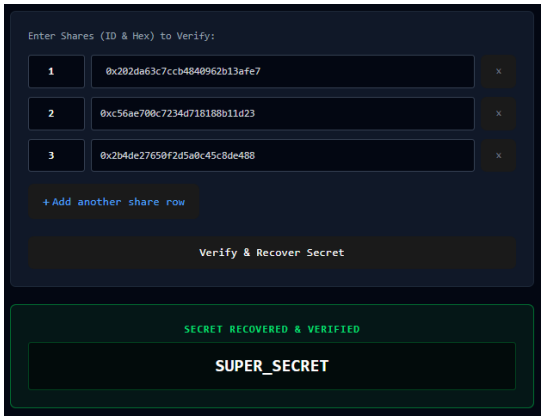


Fig. 4. Hasil Rekonstruksi Sukses dengan Share Valid

Sebagaimana terlihat pada Gambar 4, sistem berhasil memverifikasi validitas setiap share melalui fungsi `verifyShare` pada Smart Contract dan merekonstruksi rahasia asli ”SUPER_SECRET”. Hal ini membuktikan bahwa mekanisme interpolasi polinomial berjalan dengan benar ketika syarat $t \geq K$ terpenuhi.

3) Rekonstruksi dengan Share Tidak Mencukupi (Insufficient): Pengujian selanjutnya bertujuan menguji properti keamanan Shamir’s Secret Sharing, di mana rahasia tidak boleh bocor jika jumlah share kurang dari threshold. Percobaan dilakukan dengan hanya memasukkan 2 *share* (ID 1 dan ID 2), padahal threshold yang ditetapkan adalah 3.

Fig. 5. Kegagalan Rekonstruksi Akibat Share Kurang dari Threshold

Hasil pada Gambar 5 menunjukkan sistem menolak proses rekonstruksi dengan pesan *”Recovery Failed”*. Secara matematis, dua titik tidak cukup untuk merekonstruksi polinomial derajat 2 (yang membutuhkan minimal 3 titik), sehingga rahasia tetap aman dan tidak dapat dipulihkan.

4) Rekonstruksi dengan Deteksi Share Invalid (Tampered Share): Skenario ini merupakan fitur unggulan dari sistem yang dikembangkan, yaitu kemampuan mendeteksi *cheating* atau manipulasi data. Pengujian dilakukan dengan memasukkan 4 share (ID 1, 2, 3, dan 4), namun share milik ID 3 dimodifikasi sedikit nilainya (dimanipulasi).

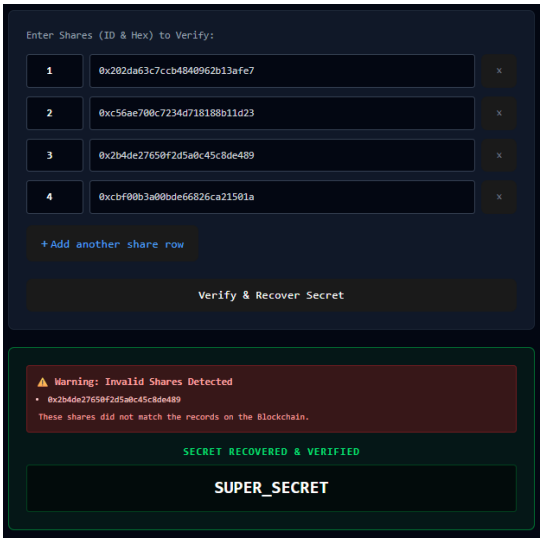


Fig. 6. Peringatan Deteksi Share Invalid dan Keberhasilan Rekonstruksi Parsial

Pada Gambar 6, terlihat input ID 3 memiliki nilai heksadesimal yang berakhiran `...489`, sedangkan nilai aslinya (pada Gambar 4) berakhiran `...488`.

B. Pembahasan

- **Deteksi Anomali:** Sistem menampilkan peringatan *"Warning: Invalid Shares Detected"* untuk ID 3. Ini terjadi karena saat fungsi `verifyShare` dipanggil, hash dari share yang dimanipulasi tidak cocok dengan hash yang tersimpan di Smart Contract.
- **Robustness:** Meskipun terdapat satu share palsu, sistem tetap berhasil memulihkan rahasia "SUPER_SECRET". Hal ini karena sistem secara otomatis membuang share yang invalid, dan menggunakan sisa share yang valid (ID 1, 2, dan 4). Karena jumlah share valid (3) masih memenuhi threshold ($K = 3$), rekonstruksi tetap dapat dilakukan.

Mekanisme ini membuktikan bahwa integrasi Blockchain efektif mencegah serangan partisipan jahat yang mencoba mengirimkan share palsu untuk mengacaukan hasil rekonstruksi.

V. Kesimpulan Saran

A. Kesimpulan

Berdasarkan tahap perancangan, implementasi, dan pengujian yang telah dilakukan pada sistem *Secret Share Registry* berbasis Blockchain, dapat ditarik beberapa kesimpulan sebagai berikut:

1) **Keberhasilan Integrasi Hybrid:** Penelitian ini berhasil mengimplementasikan sistem pembagian rahasia dengan pendekatan *hybrid*, yaitu menggabungkan efisiensi komputasi *off-chain* menggunakan algoritma *Shamir's Secret Sharing* dengan keamanan penyimpanan data verifikasi secara *on-chain* pada jaringan Ethereum (Sepolia Testnet).
2) **Mekanisme Verifikasi Integritas Share:** Penggunaan Smart Contract untuk menyimpan *commitment* (hash) dari setiap *share* terbukti efektif dalam menjamin integritas data. Berdasarkan pengujian, sistem mampu mendeteksi secara otomatis apabila terdapat partisipan yang menyerahkan *share* palsu atau telah dimanipulasi (*tampered share*), sehingga mencegah proses rekonstruksi yang menghasilkan data sampah.
3) **Ketahanan Sistem (Robustness):** Sistem menunjukkan tingkat ketersediaan (*availability*) yang tinggi. Dalam skenario serangan di mana terdapat *share* yang tidak valid, sistem tetap mampu merekonstruksi rahasia asli selama jumlah *share* valid yang tersisa masih memenuhi ambang batas (*threshold*) yang ditentukan ($t \geq K$).
4) **Transparansi dan Immutability:** Pemanfaatan teknologi Blockchain memberikan sifat kekekalan (*immutability*) pada data registri pembagian rahasia. Jejak distribusi *share* tercatat secara transparan melalui *Transaction Hash*, yang memungkinkan audit publik tanpa perlu mengungkapkan nilai rahasia itu sendiri.

B. Saran

Pengembangan sistem ini masih memiliki peluang untuk ditingkatkan. Berikut adalah beberapa saran untuk pengembangan penelitian selanjutnya:

1) **Optimasi Biaya Gas:** Saat ini, penyimpanan array ID dan Hash di *mainnet* Ethereum membutuhkan biaya gas yang cukup tinggi. Penelitian selanjutnya disarankan untuk mengevaluasi penggunaan solusi *Layer-2* (seperti Polygon atau Arbitrum) untuk menekan biaya transaksi tanpa mengorbankan keamanan.
2) **Desentralisasi Dealer:** Pada sistem saat ini, peran *Dealer* masih bersifat terpusat. Pengembangan selanjutnya dapat menerapkan protokol *Distributed Key Generation* (DKG) agar tidak ada satu entitas tunggal yang mengetahui rahasia utuh sejak awal proses.
3) **Dukungan Tipe Data Dinamis:** Implementasi saat ini berfokus pada rahasia berbasis teks atau string heksadesimal. Sistem dapat dikembangkan lebih lanjut untuk mendukung pembagian dan verifikasi file biner (seperti dokumen PDF atau gambar) secara langsung melalui antarmuka pengguna, dengan tetap menjaga efisiensi penyimpanan *on-chain*.

VI. Ucapan Terima Kasih

Puji syukur penulis panjatkan kepada Tuhan Yang Maha Esa yang telah memberikan karunia, sehingga penulis dapat Makalah IF4020 Kriptografi – Sem. II Tahun 2025/2026 menyelesaikan makalah yang berjudul "Pemanfaatan *Blockchain* untuk Verifikasi Keaslian Share pada Skema Pembagian Data Rahasia" yang dapat selesai tepat pada waktunya. Tak lupa juga penulis mengucapkan terima kasih kepada Bapak Dr. Ir. Rinaldi, M.T yang telah membimbing pada mata kuliah IF4020 Kriptografi. Terakhir, penulis mengucapkan terima kasih kepada orang tua, keluarga, dan seluruh pihak yang membantu penulis dalam menyelesaikan makalah ini.

REFERENCES

[1] Martin Tompa & Heather Woll, "How to Share a Secret with Cheaters", https://scispace.com/pdf/how-to-share-a-secret-with-cheaters-4l31u4167l.pdf, diakses 30 Desember 2025.

[2] Mohamed Imran Zacky, Syahri Helmi, dan Isadora Della Cella, "Smart Contracts on the Blockchain: Design, Use Cases, and Prospects", https://journal.pandawan.id/b-front/article/download/363/298.pdf

[3] Phillip Rogaway Thomas Shrimpton, "Cryptographic Hash-Function Basics: Definitions, and Separations for Preimage Resistance, and Collision Resistance", https://link.springer.com/content/pdf/10.1007/978-3-540-25937-4_24.pdf, diakses 30 Desember 2025.

[4] Rinaldi Munir, "Skema Pembagian Data Rahasia (*Secret Sharing Scheme*)", https://informatika.stei.itb.ac.id/ rinaldi.munir/Kriptografi/2025-2026/37-Skema-Pembagian-Data-Rahasia-2025.pdf, diakses 30 Desember 2025.

[5] Shi Dong, Khushnood Abbas, Meixi Li, dan Joarder Kamruzzaman, "Blockchain technology and application: an overview", https://pmc.ncbi.nlm.nih.gov/articles/PMC10703090/pdf/peerj-cs-09-1705.pdf, diakses 30 Desember 2025.

APPENDIX

A. Repositori GitHub

Kode lengkap implementasi Skema Pembagian Data Rahasia dengan Kunci Multilevel tersedia di repositori GitHub:

GitHub Repository:
https://github.com/Bana-man/Secret-Shares-Blockchain

B. Video Penjelasan Kode Program

Berikut merupakan video penjelasan makalah:

Youtube:
https://youtube.com/playlist?list=PLZHjGSNAZck5IRRsaz_qYaux11nap3XQU&si=TiBaaqUlIoTXl73A