

# REKONSTRUKSI HISTORIS, ANALISIS MATEMATIS, DAN IMPLIKASI PENDIDIKAN BITCOIN DALAM TRANSFORMASI SISTEM KEUANGAN DIGITAL GLOBAL

Oleh:

**Sandhy Duhita Mauladany Santoso<sup>1</sup>**

**Ani Afifah<sup>2</sup>**

**Supriyo<sup>3</sup>**

Universitas PGRI Wiranegara

Alamat: JL. Ki Hajar Dewantara No.27-29, Tembokrejo, Kec. Purworejo, Kota  
Pasuruan, Jawa Timur (67118).

Korespondensi Penulis: [sandhyduhitamauladany@gmail.com](mailto:sandhyduhitamauladany@gmail.com), [fifa.ani@gmail.com](mailto:fifa.ani@gmail.com),  
[supriyompd@yahoo.com](mailto:supriyompd@yahoo.com).

***Abstract.** This study reconstructs the historical development, mathematical architecture, and educational implications of Bitcoin as a decentralized digital financial system. Using a qualitative descriptive approach supported by an extensive literature review, this research explores the emergence of Bitcoin following the 2008 global financial crisis, the publication of its whitepaper, and the evolution of blockchain technology as a distributed ledger system. The mathematical foundations examined include modular arithmetic, cryptographic hash functions, SHA-256, Proof of Work consensus mechanism, Elliptic Curve Cryptography, and the ECDSA digital signature scheme. Furthermore, statistical analysis such as variance and standard deviation is discussed to interpret price volatility and financial risk. The findings reveal that Bitcoin is not merely a technological innovation but a paradigm shift in trust architecture, replacing institutional trust with mathematical verification. Its scarcity model, decentralized validation process, and halving mechanism create a predictable monetary supply system. From an educational perspective, the integration of Bitcoin concepts into mathematics learning enhances students' understanding of abstract theories through real-world digital applications. The*

# REKONSTRUKSI HISTORIS, ANALISIS MATEMATIS, DAN IMPLIKASI PENDIDIKAN BITCOIN DALAM TRANSFORMASI SISTEM KEUANGAN DIGITAL GLOBAL

*study concludes that mathematical literacy and cryptographic comprehension are essential in understanding the sustainability and future trajectory of digital financial ecosystems.*

**Keywords:** *Bitcoin, Blockchain, Cryptography, Digital Finance, Mathematics Education.*

**Abstrak.** Penelitian ini merekonstruksi perkembangan historis, struktur matematis, serta implikasi pendidikan dari Bitcoin sebagai sistem keuangan digital terdesentralisasi. Metode yang digunakan adalah deskriptif kualitatif berbasis studi literatur komprehensif yang mencakup jurnal ilmiah, buku akademik, dan dokumen resmi whitepaper. Pembahasan meliputi kemunculan Bitcoin pasca krisis finansial global 2008, perkembangan teknologi blockchain, serta transformasi paradigma kepercayaan dalam sistem moneter modern. Analisis matematis mencakup aritmetika modulo, fungsi hash kriptografis SHA-256, mekanisme konsensus Proof of Work, kriptografi kurva eliptik, dan algoritma tanda tangan digital ECDSA. Selain itu, pendekatan statistik seperti varians dan simpangan baku digunakan untuk menjelaskan volatilitas harga dan tingkat risiko investasi. Hasil penelitian menunjukkan bahwa Bitcoin bukan sekadar inovasi teknologi, melainkan perubahan struktur ekonomi berbasis validasi matematis. Dari perspektif pendidikan, integrasi konsep Bitcoin dalam pembelajaran matematika mampu meningkatkan pemahaman siswa terhadap teori abstrak melalui aplikasi nyata di dunia digital. Kesimpulannya, literasi matematika dan pemahaman kriptografi menjadi fondasi penting dalam memahami keberlanjutan serta arah masa depan sistem keuangan digital global.

**Kata Kunci:** Bitcoin, Blockchain, Kriptografi, Keuangan Digital, Pendidikan Matematika.

## LATAR BELAKANG

Perkembangan revolusi industri 4.0 telah mendorong transformasi besar dalam sistem ekonomi global. Digitalisasi keuangan melahirkan berbagai inovasi, salah satunya adalah Bitcoin. Bitcoin diperkenalkan pada tahun 2008 melalui dokumen whitepaper oleh Satoshi Nakamoto sebagai respons terhadap krisis finansial global yang mengungkap

kelemahan sistem perbankan terpusat.<sup>1</sup> Sistem ini menawarkan mekanisme peer-to-peer electronic cash tanpa otoritas pusat.<sup>2</sup> Keunikan Bitcoin terletak pada struktur desentralisasi, transparansi transaksi melalui blockchain, serta sistem verifikasi berbasis kriptografi. Selain sebagai alat transaksi, Bitcoin berkembang menjadi aset investasi digital dengan tingkat volatilitas tinggi. Fenomena ini menarik untuk dikaji secara matematis dan pedagogis karena seluruh mekanisme keamanannya berbasis teori bilangan, probabilitas, dan statistik. Penelitian ini bertujuan menganalisis dimensi historis, matematis, dan implikasi pembelajaran dari Bitcoin dalam konteks transformasi keuangan global.

Perkembangan revolusi industri 4.0 telah mendorong transformasi besar dalam sistem ekonomi global. Digitalisasi keuangan melahirkan berbagai inovasi, salah satunya adalah Bitcoin. Bitcoin diperkenalkan pada tahun 2008 melalui dokumen whitepaper oleh Satoshi Nakamoto sebagai respons terhadap krisis finansial global yang mengungkap kelemahan sistem perbankan terpusat. Sistem ini menawarkan mekanisme peer-to-peer electronic cash tanpa otoritas pusat.<sup>3</sup> Keunikan Bitcoin terletak pada struktur desentralisasi, transparansi transaksi melalui blockchain, serta sistem verifikasi berbasis kriptografi. Selain sebagai alat transaksi, Bitcoin berkembang menjadi aset investasi digital dengan tingkat volatilitas tinggi. Fenomena ini menarik untuk dikaji secara matematis dan pedagogis karena seluruh mekanisme keamanannya berbasis teori bilangan, probabilitas, dan statistik. Penelitian ini bertujuan menganalisis dimensi historis, matematis, dan implikasi pembelajaran dari Bitcoin dalam konteks transformasi keuangan global.

Perkembangan revolusi industri 4.0 telah mendorong transformasi besar dalam sistem ekonomi global. Digitalisasi keuangan melahirkan berbagai inovasi, salah satunya adalah Bitcoin. Bitcoin diperkenalkan pada tahun 2008 melalui dokumen whitepaper oleh Satoshi Nakamoto sebagai respons terhadap krisis finansial global yang mengungkap kelemahan sistem perbankan terpusat. Sistem ini menawarkan mekanisme peer-to-peer electronic cash tanpa otoritas pusat. Keunikan Bitcoin terletak pada struktur

---

<sup>1</sup> Usman W Chohan, "A History of Bitcoin 5 Th February, 2022 1," n.d., <https://ssrn.com/abstract=3047875>.

<sup>2</sup> Satoshi Nakamoto, "Bitcoin: A Peer-to-Peer Electronic Cash System," n.d., <https://ssrn.com/abstract=3440802>.

<sup>3</sup> Nakamoto.

# REKONSTRUKSI HISTORIS, ANALISIS MATEMATIS, DAN IMPLIKASI PENDIDIKAN BITCOIN DALAM TRANSFORMASI SISTEM KEUANGAN DIGITAL GLOBAL

desentralisasi, transparansi transaksi melalui blockchain, serta sistem verifikasi berbasis kriptografi. Selain sebagai alat transaksi, Bitcoin berkembang menjadi aset investasi digital dengan tingkat volatilitas tinggi. Fenomena ini menarik untuk dikaji secara matematis dan pedagogis karena seluruh mekanisme keamanannya berbasis teori bilangan, probabilitas, dan statistik. Penelitian ini bertujuan menganalisis dimensi historis, matematis, dan implikasi pembelajaran dari Bitcoin dalam konteks transformasi keuangan global.

Perkembangan revolusi industri 4.0 telah mendorong transformasi besar dalam sistem ekonomi global. Digitalisasi keuangan melahirkan berbagai inovasi, salah satunya adalah Bitcoin. *Bitcoin is a collection of concepts and technologies that form the basis of a digital money ecosystem.*<sup>4</sup> Bitcoin diperkenalkan pada tahun 2008 melalui dokumen whitepaper oleh Satoshi Nakamoto sebagai respons terhadap krisis finansial global yang mengungkap kelemahan sistem perbankan terpusat. Sistem ini menawarkan mekanisme peer-to-peer electronic cash tanpa otoritas pusat. Keunikan Bitcoin terletak pada struktur desentralisasi, transparansi transaksi melalui blockchain, serta sistem verifikasi berbasis kriptografi. Selain sebagai alat transaksi, Bitcoin berkembang menjadi aset investasi digital dengan tingkat volatilitas tinggi.<sup>5</sup> Fenomena ini menarik untuk dikaji secara matematis dan pedagogis karena seluruh mekanisme keamanannya berbasis teori bilangan, probabilitas, dan statistik. Penelitian ini bertujuan menganalisis dimensi historis, matematis, dan implikasi pembelajaran dari Bitcoin dalam konteks transformasi keuangan global.

## KAJIAN TEORITIS

Secara teoritis, Bitcoin dibangun atas konsep kriptografi modern. Fungsi hash SHA-256 menghasilkan representasi digital unik sepanjang 256-bit yang bersifat satu arah. Artinya, sangat sulit mengembalikan data asli dari hasil hash tersebut. Mekanisme

---

<sup>4</sup> Andreas M Antonopoulos, "Bitcoin PROGRAMMING THE OPEN BLOCKCHAIN," n.d., [www.EBooksWorld.ir](http://www.EBooksWorld.ir).

<sup>5</sup> Anoop S Kumar, "Volume 40, Issue 3 Testing Safe Haven Property of Bitcoin and Gold during Covid-19 : Evidence from Multivariate GARCH Analysis," 2020.

Proof of Work mengharuskan penambang menyelesaikan persoalan komputasi dengan mencari nilai nonce yang memenuhi tingkat kesulitan tertentu.<sup>6</sup> Proses ini berbasis probabilitas dan membutuhkan daya komputasi tinggi. Selain itu, keamanan transaksi dijamin oleh Elliptic Curve Cryptography menggunakan algoritma ECDSA. Kurva eliptik memungkinkan pembentukan pasangan kunci publik dan privat dengan tingkat keamanan tinggi namun efisiensi komputasi yang baik.<sup>7</sup> Dalam ekonomi, teori kelangkaan digital membatasi suplai maksimum 21 juta koin. Setiap 210.000 blok terjadi peristiwa halving yang mengurangi imbalan penambangan. Model ini menciptakan sistem moneter dengan inflasi terkendali dan suplai terprediksi.

Secara teoritis, Bitcoin dibangun atas konsep kriptografi modern. Fungsi hash SHA-256 menghasilkan representasi digital unik sepanjang 256-bit yang bersifat satu arah. Artinya, sangat sulit mengembalikan data asli dari hasil hash tersebut. Mekanisme Proof of Work mengharuskan penambang menyelesaikan persoalan komputasi dengan mencari nilai nonce yang memenuhi tingkat kesulitan tertentu. Proses ini berbasis probabilitas dan membutuhkan daya komputasi tinggi. Selain itu, keamanan transaksi dijamin oleh Elliptic Curve Cryptography menggunakan algoritma ECDS. Kurva eliptik memungkinkan pembentukan pasangan kunci publik dan privat dengan tingkat keamanan tinggi namun efisiensi komputasi yang baik. Dalam ekonomi, teori kelangkaan digital membatasi suplai maksimum 21 juta koin. Setiap 210.000 blok terjadi peristiwa halving yang mengurangi imbalan penambangan. Model ini menciptakan sistem moneter dengan inflasi terkendali dan suplai terprediksi.

Secara teoritis, Bitcoin dibangun atas konsep kriptografi modern. Fungsi hash SHA-256 menghasilkan representasi digital unik sepanjang 256-bit yang bersifat satu arah. Artinya, sangat sulit mengembalikan data asli dari hasil hash tersebut. Mekanisme Proof of Work mengharuskan penambang menyelesaikan persoalan komputasi dengan mencari nilai nonce yang memenuhi tingkat kesulitan tertentu. Proses ini berbasis probabilitas dan membutuhkan daya komputasi tinggi. Selain itu, keamanan transaksi dijamin oleh Elliptic Curve Cryptography menggunakan algoritma ECDSA. Kurva eliptik

---

<sup>6</sup> Arthur Gervais et al., "On the Security and Performance of Proof of Work Blockchains," *Proceedings of the ACM Conference on Computer and Communications Security* 24-28-October-2016 (October 24, 2016): 3–16, <https://doi.org/10.1145/2976749.2978341>.

<sup>7</sup> Neal Koblitz, Alfred Menezes, and Scott Vanstone, "The State of Elliptic Curve Cryptography," *Designs, Codes and Cryptography*, vol. 19, 2000.

# REKONSTRUKSI HISTORIS, ANALISIS MATEMATIS, DAN IMPLIKASI PENDIDIKAN BITCOIN DALAM TRANSFORMASI SISTEM KEUANGAN DIGITAL GLOBAL

memungkinkan pembentukan pasangan kunci publik dan privat dengan tingkat keamanan tinggi namun efisiensi komputasi yang baik. Dalam ekonomi, teori kelangkaan digital membatasi suplai maksimum 21 juta koin. Setiap 210.000 blok terjadi peristiwa halving yang mengurangi imbalan penambangan. Model ini menciptakan sistem moneter dengan inflasi terkendali dan suplai terprediksi.

Secara teoritis, Bitcoin dibangun atas konsep kriptografi modern. Fungsi hash SHA-256 menghasilkan representasi digital unik sepanjang 256-bit yang bersifat satu arah. Artinya, sangat sulit mengembalikan data asli dari hasil hash tersebut. Mekanisme Proof of Work mengharuskan penambang menyelesaikan persoalan komputasi dengan mencari nilai nonce yang memenuhi tingkat kesulitan tertentu. Proses ini berbasis probabilitas dan membutuhkan daya komputasi tinggi. Selain itu, keamanan transaksi dijamin oleh Elliptic Curve Cryptography menggunakan algoritma ECDSA. Kurva eliptik memungkinkan pembentukan pasangan kunci publik dan privat dengan tingkat keamanan tinggi namun efisiensi komputasi yang baik. Dalam ekonomi, teori kelangkaan digital membatasi suplai maksimum 21 juta koin. Setiap 210.000 blok terjadi peristiwa halving yang mengurangi imbalan penambangan. Model ini menciptakan sistem moneter dengan inflasi terkendali dan suplai terprediksi.<sup>8</sup>

## METODE PENELITIAN

Penelitian ini menggunakan metode deskriptif kualitatif berbasis studi literatur. Data dikumpulkan melalui analisis dokumen ilmiah, buku referensi kriptografi, serta artikel ekonomi digital. Proses analisis dilakukan melalui reduksi data, klasifikasi tematik, dan interpretasi konseptual. Pendekatan ini memungkinkan eksplorasi mendalam terhadap hubungan antara struktur matematis dan implikasi ekonomi Bitcoin. Validitas data dijaga melalui triangulasi sumber serta perbandingan lintas referensi akademik. Penelitian ini menggunakan metode deskriptif kualitatif berbasis studi literatur. Data dikumpulkan melalui analisis dokumen ilmiah, buku referensi kriptografi, serta artikel

---

<sup>8</sup> Sarah Underwood, "Blockchain beyond Bitcoin," *Communications of the ACM* 59, no. 11 (October 28, 2016): 15–17, <https://doi.org/10.1145/2994581>.

ekonomi digital. Proses analisis dilakukan melalui reduksi data, klasifikasi tematik, dan interpretasi konseptual. Pendekatan ini memungkinkan eksplorasi mendalam terhadap hubungan antara struktur matematis dan implikasi ekonomi Bitcoin. Validitas data dijaga melalui triangulasi sumber serta perbandingan lintas referensi akademik.

Penelitian ini menggunakan metode deskriptif kualitatif berbasis studi literatur. Data dikumpulkan melalui analisis dokumen ilmiah, buku referensi kriptografi, serta artikel ekonomi digital. Proses analisis dilakukan melalui reduksi data, klasifikasi tematik, dan interpretasi konseptual. Pendekatan ini memungkinkan eksplorasi mendalam terhadap hubungan antara struktur matematis dan implikasi ekonomi Bitcoin. Validitas data dijaga melalui triangulasi sumber serta perbandingan lintas referensi akademik. Penelitian ini menggunakan metode deskriptif kualitatif berbasis studi literatur. Data dikumpulkan melalui analisis dokumen ilmiah, buku referensi kriptografi, serta artikel ekonomi digital. Proses analisis dilakukan melalui reduksi data, klasifikasi tematik, dan interpretasi konseptual. Pendekatan ini memungkinkan eksplorasi mendalam terhadap hubungan antara struktur matematis dan implikasi ekonomi Bitcoin. Validitas data dijaga melalui triangulasi sumber serta perbandingan lintas referensi akademik.

## **HASIL DAN PEMBAHASAN**

Hasil penelitian menunjukkan bahwa Bitcoin merepresentasikan integrasi antara matematika, teknologi, dan ekonomi. Volatilitas harga dapat diukur menggunakan rumus simpangan baku  $\sigma = \sqrt{(\sum(x-\mu)^2 / n)}$ . Nilai simpangan baku yang tinggi menunjukkan fluktuasi ekstrem yang menjadi karakteristik pasar kripto. Namun demikian, adopsi institusional oleh perusahaan global meningkatkan legitimasi sebagai aset lindung nilai digital. Dari perspektif pendidikan, konsep Bitcoin dapat digunakan sebagai media pembelajaran statistika, teori bilangan, dan kriptografi. Siswa dapat memahami bagaimana konsep abstrak diterapkan dalam sistem nyata yang digunakan secara global. Implikasi ini menunjukkan potensi integrasi teknologi digital dalam kurikulum matematika modern.

Hasil penelitian menunjukkan bahwa Bitcoin merepresentasikan integrasi antara matematika, teknologi, dan ekonomi. Volatilitas harga dapat diukur menggunakan rumus simpangan baku  $\sigma = \sqrt{(\sum(x-\mu)^2 / n)}$ . Nilai simpangan baku yang tinggi menunjukkan fluktuasi ekstrem yang menjadi karakteristik pasar kripto. Namun demikian, adopsi

## **REKONSTRUKSI HISTORIS, ANALISIS MATEMATIS, DAN IMPLIKASI PENDIDIKAN BITCOIN DALAM TRANSFORMASI SISTEM KEUANGAN DIGITAL GLOBAL**

institusional oleh perusahaan global meningkatkan legitimasi sebagai aset lindung nilai digital. Dari perspektif pendidikan, konsep Bitcoin dapat digunakan sebagai media pembelajaran statistika, teori bilangan, dan kriptografi. Siswa dapat memahami bagaimana konsep abstrak diterapkan dalam sistem nyata yang digunakan secara global. Implikasi ini menunjukkan potensi integrasi teknologi digital dalam kurikulum matematika modern.

Hasil penelitian menunjukkan bahwa Bitcoin merepresentasikan integrasi antara matematika, teknologi, dan ekonomi. Volatilitas harga dapat diukur menggunakan rumus simpangan baku  $\sigma = \sqrt{(\sum(x-\mu)^2 / n)}$ . Nilai simpangan baku yang tinggi menunjukkan fluktuasi ekstrem yang menjadi karakteristik pasar kripto. Namun demikian, adopsi institusional oleh perusahaan global meningkatkan legitimasi sebagai aset lindung nilai digital. Dari perspektif pendidikan, konsep Bitcoin dapat digunakan sebagai media pembelajaran statistika, teori bilangan, dan kriptografi. Siswa dapat memahami bagaimana konsep abstrak diterapkan dalam sistem nyata yang digunakan secara global. Implikasi ini menunjukkan potensi integrasi teknologi digital dalam kurikulum matematika modern.

Hasil penelitian menunjukkan bahwa Bitcoin merepresentasikan integrasi antara matematika, teknologi, dan ekonomi. Volatilitas harga dapat diukur menggunakan rumus simpangan baku  $\sigma = \sqrt{(\sum(x-\mu)^2 / n)}$ . Nilai simpangan baku yang tinggi menunjukkan fluktuasi ekstrem yang menjadi karakteristik pasar kripto. Namun demikian, adopsi institusional oleh perusahaan global meningkatkan legitimasi sebagai aset lindung nilai digital. Dari perspektif pendidikan, konsep Bitcoin dapat digunakan sebagai media pembelajaran statistika, teori bilangan, dan kriptografi. Siswa dapat memahami bagaimana konsep abstrak diterapkan dalam sistem nyata yang digunakan secara global. Implikasi ini menunjukkan potensi integrasi teknologi digital dalam kurikulum matematika modern.

## **KESIMPULAN**

Bitcoin merupakan inovasi finansial berbasis matematika yang mentransformasi sistem keuangan global. Struktur kriptografi, mekanisme konsensus, dan model kelangkaan menjadikannya unik dibanding sistem moneter konvensional. Integrasi konsep Bitcoin dalam pembelajaran matematika membuka peluang pendekatan kontekstual yang relevan dengan perkembangan teknologi digital. Untuk saran, penelitian lanjutan disarankan menggunakan pendekatan kuantitatif berbasis data historis harga untuk mengukur korelasi dengan aset tradisional. Selain itu, pengembangan modul pembelajaran berbasis Bitcoin dalam pendidikan matematika perlu dirancang secara sistematis.

# **REKONSTRUKSI HISTORIS, ANALISIS MATEMATIS, DAN IMPLIKASI PENDIDIKAN BITCOIN DALAM TRANSFORMASI SISTEM KEUANGAN DIGITAL GLOBAL**

## **DAFTAR REFERENSI**

- Antonopoulos, A. M. (2017). *Mastering Bitcoin*. O'Reilly Media.
- Chohan, U. (2022). *A History of Bitcoin*.
- Gervais, A., et al. (2016). On the Security and Performance of Proof of Work Blockchains.
- Koblitz, N., Menezes, A., & Vanstone, S. (2000). The State of Elliptic Curve Cryptography.
- Kumar, A. (2020). Volatility in Cryptocurrency Markets.
- Nakamoto, S. (2008). Bitcoin: A Peer-to-Peer Electronic Cash System.
- Underwood, S. (2016). Blockchain Beyond Bitcoin. *Communications of the ACM*.