**Blockchain and Cryptocurrency**

* **Blockchain is a digital ledger that records transactions across a network of computers and Cryptocurrency is a type of digital money that uses encryption to secure and verify transfers**
* **Blockchain and cryptocurrency are related because blockchain is the technology that enables cryptocurrency to exist and function.**
* **Many banks have invested in cryptocurrency and blockchain companies. For instance:** [**Standard Chartered has invested in Ripple, a blockchain network, and Cobalt, a UK-based trading technology provider**](https://markets.businessinsider.com/news/currencies/13-top-banks-investing-cryptocurrency-blockchain-technology-funding-blockdata-bitcoin-2021-8)
* Almost 3 In 10 Organizations in The Banking Sector Have adopted Blockchain Technology. As a result, Banking is the sector with the highest distribution of blockchain market value.
* **Banks are focusing on crypto custody services, where they safeguard clients’ digital assets for a fee.**
* **Instead of traditional ATM cards, banks can create secure, blockchain-based apps.** [**These apps offer better safety, control, and efficiency for customers**](https://www.banks.com/articles/investing/cryptocurrency/blockchain-benefits-banks/)
* **Cryptocurrency thefts amounted to $1.38 billion by June 24, more than doubling from $657 million during the same period in 2023.**
* **Bitcoin, the first cryptocurrency, has the largest market capitalization, at $249 billion in early 2020.**
* **The**[**global cryptocurrency market capitalization**](https://www.coingecko.com/en/global-charts#:~:text=The%20global%20cryptocurrency%20market%20cap,a%20Bitcoin%20dominance%20of%2048.12%25.)**currently stands at $1.22T, and with the rapid growth of some of the neobanks, it might not be too long before one breaks into the top 100.**
* **Accenture has**[**estimated**](https://www.accenture.com/t20170120T074124Z__w__/us-en/_acnmedia/Accenture/Conversion-Assets/DotCom/Documents/Global/PDF/Consulting/Accenture-Banking-on-Blockchain.pdf#zoom=50)**that the biggest investment banks could save $10bn by using blockchain technology to improve the efficiency of clearing and settlement.**

|  |  |
| --- | --- |
| **Year** | **Bitcoin Price ($)** |
| 2012 | 5.45 |
| 2013 | 13.4 |
| 2014 | 807.39 |
| 2015 | 314.81 |
| 2016 | 432.76 |
| 2017 | 1,034.07 |
| 2017 | 7,365.99 |
| 2017 | 19,279.90 |
| 2018 | 11,516.83 |
| 2018 | 3,885.21 |
| 2019 | 12,586.78 |
| 2020 | 6,944.33 |
| 2020 | 10,002.48 |

|  |  |
| --- | --- |
| **Region** | **Number of blockchain users (in millions)** |
| Asia | 160 |
| Europe | 38 |
| Africa | 32 |
| North America | 28 |
| South America | 24 |
| Oceania | 1 |

**Cybersecurity Measures in Banking**

* Cybersecurity in banking involves various measures and protocols designed to protect financial institutions and their customers from cyber threats.
* In 2023, as per report by the Indian Cybercrime Coordination Centre, digital financial frauds have accounted for rupee 1.25 lakh crore over the past three years.
* The average cost of a [data breach](https://www.ibm.com/reports/data-breach) for a U.S. company in 2022 was $9.44 million, up from $9.05 million the previous year.
* Various measures banks should and have adopted against cyberattacks: -

1. Apply [multilayer security measures](https://www.crowe.com/cybersecurity-watch/breaches-and-the-value-of-a-defense-in-depth-model) such as firewalls, intrusion detection, and prevention systems
2. Continually monitor and assess security practices
3. Update and patch software and systems on a regular basis
4. Encrypt data and devices
5. Provide employee security training and awareness programs
6. Create a detailed incident response plan
7. Implement strong backup and disaster recovery procedures
8. Regularly review and update cybersecurity policies and procedures, and ensure compliance with industry standards and regulations.
9. Invest in advanced security technologies, such as AI-powered threat detection and response systems, to stay ahead of evolving cyber threats.

* In just two years between 2020 and 2022, the number of [insider threat incidents](https://www.proofpoint.com/us/resources/threat-reports/cost-of-insider-threats) worldwide rose by 44%.
* The Gramm-Leach-Bliley Act of 1999 (GLBA; P.L. 106-102) directs financial regulators to implement disclosure requirements and mandate security measures to safeguard private information. Specifically, Subtitle A of Title V of GLBA provides a framework for regulating data privacy and security practices for financial institutions.
* The Sarbanes-Oxley Act of 2002 (P.L. 107-204) requires certain corporations, including banks, to identify internal and external risks to their business and the ways that the company guards against those risks.
* According to a 2023 report by the consulting firm Deloitte, the global financial services industry spent an estimated $18.3 billion on cybersecurity in 2022, with a projected growth to $22.5 billion by 2024.
* In the United States, the 2023 Cybersecurity and Infrastructure Security Agency (CISA) report found that the financial services sector spent approximately $12.7 billion on cybersecurity in 2022, a 12% increase from 2022.
* Investment in Cybersecurity Startups by Banks (2014-2018):

|  |  |  |
| --- | --- | --- |
| **Year** | **Funding Amount ($M)** | **Number of Deals** |
| 2014 | 174 | 3 |
| 2015 | 442 | 4 |
| 2016 | 268 | 8 |
| 2017 | 438 | 12 |
| 2018 | 349 | 13 |

**Biometric Authentication System**

* The Deloitte Center for Financial Services expects synthetic identity fraud to generate at least US$23 billion in losses by 2030,[3](https://www2.deloitte.com/us/en/insights/industry/financial-services/financial-services-industry-predictions/2023/financial-institutions-synthetic-identity-fraud.html#endnote-3) prompting many banks and fintech to develop more advanced biometric security systems to weed out would-be perpetrators.
* To help counteract these fraudulent actions, new and powerful biometric tools can provide additional layers of defence by evaluating whether users are human, testing the veracity of visual artifacts and manipulated recordings.
* With major players such as Bank of America, Citibank and Wells Fargo using biometric authentication tools — the market is [projected to grow to nearly $9 billion by 2026](https://www.prnewswire.com/news-releases/global-biometrics-for-banking-and-financial-services-market-report-2022-2026-regulatory-mandates-promote-adoption-biometrics-technology-in-banking-sector-301513133.html).
* Types of biometric in banking are: Face recognition, Fingerprint recognition, Voice recognition, behavioural biometrics, Finger or palm vein recognition, Iris scans.
* Fingerprints take the lead on precision security. No two fingerprints are alike, so fingerprint authentication has an inherent security and permanence compared with many other forms of identification.
* The Process of a Biometric Payment

1. Enrolment: The user’s biometric data is initially recorded and securely stored in a database.
2. Authentication: The user’s biometric data is captured using a biometric sensor or device, like a fingerprint scanner on a smartphone or a facial recognition camera.
3. Verification: Their data is compared to the stored data in the database to verify the person's identity.
4. Transaction Authorization: Once the identity is verified, the payment or transaction is authorized, and the funds are transferred or the purchase is approved.

* Biometric Authentication Market Growth (2021-2030)

|  |  |
| --- | --- |
| **Year** | **Market Value (in billion U.S. dollars)** |
| 2021 | 12.8 |
| 2022 | 15.6 |
| 2023 | 18.5 |
| 2024 | 21.6 |
| 2025 | 25.2 |
| 2026 | 29.3 |
| 2027 | 34.1 |
| 2028 | 39.7 |
| 2029 | 46.2 |
| 2030 | 53.6 |