**Blockchain and Cryptocurrency in Banking**

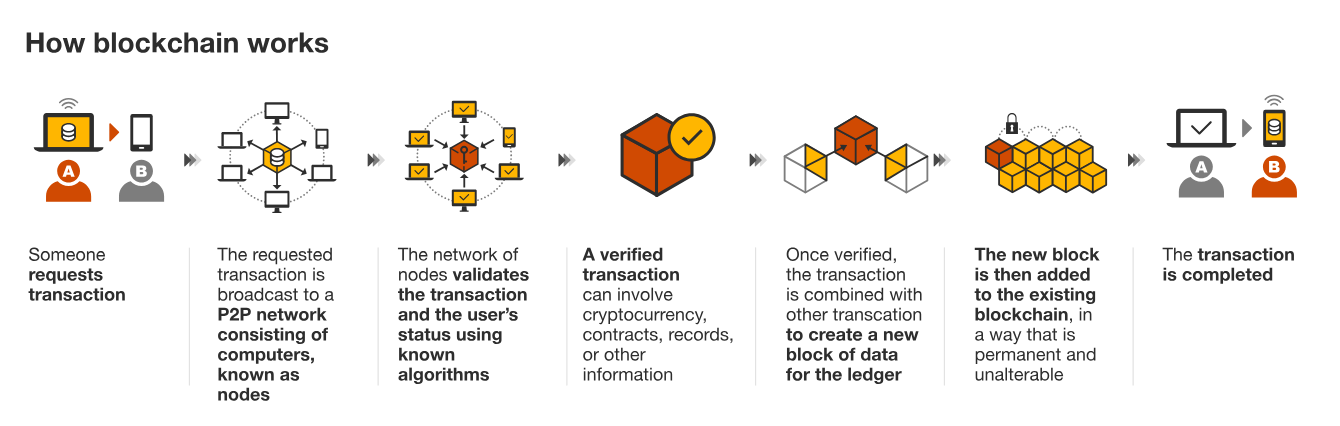
A Blockchain is a decentralized ledger of all transactions across a peer-to-peer network. Using this technology, participants can confirm transactions without a need for a central clearing authority. Potential applications can include enterprise blockchain applications, sustainability, tokenization, fund transfers, supply chain tracking and many other areas.

Cryptocurrency is a medium of exchange, created and stored electronically on the blockchain, using cryptographic techniques to verify the transfer of funds and an algorithm to control the creation of monetary units. Bitcoin is the best-known example.

* Has no intrinsic value in that it is not redeemable for another commodity, such as gold.
* Has no physical form and exists only in the network.
* Its supply is determined by the protocol, not a central bank and the network is completely decentralized.

**Blockchain’s benefits and unknowns**

|  |  |
| --- | --- |
| Benefits | Unknown |
| Increased transparency | Complex technology |
| Accurate tracking | Regulatory implication |
| Permanent ledger | Implementation challenges |
| Cost reduction | Competing platforms |



**How can blockchain be used in banking?**

* Accounting and audit
* Borrowing and lending
* Trade finance
* Trading
* Fundraising

**U.S Blockchain in Retail Banking Market**

A graph of a blockchain in retail banking market

Description automatically generated

* About 21 percent of American adults have owned cryptocurrency as of 2022, according to NBC News.
* In the United States, high-income earners are disproportionately represented among crypto investors, with those making $100,000 or more annually comprising 25 percent of crypto owners but only 15 percent of the general public.
* About 70 percent of cryptocurrency owners are men, but they represent only 48 percent of the general population. Women comprise 30 percent of crypto owners but 52 percent of the general population.
* The value of all existing cryptocurrency is around $2.33 trillion, with around $1.2 trillion of that being attributed to Bitcoin (as of May 6, 2024), according to CoinMarketCap.com.

**Conclusion**

While blockchain was initially designed to offer an alternative to traditional finance, it is now drawing interest from the financial institutions it was meant to rival. After years of downplaying and ever ridiculing the technology, banks are now realizing that the benefits of blockchain can no longer be ignored. Many applications of blockchain in banking offer ways to improve the sector’s existing operations and procedures. However, it is also likely that in the future banks would be implementing blockchain solutions designed to exist outside the traditional system. If that happens, the blockchain challenge to the sector will have been successful.

**Cybersecurity measures in banking**

Cybersecurity in banking refers to the measures taken by financial institutions to protect their systems and networks from cyberattacks. With the increasing reliance on technology in the banking sector, the need for robust cybersecurity measures has never been greater.

Banks and financial institutions employ various tools and technologies designed to detect and prevent cyberattacks in the form of hacking, data breaches, identity theft, malware, viruses, and unauthorised access to networks and sensitive data.

In recent years, there has been a significant uptick in the frequency and sophistication of [attacks](https://www.sentinelone.com/labs/operation-magalenha-long-running-campaign-pursues-portuguese-credentials-and-pii/) on the financial and banking industry.

* Financial institutions were the second most impacted sector based on the number of reported [data breaches](https://www.sentinelone.com/cybersecurity-101/what-is-a-data-breach/) last year. Institutions in the U.S., Argentina, Brazil, and China were most affected. As of December 2022, finance and insurance organizations globally [experienced](https://flashpoint.io/blog/risk-intelligence-year-in-review-financial/) 566 breaches, leading to over 254 million leaked records.
* Ransomware attacks on financial services have [increased](https://news.sophos.com/en-us/2023/07/13/the-state-of-ransomware-in-financial-services-2023/#:~:text=The%202023%20survey%20revealed%20that,sector%20in%20the%202021%20report.) from 55% in 2022 to 64% in 2023, which is nearly double the 34% reported in 2021. Only 1 in 10 attacks were stopped before encryption took place, making a total of 81% of organizations a victim of data encryption.
* Data breaches [cost](https://newsroom.ibm.com/2023-07-24-IBM-Report-Half-of-Breached-Organizations-Unwilling-to-Increase-Security-Spend-Despite-Soaring-Breach-Costs) the finance sector the second highest costs amongst all others at $5.9 million.

**U.S Cyber Security Market**

A graph of a number of people

Description automatically generated with medium confidence

**Average Cost Of Data Breach In United States**

A graph of numbers and a number of years

Description automatically generated with medium confidence

**Risks Faced by the Financial Sector**

In their 2022 Cybersecurity and Financial System Resilience [report](https://www.federalreserve.gov/publications/files/cybersecurity-report-202207.pdf), the Federal Reserve Board actively notes all [potential risks](https://www.sentinelone.com/cybersecurity-101/what-is-cyber-risk-management/) and emerging threats that affect the state of the U.S. economy. At no surprise, cybersecurity concerns topped the list, calling out Ransomware-as-a-Service (RaaS) and sophisticated [Distributed Denial of Service](https://www.sentinelone.com/cybersecurity-101/what-is-a-distributed-denial-of-service-ddos/) (DDoS) attacks as the biggest risks to financial institutions’ ability to operate and safeguard customer data.

* RaaS – [RaaS](https://www.sentinelone.com/anthology) is characterized by heightened sophistication, rapid proliferation, and difficulty of attribution. RaaS empowers threat actors to establish templates that could be considered “franchised” threats. Accomplished threat actors license their software to other malicious parties, typically in exchange for a portion of the ransom proceeds. This threat model provides less advanced threat actors with many more ways of disrupting businesses. Victims that decline ransom payment often find themselves with the burden of reconstructing their infrastructure in order to reinstate normal business operations.
* DDoS Attacks – In sophisticated [DDoS attacks](https://www.sentinelone.com/cybersecurity-101/what-is-a-distributed-denial-of-service-ddos/), the attacker aims to render a machine or network resource unavailable to legitimate users by overwhelming the target or its surrounding infrastructure with traffic. The United States’ financial services sector has long been a target of DDoS attacks, which has also affected associated external entities and other stakeholders.

**Biometric authentication systems**

Biometrics in financial digital services, in most cases, concerns the protection of users' financial and personal data and the conduct of financial transactions. In this case, the system makes payments by confirming certain bodily attributes, such as fingerprints, for instance.

Biometrics is very popular. It reduces the chances of theft and misuse of financial data due to each user's unique information and its impossibility to copy. Today, all reliable banking service providers use biometrics.

One of the notable examples of using biometrics is Amazon One – a palm-reading system that allows users to securely connect their fingerprints to their bank accounts for faster online transactions.

A graph of growth with numbers and a black text

Description automatically generated with medium confidence

Here are some statistics:

* The 2023 [Statista survey](https://www.statista.com/statistics/1441237/future-adoption-of-passwordless-authentication-by-various-industries-worldwide/)found that nearly half of the businesses in the retail and financial services industries plan to implement password less authentication in the next one to three years.
* In 2023, [nearly 60%](https://www.statista.com/statistics/1446265/top-solutions-to-replace-workplace-passwords-us/) of respondents among IT and cybersecurity executives in the United States said they intend to replace workplace passwords with facial recognition, fingerprint scanning, iris scanning, or voice authentication.
* [46%](https://www.statista.com/statistics/1446265/top-solutions-to-replace-workplace-passwords-us/)of respondents said their company has replaced or plans to replace passwords at work with multi-factor authentication.

**Main Types of Biometrics in Banking**

* Finger or palm print recognition. These are the easiest ways for users to authenticate.
* Facial recognition.
* Voice recognition.
* Iris scan. This method is not as popular as the previous two, but the trends are on its side.
* Infrared image. Manufacturers of connected watches are about to introduce such a technique to recognize the veins on the wrist.

The simplest example of using biometrics for payments is Google Pay and Apple Pay. As for banks, Japan Seven Bank uses facial scan in its ATMs. Qatar National Bank went further and implemented iris recognition for ATM customer service.

As for the United States, at least 30 banks use biometric authentication for mobile and web applications, including Bank of America, InTrust Bank, and California Commerce Bank.

The most prominent future trends are iris scanning, behavioral biometric intelligence, and AI and ML.