



BLOCKCHAIN – A CYBER OVERVIEW SCIENCE, TECHNOLOGY AND TELECOMMUNICATION COMMITTEE JULY 22, 2021

PRESENTED BY:
RAJA SAMBANDAM CISA, CRISC, CISSP
CHIEF INFORMATION SECURITY OFFICER



NM DEPARTMENT OF
INFORMATION
TECHNOLOGY

PRESENTATION SUMMARY

- ▶ Blockchain
 - Definition and Overview
 - Categories
 - Use Cases and Applications
 - State Government
 - Elections
- ▶ Security Risk and Concerns
- ▶ Cybersecurity Statistics and Trends
- ▶ Final Thoughts

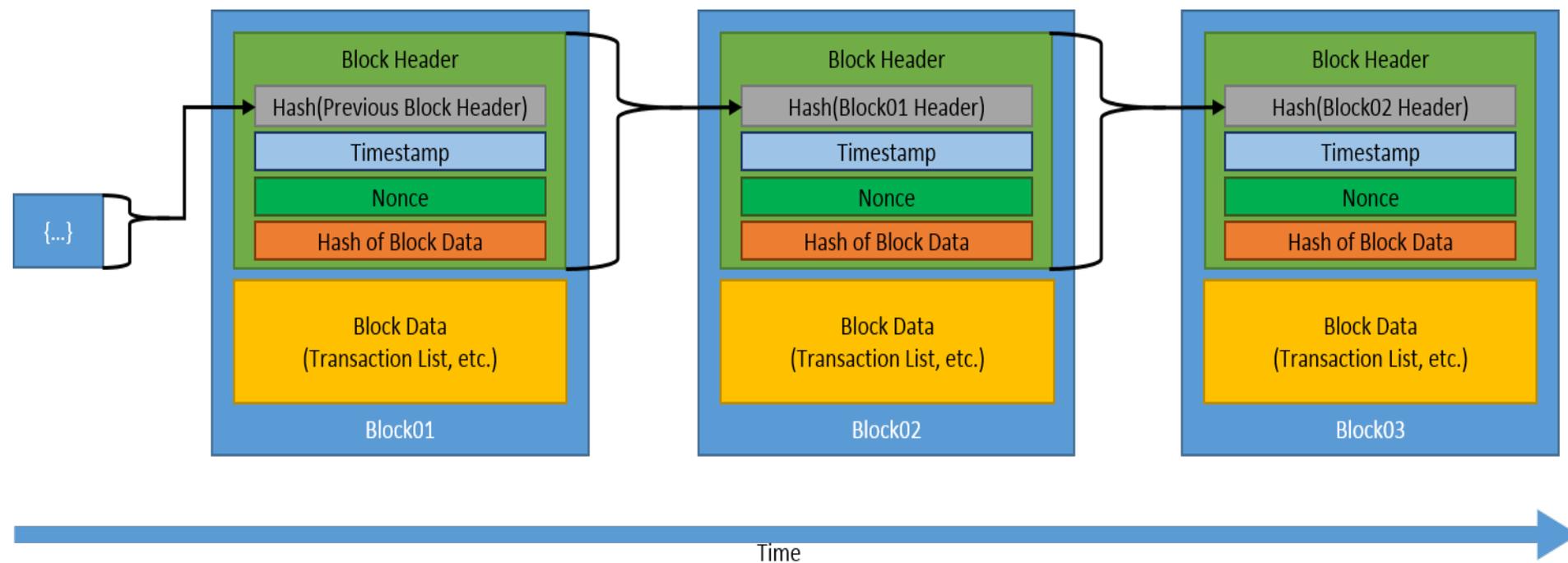
BLOCKCHAIN - DEFINITION

- ▶ Blockchain is a system of recording information and is essentially a digital ledger.
 - tamper evident and tamper resistant;
 - implemented in a distributed fashion without a central repository; and
 - usually without a central authority (i.e., a bank, company, or government).

BLOCKCHAIN - OVERVIEW

- The transactional records (data) are grouped into blocks
- A block is connected to the previous one by including a unique identifier that is based on the previous block's data
- If data is changed in one block, it's unique identifier changes, which can be seen in every subsequent block, providing tamper evidence
- This domino effect allows all users within the blockchain to know if a previous block's data has been tampered with
- Since a blockchain network is difficult to alter or destroy, it provides a resilient method of collaborative record keeping

BLOCKCHAIN – OVERVIEW VISUALIZED



BLOCKCHAIN CATEGORIES

▶ Permissionless

- Permissionless blockchain networks are decentralized ledger platforms open to anyone publishing blocks, without needing permission from any authority
- Permissionless blockchain platforms are often open-source software, freely available to anyone who wishes to download them. Public Blockchains such as Bitcoin, Ethereum, Litecoin, Dash, and Monero fall under this category

▶ Permissioned

- Permissioned blockchain networks are ones where users publishing blocks must be authorized by some authority, be it centralized or decentralized
- Since only authorized users are maintaining the blockchain, it is possible to restrict read access and to restrict who can issue transactions
- Examples include Hyperledger, Quorum and Corda

BLOCKCHAIN USE CASES & APPLICATIONS

▼ Smart Contracts

- Smart contracts are Blockchain-based contracts enforced in real-time. They are created as an agreement between two or more parties without the involvement of any intermediary. The contract exists across a distributed and decentralized Blockchain network.
 - BurstIQ used Big Data-based smart contracts to facilitate the transfer of sensitive medical data between patients and doctors. These contracts specify clear outlines and parameters for data sharing. They contain personalized health plans and other relevant details for individual patients.
 - Propy is a real estate platform that uses a Blockchain-based title registry system. It automates all transactions for brokers, realtors, and their clients. Thanks to Blockchain technology, Propy makes title issuance instant and allows the buying/selling of properties via cryptocurrency.

BLOCKCHAIN USE CASES & APPLICATIONS

▼ Internet of Things (IoT)

- The latest forecasts suggest that by 2030, there'll be 50 billion devices in use globally. As this number continues to grow, it will increase vulnerabilities.
- By integrating Blockchain technology in IoT devices, the possibility of data breaches can be reduced to a great extent.
 - **HYPR** takes cybersecurity to the next level by combining smartphone technology with the highly secure **Fast IDentity Online (FIDO)** token. This is the secret behind its True Passwordless Authentication feature.
 - **Xage** boasts of being the world's first Blockchain-based cybersecurity platform exclusively catering to IoT firms functioning in energy, transportation, manufacturing, etc.

BLOCKCHAIN USE CASES & APPLICATIONS

▶ Financial Services

- Money transfer and payment processing are the most excellent Blockchain technology use cases.
- Blockchain tech enables quick transactions in real-time and eliminates transaction fees charged by banks/financial institutions.
 - **Circle** uses USD Coin (USDC), the fastest-growing regulated Stablecoin, to help individuals run and establish their internet business.
 - **Chainalysis** offers Blockchain data and analysis reports to financial institutions, exchanges, and government agencies in 40 countries across the globe. Essentially, it focuses on helping institutions monitor cryptocurrency exchanges.

BLOCKCHAIN USE CASES & APPLICATIONS

➤ Identity

- In 2019, nearly 14.4 million people fell victim to identity fraud, which roughly translates to about 1 in 15 people.
- From hacking and violating personal files to forging documents, identity theft comes in many different forms. Blockchain can help combat this menace by storing crucial personal information on a decentralized ledger.
 - **Civic** is a blockchain-based platform integrated with a digital wallet that doubles as an identity card. It empowers people by giving them more control over their digital identities.
 - **Evernym** allows you to manage and control your identity on the Web by leveraging its identity ecosystem.

BLOCKCHAIN USE CASES & APPLICATIONS

▼ Logistics

- Data silos and lack of communication and transparency are the most pertinent issues of the logistics industry. Such obstacles become even more pronounced since thousands of companies operate in this domain, costing businesses time and money.
- Blockchain technology can acknowledge data sources and automate processes, by building greater trust and transparency within the logistics industry.
 - **DHL** is a shipping giant with a global presence. It leverages Blockchain-powered logistics to track and record information related to shipments while maintaining the integrity of transactions.
 - **Maersk**, an integrated logistics company, has collaborated with IBM to bring Blockchain into the global trade scenario. Through this partnership, Maersk optimizes supply chain management and digitally track products across international borders in real-time.

BLOCKCHAIN IN STATE GOVERNMENT

➤ State of Illinois

- Illinois is at the forefront of experimental blockchain in government. The state-funded initiative has already put in place measures to use a distributed blockchain ledger to enhance the security of birth certificates, death certificates, voter registration cards, social security numbers and much more.

➤ State of Delaware

- Similar to Illinois' Blockchain Initiative, the State of Delaware is also launching its own initiative to explore the benefits of blockchain in business and government. So far, the state has mostly focused its efforts into archiving public documents and safely securing private records. The next step in Delaware's initiative is to begin implementing smart contracts between the government and corporations.

BLOCKCHAIN IN ELECTIONS

▼ Elections

- Voatz is a mobile voting platform that runs on blockchain. The encrypted biometric security system makes it secure to vote on a mobile device from anywhere in the world without fear of hacking or data corruption. West Virginia is one of the first states to use the company's platform to collect votes from eligible service people and travelers abroad during elections.
- Follow My Vote is a secure online voting platform using an open-source virtual blockchain ballot box. The technology decreases spending on physical ballots and can be accessed via any device. Follow My Vote implements the end-to-end tools that elections need in order to provide total safety and confidence in the voting process

SECURITY RISKS AND CONCERNS

- **Routing attacks.** Blockchains depend on immense data transfers performed in real-time. Resourceful hackers can intercept the data on its way to ISPs (Internet Service Providers). Unfortunately, blockchain users don't notice anything amiss.
- **51% attacks.** Large-scale public blockchains use a massive amount of computing power to perform mining. However, a group of unethical miners can seize control over a ledger if they can bring together enough resources to acquire more than 50% of a blockchain network's mining power. Private blockchains aren't susceptible to 51% attacks, however.
- **Sybil attacks.** Named for the book that deals with multiple personality disorder, Sybil attacks flood the target network with an overwhelming number of false identities, crashing the system.
- **Phishing attacks.** This classic hacker tactic works with blockchain as well. Phishing is a scam wherein cyber-criminals send false but convincing-looking emails to wallet owners, asking for their credentials.

CYBERSECURITY STATISTICS & TRENDS

- 95% of data breaches are caused by human error
- In the first half of 2020, data breaches exposed over 35 billion records
- Of the data breaches recorded, 45% were hacking, 22% phishing, and 17% malware
- Over 90% of malware is delivered via email
- Over 200,000 malware samples are produced every day. This number is expected to increase over time
- Thirty-four percent (34%) of organizations affected by malware took a week or more to regain access to their data.
- Cybercrime damage is expected to cost \$6 trillion annually in 2021.
- Ransomware costs businesses over \$75 billion annually.
- Counterfeit invoices are the leading cover for malware spreading.
- By 2023, 50% of the world's data breaches will occur in the United States.

FINAL THOUGHTS...

- ▶ The inherently decentralized nature of blockchain technology has several applications of which cybersecurity should be investigated.
- ▶ Blockchain technology offers the highest standards of data transparency and integrity.
- ▶ As blockchain technology automates data storage, it eliminates the number one cause of data breaches – human error.
- ▶ Cybercrime is the number one threat facing businesses and blockchain technology could go a long way in combating it.

THANK YOU

QUESTIONS?

