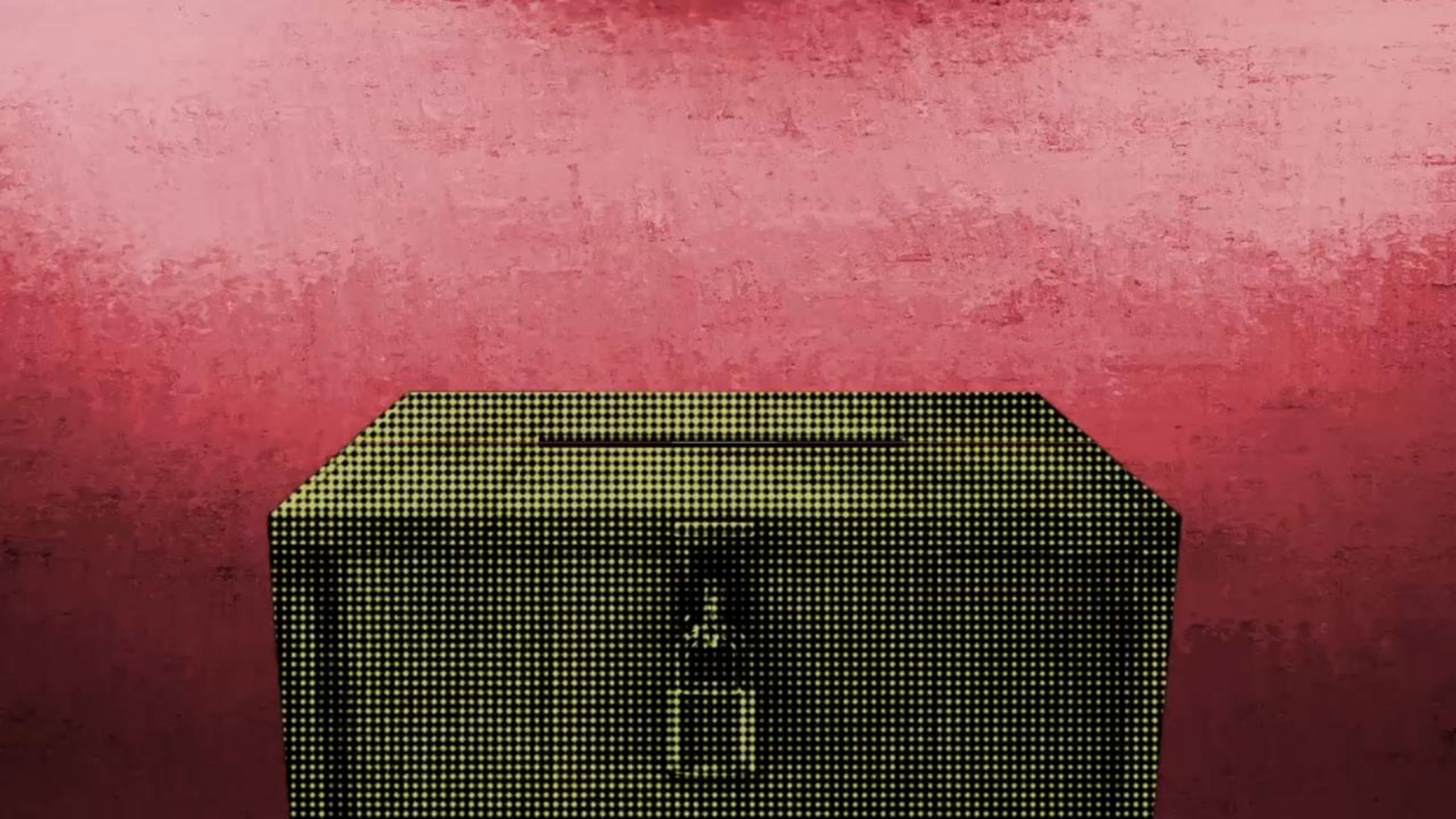
ISEC Infosecurity Tour 2018

Cybersecurity and Blockchain

John R. Robles, President

John R. Robles & Associates

787-747-3961



Cybersecurity and Blockchain

- **What is Cybersecurity?**
- It is:

The protection of cyberspace from physical and cyber threats which include:

  - Stealing information and money and
  - Disrupting, destroying or threatening the delivery of essential services.

- Specific crimes include:
  - Banking and financial fraud,
  - Intellectual property violation, child pornography and exploitation, and
  - Other crimes which result in human and economic suffering and bad consequences.

Cybersecurity and Blockchain

- **What is a Blockchain?**… the newest and latest Buzz Word
- It is an element of **Cybersecurity which is protecting the Cyberspace**

  - The first use of Blockchain was in the cryptocurrency, Bitcoin
  - A Blockchain is a **secure database of transactions** which has the following characteristics:
    - The Database is Distributed over various nodes
    - The Network is Decentralized - P2P - Peer-to-Peer (No one node is an administrator)
    - Addition to the Database is Consensus-based, hack proof (All nodes must agree to additions to the database)
    - Public, anyone can add transactions or Private, for authorized persons
  - The database of transactions or Blockchain is constructed as a series of Blocks which is constantly growing.
  - The Blocks are linked and secured using cryptography.
  - Bitcoin is the database of bitcoin transactions

Cybersecurity and Blockchain

- What's the Big Deal behind Blockchain?
- The Blockchain technology promises:
  - Disruptive applications
  - Transformative applications
  - Revolutionary applications
  - It's the latest new IT technology - It is **Internet 3.0!**
  - To be used in an increasingly sharing economy
  - The Puerto Rico government is studying it and reviewing Use Cases for the technology
  - Read the article in El Nuevo Dia (sabado, 17 de marzo de 2018)
    - Gobierno local pondera como regular el "blockchain"
    - Ante el apogeo de la nueva tecnología, funcionarios locales muestran entusiasmo pero también cautela

FINANZAS

Gobierno local pondera cómo regular el "blockchain"

Ante el apogeo de la nueva tecnología, funcionarios locales muestran entusiasmo pero también cautela

sábado, 17 de marzo de 2018 - 12:00 AM

Por Dennis Costa

Cybersecurity and Blockchain

- The **inherent security** of Blockchain makes the technology very attractive
- Before, transactions were controlled and secured by:
  - Batch Totals
    - **Problem**: Transactions can be altered and the batch total can be modified to reflect the alteration
  - Hash Totals
  - These totals would detect modifications, errors, or omissions in the processing and transmission of transactions
  - Manual Reconciliations of these totals is made across departments and enterprises
  - Reconciliation of transaction totals is a duplicative process which can be time consuming
- Blockchain ensures that transactions in the blocks of the Blockchain cannot be altered.
  - It is **Pure Security**
  - That is one reason Blockchain is: **Disruptive**!, **Transformative**!, and **Revolutionary**!
  - No problem with the possibility of transaction tampering.
    - **It is not possible!**

Cybersecurity and Blockchain

- Other transactional controls included:
- Backups of data
  - **First**, to tapes. Onsite and then off-site
  - **Then,** synchronized backups with off-site facilities
  - **Then,** the use of transmission of data via Internet and the Cloud (Dropbox, Microsoft OneDrive, Google Drive, etc., etc.)
- Implementing Blockchain requires and demands the replications of the transaction database or Blockchain across various nodes. (Backup is built-in, the database of transactions is replicated and distributed)
- Today we require controls over sensitive and confidential information to include:
  - Encryption (at rest and in motion)

Cybersecurity and Blockchain

- A Blockchain is a series of transactions grouped into blocks where the information in the blocks is **Virtually Impossible** to:
  - Add to,
  - Delete ,or
  - Modify

without being detected by other users or nodes

- A Blockchain is decentralized and distributed
  - Everyone must verify and consent to the formation of the information blocks
  - At least 50% of the nodes must consent to the formation

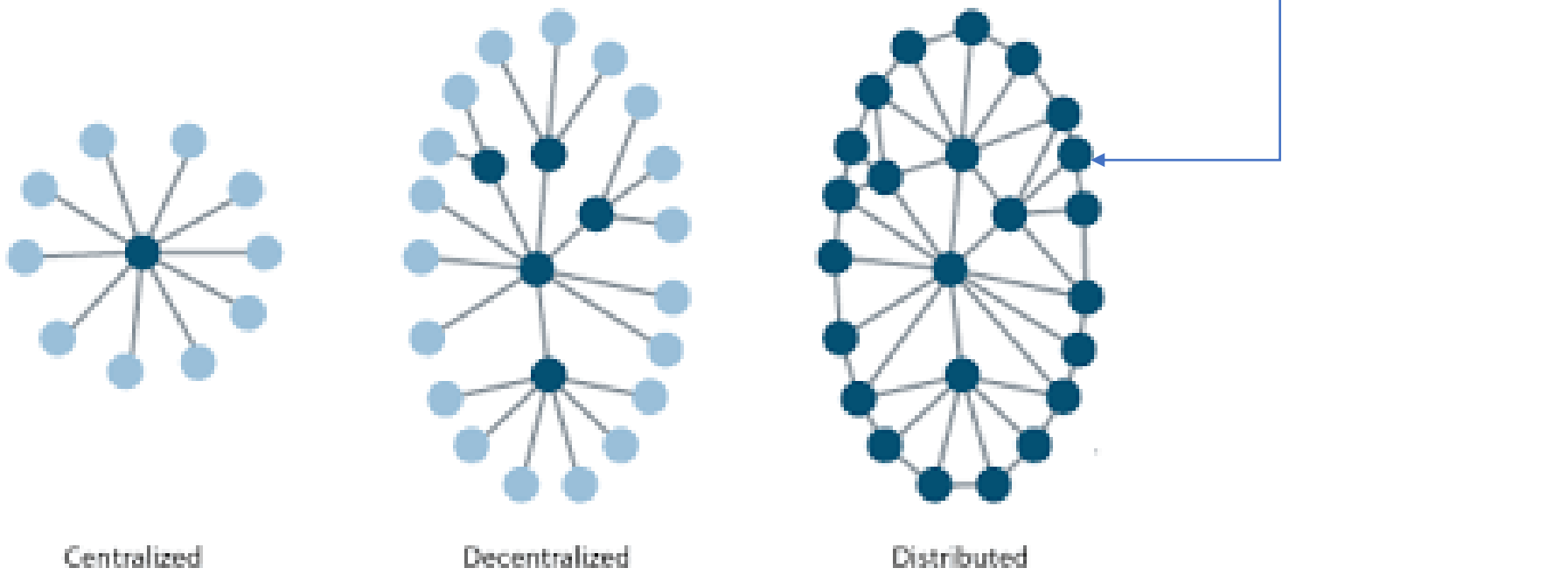
- A Block is created by:
  - Gathering and ordering data into blocks
  - Chaining them together securely using cryptography
  - All transactions is a block are time-stamped
  - When a Block is completed with required transactions, the block is also time-stamped
  - All data is sequential

Cybersecurity and Blockchain

- Each Block contains, at least, the following:
  - Previous block Hash
  - Transaction data
  - Time Stamp
  - Current Block Hash

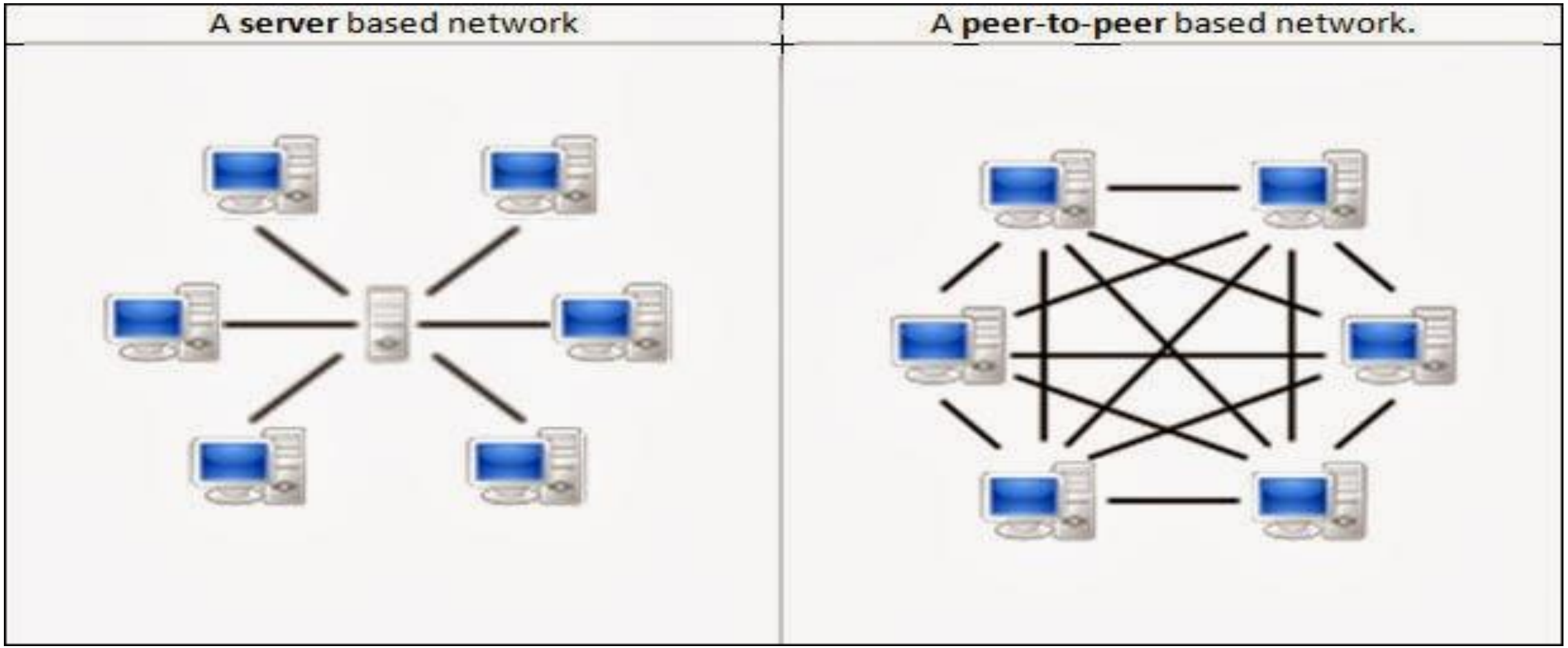
Cybersecurity and Blockchain

A Blockchain Network is : Decentralized and Distributed



Cybersecurity and Blockchain

A Blockchain Network is : Decentralized and Distributed – P2P – Peer-to-Peer



Cybersecurity and Blockchain

- Securing the Blockchain

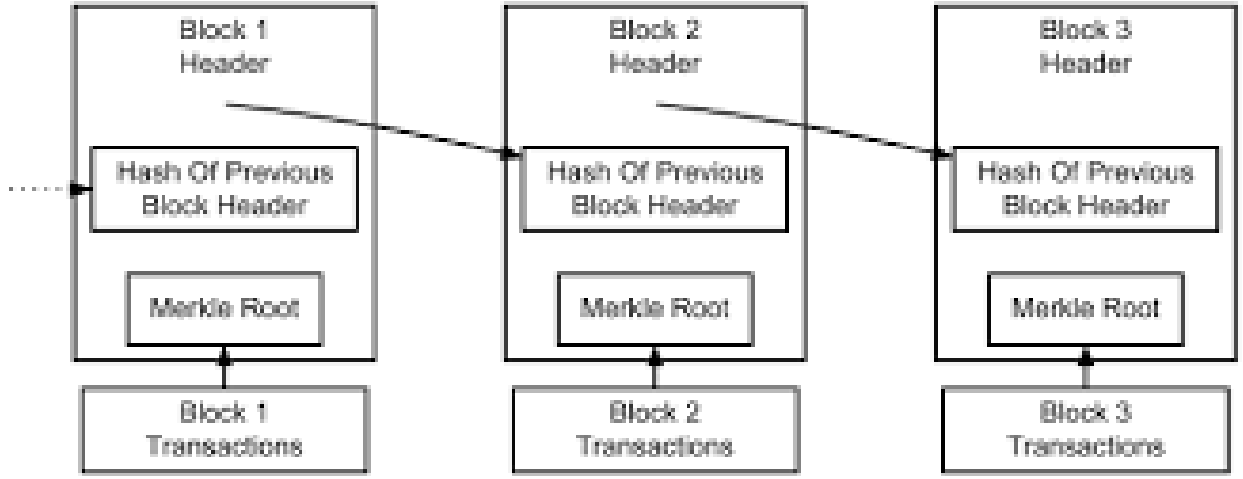
1. Each block has a **Hash calculated** for it.
2. Each node must go through the same Hashing function and get the same Hash identifier.
3. If one bit of information in a block is modified, the Hash number is recalculated.
4. The Hash from one block is added to the data in the next block

Cybersecurity and Blockchain

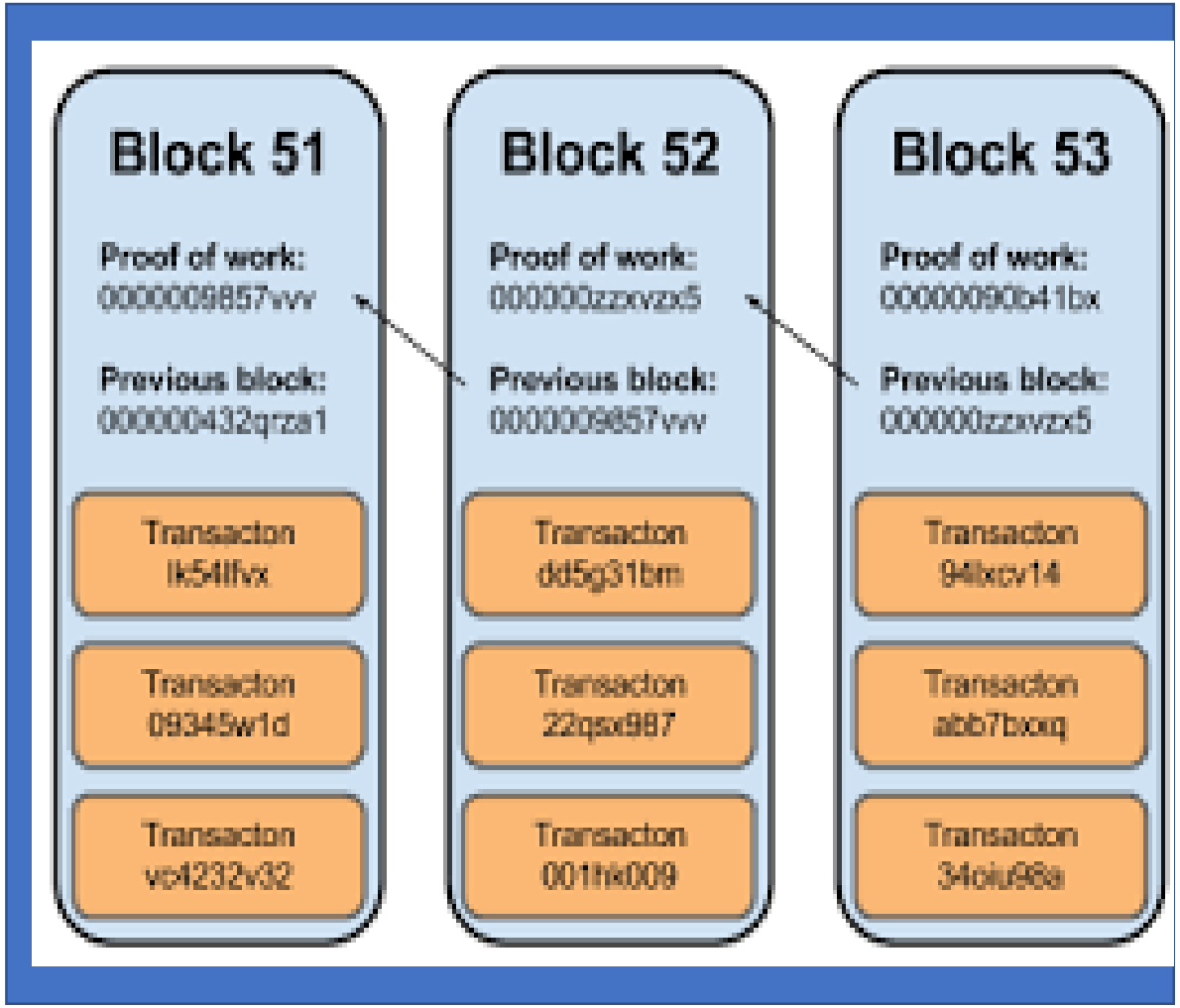
- Securing the Blockchain

5. If previous data in the chain is modified, the Hash from the block will not be the same as the previous Hash stored in the current block.
6. All identified nodes have a copy of the entire blockchain and therefore can detect any changes in the information in the blocks.
7. When all the hashes match up across the chain, all nodes know that they can trust their records.

Connecting and Chaining up Blocks in a Blockchain

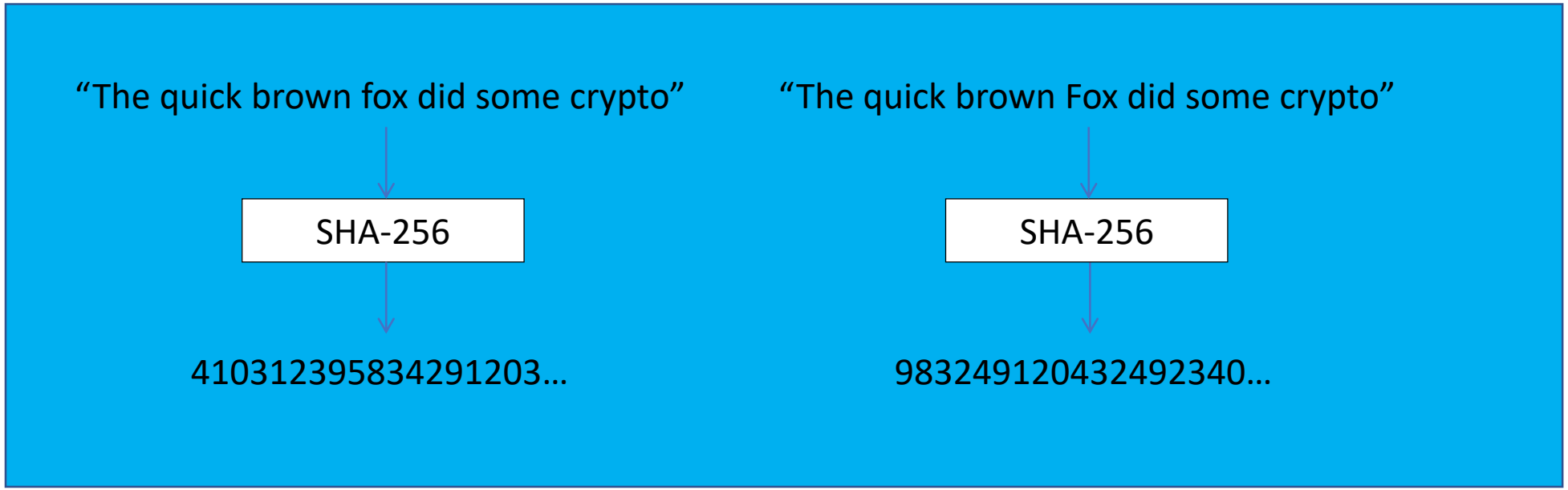


Simplified Bitcoin Block Chain



Cybersecurity and Blockchain

- How is a Blockchain constructed?
- A hash function (like SHA-256) takes a block of data in, and produces an effectively random fixed size integer.
- Any change to the input changes the Hash



Cybersecurity and Blockchain

- Today we require controls over sensitive and confidential information to include:
  - Encryption (at rest and in motion)
- With Blockchain, you establish Public and Private Blockchains
  - Public and Private keys are used to improve privacy
- Bitcoin's Blockchain is public.
  - Anyone can add a transaction to the Bitcoin Blockchain
- In a Private Blockchain, a central authority determines who can add transactions to the Blockchain and on which nodes it can be done.
- The Blockchain Eco-System consists of:
  - A node application - Software
  - A shared ledger - Data
  - A consensus algorithm - Software
  - A virtual machine - Hardware

Cybersecurity and Blockchain

- **The Future: How do we use Blockchain Technology**
- Now that you have a Secure Technology, what are the Use Cases?
- Use Cases in:
  - Finance
  - Healthcare
  - Digital Identity
  - Government
  - Artificial Intelligence (AI)
  - Internet of Things (IoT)
- Any application where there's an issue of Records/ Transactions Management
- Companies are starting pilots where Blockchains are being used.
- Blockchain technology is slow because of the calculations and computing resources being duplicated across the P2P network.

Cybersecurity and Blockchain

- Software companies are working on solutions to make Blockchain processing much quicker and less complicated
- Scaling problems
- No standardized implementation
- There are questions of liability and other legal issues.
- Cryptography is used,
  - However,
  - Security concerns could slow blockchain adaption

Cybersecurity and Blockchain

- **The Future:**
- Blockchain will be a revolution in how businesses, government, organizations and individuals work together.
- It can be a simple secure way to establish trust for virtually any kind of transaction helping simplify the movement of money, products, or sensitive information worldwide.
- Blockchain, the New Technology of Trust
  - The Transformation has begun
  - Organizations must be prepared as the technology matures.

Bitcoin Market Price | Downloads | Bitcoin Market Price | Bitcoin Market Price | capture a web page | How to Capture a W | download gadwin -

file:///C:/Dropbox/01_A_Clients/99%20PRCCUG/99%20Presentations/12%2019%2013%20BitCoin%20Presentation/Bitcoin%20Market%20Price%20(USD).htm

Apps | Todoist | Google | 01 Bills Pymt | 01 News | 01_Vatican | 02 GK's Sites | John Stuff | 14 Tech &, Win 8 | 16 Millie's Stuff | Cloud Computing | Cloud Use Cases | Other bookmarks

Blockchain — Home | Charts | Stats | Markets | Developers | Wallet | Search

30 Days - 60 Days - 180 Days - 1 Year - All Time

Logarithmic Scale - 7 day average - Show data points - (CSV - JSON)

ENG 9:18 PM 12/17/2013

Gracias!!