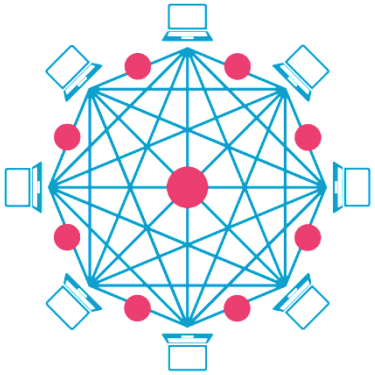
Blockchain Technology and its Significance to Cyber Security



International Conference on
Public Key Infrastructure and its Applications PKIA 2017
Bangalore, November 14-15, 2017

Mrs P.R.Lakshmi Eswari

e-Security Team

C-DAC, Hyderabad

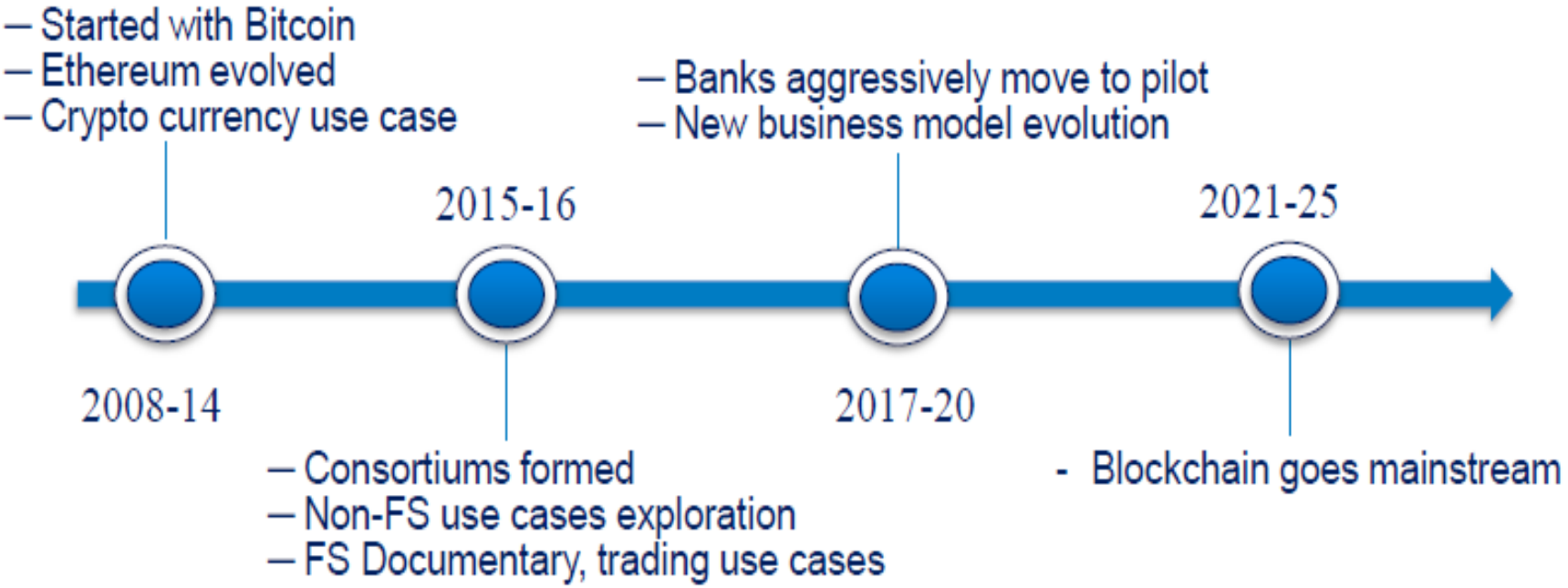
Gartner Hype Cycle for Emerging Technologies, 2016

gartner.com/SmarterWithGartner

Source: Gartner

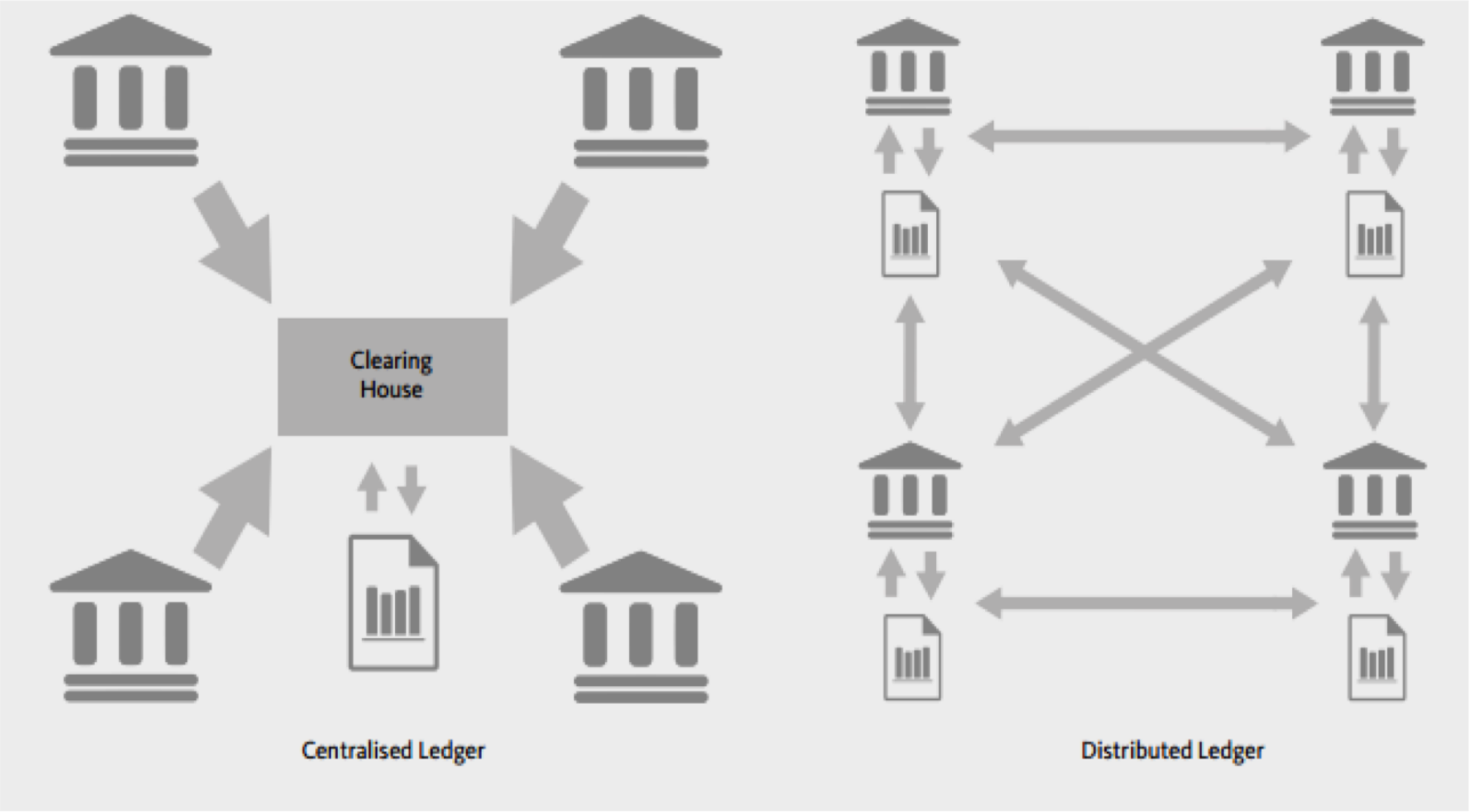
Gartner

Current Stage of Evolution



- **World Economic Forum survey projects Blockchain "tipping point" by 2023 and 10% of global GDP will be stored with Blockchain powered networks by 2027.**

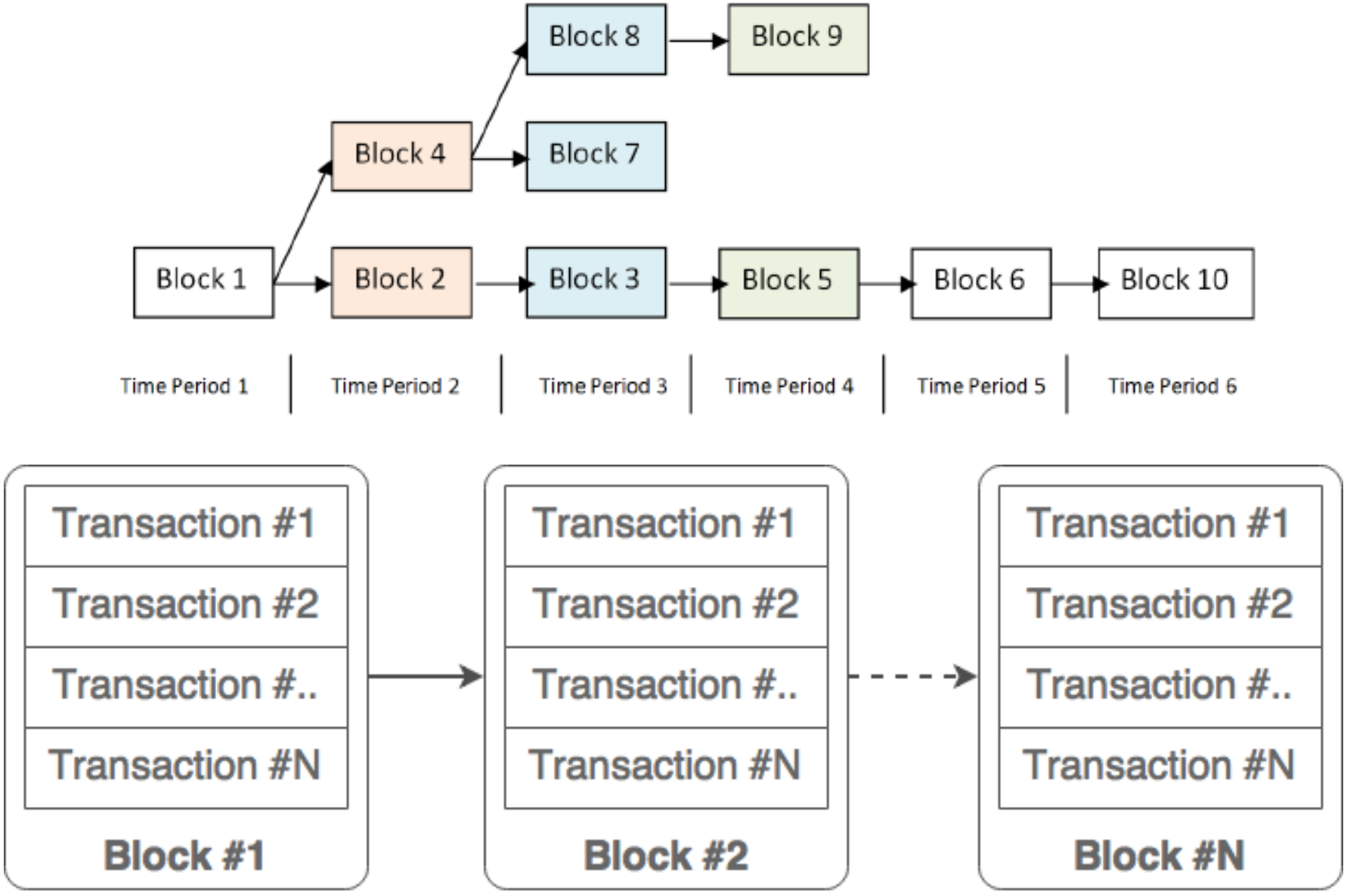
Centralized Vs Distributed Ledger



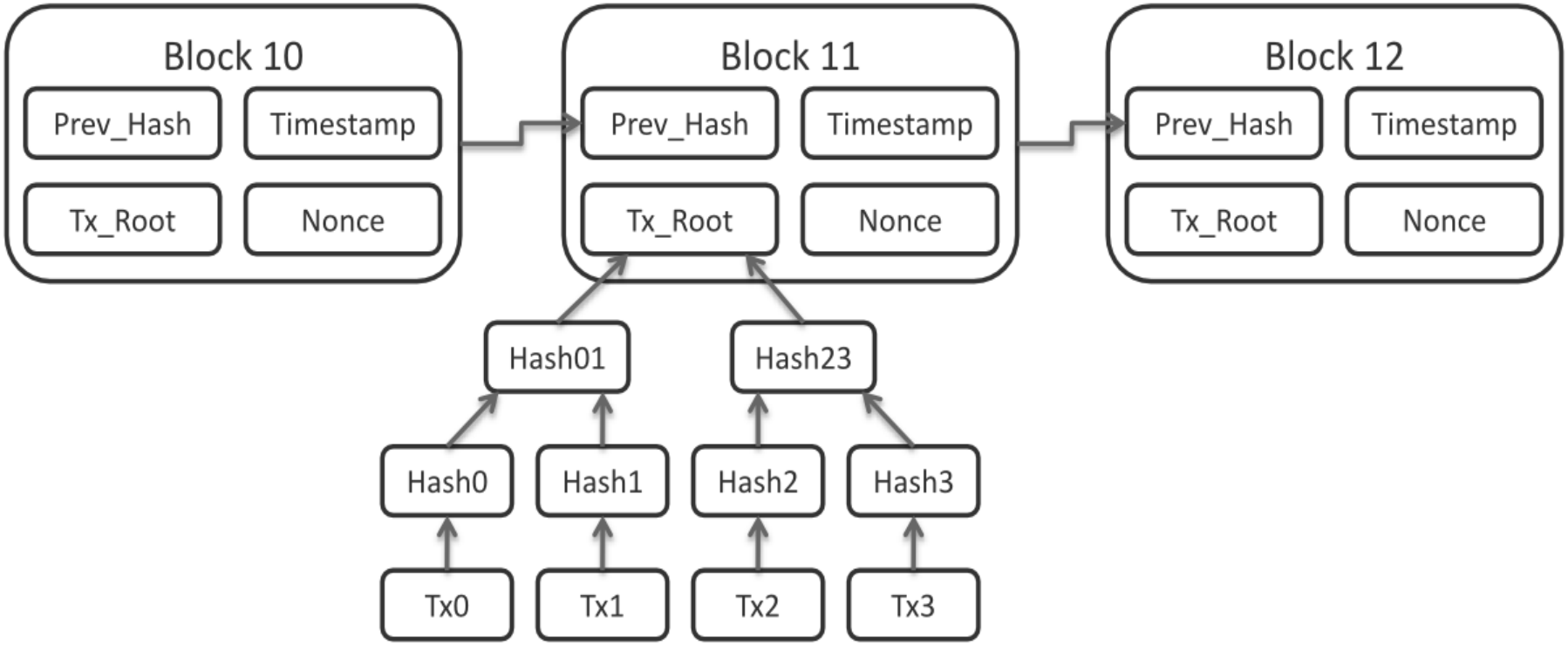
Blockchain Technology

- A blockchain is a continuously growing list of records, called blocks
- Blocks are linked and secured
- Block typically contains
  - a hash pointer as a link to a previous block
  - a timestamp and
  - transaction data
- Inherently resistant to modification of the data by design
- It can serve as an open, distributed ledger that can record transactions between two parties in a verifiable and permanent way
- As a distributed ledger it is typically managed by a peer-to-peer network collectively adhering to a protocol for validating new blocks.
- Once recorded, the data in any given block cannot be altered without the alteration of all subsequent blocks

Chronologically updated

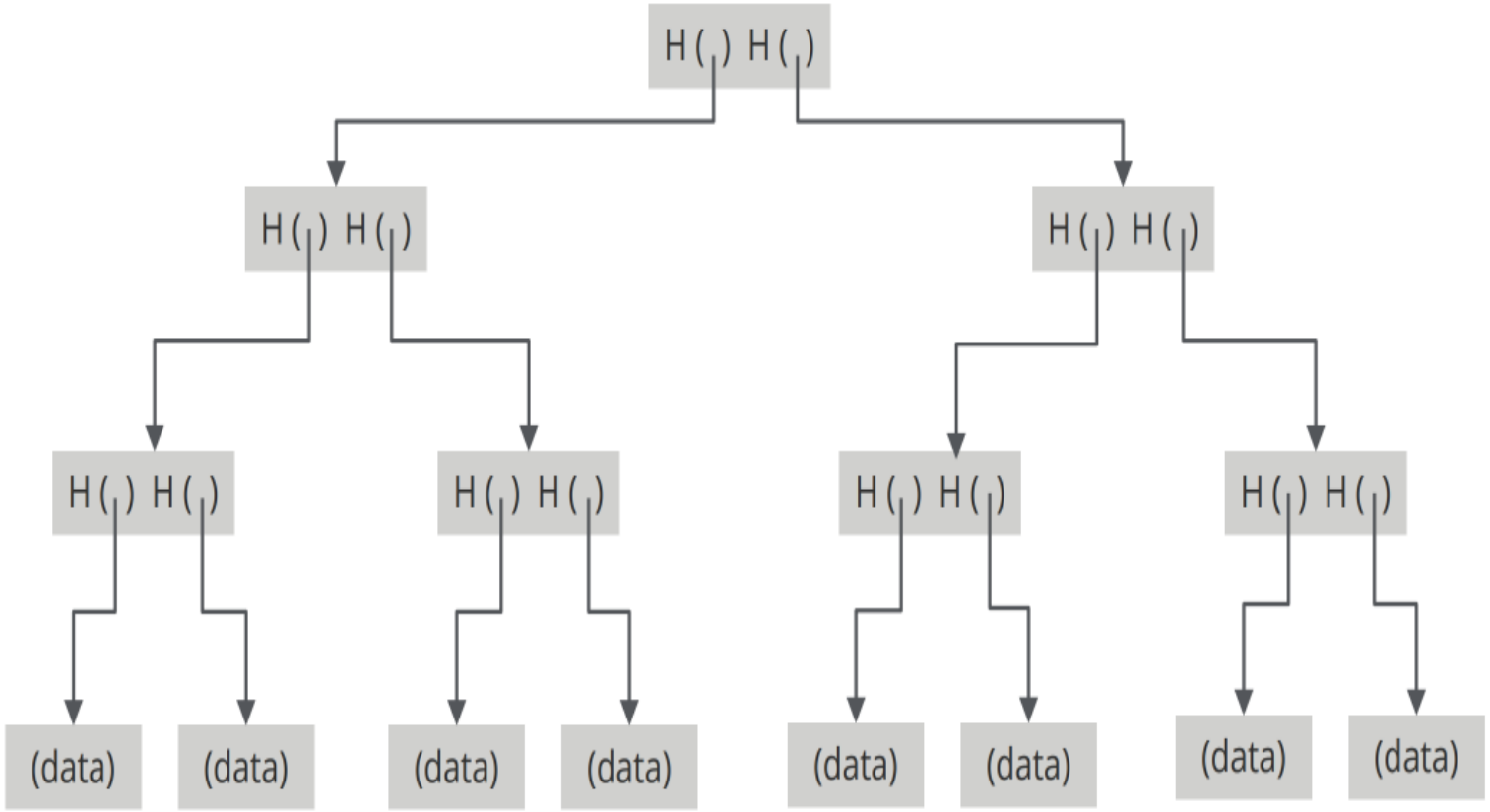


Blockchain

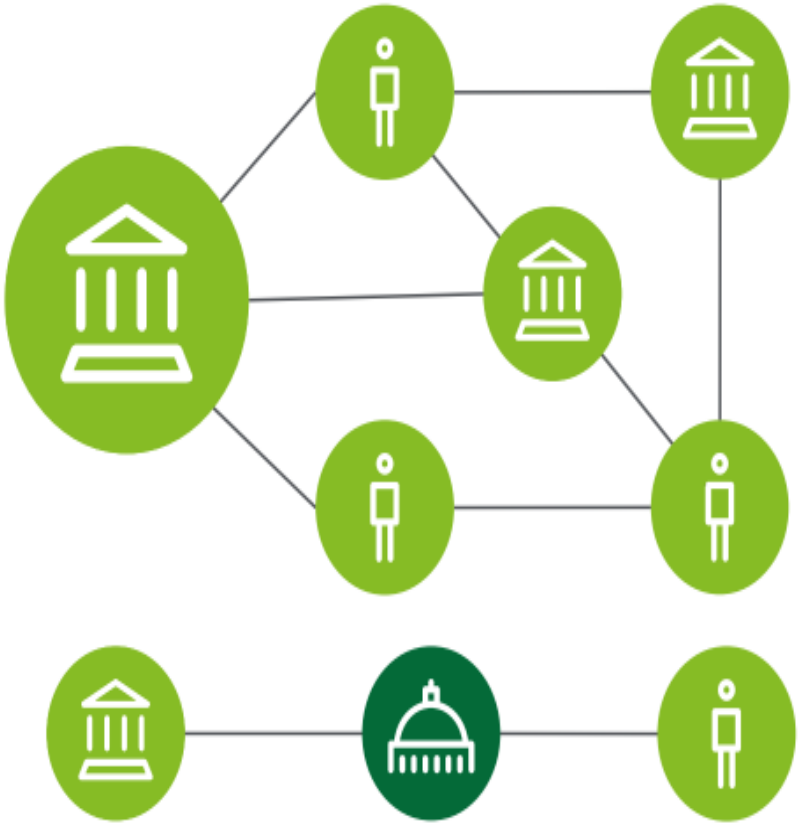


- BCT helps to create verification records (fingerprints) for digital assets
- These fingerprints are stored in block and then linked in a chain of blocks where the subsequent block also has verification record

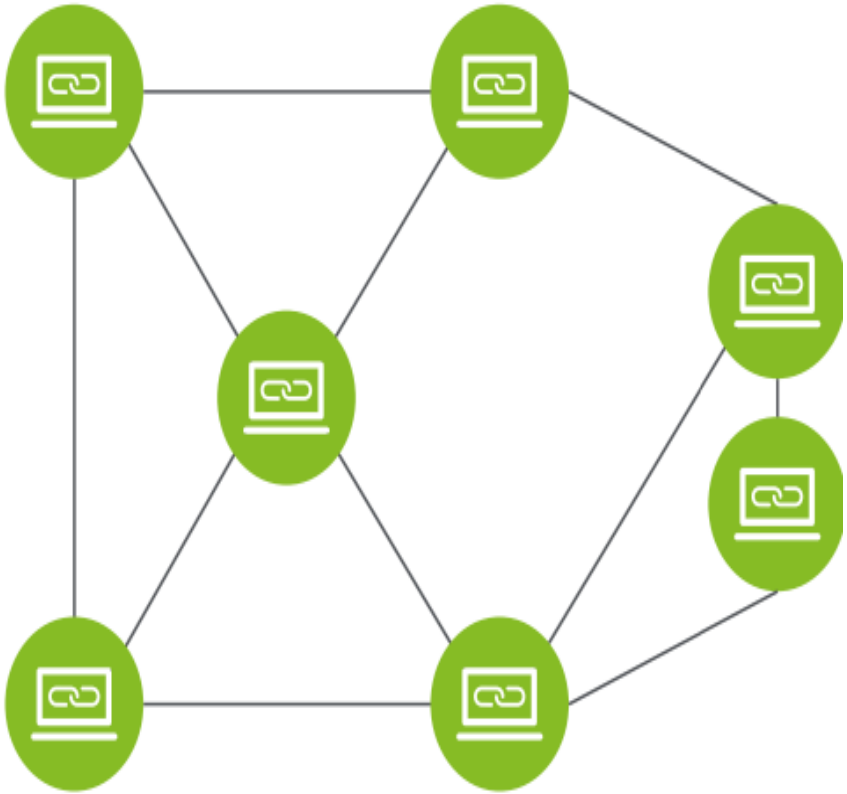
Merkle Tree Structure



Traditional Database Vs Block chain based Distributed Ledger



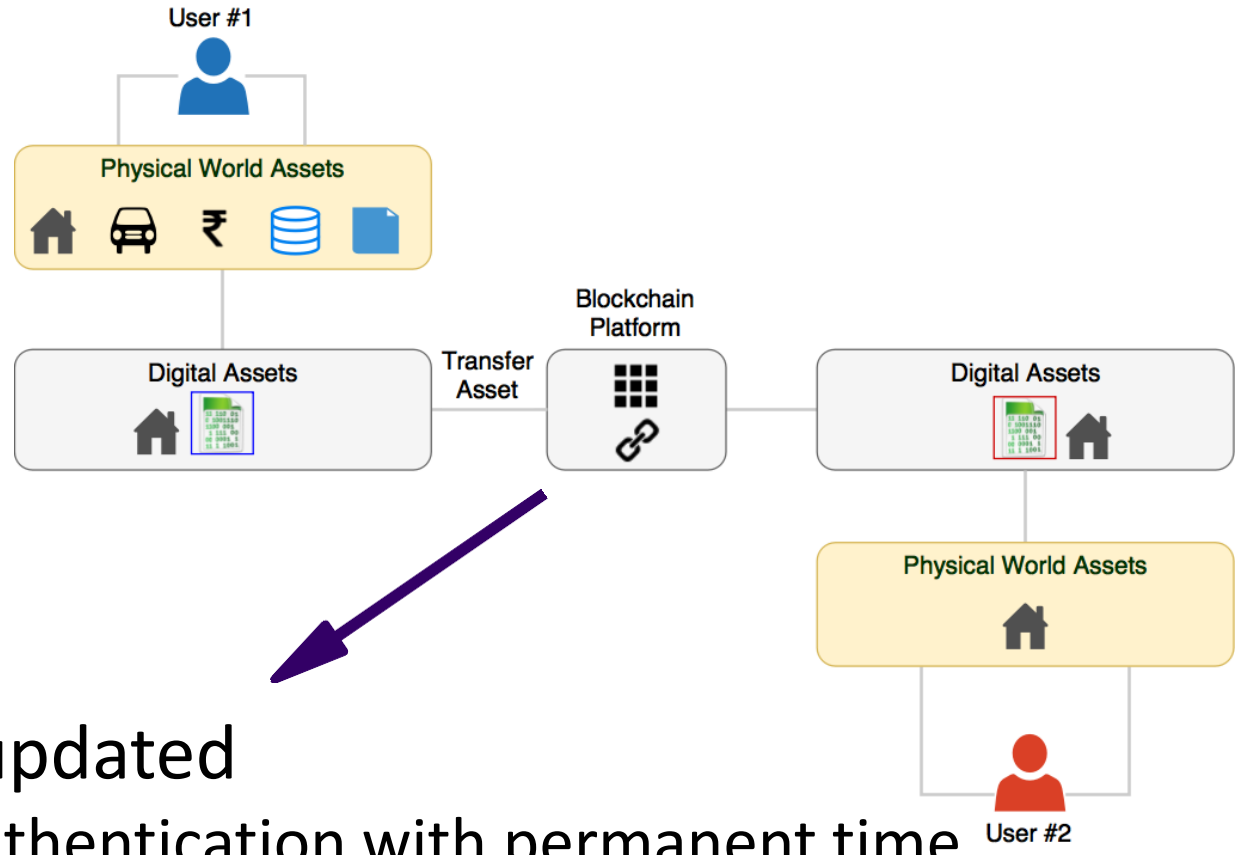
Central Authorities and Multiple Intermediaries facilitate the information sources and create trust



Distributed nodes that maintain a shared source of Information Trust enabled by cryptographic algorithm

Blockchain - Purpose

- Blockchain is a shared & distributed ledger
- It facilitates the process of recording transactions and tracking assets in a business network
- An asset can be tangible a house, a car, cash, land — or intangible like intellectual property, such as patents, copyrights, or branding
- Virtually anything of value can be tracked and traded on a blockchain network, reducing risk and cutting costs for all involved



Record/ Transaction

- Chronologically updated
  - Verification & authentication with permanent time stamping
- Distributed
  - Identical copy shared with all/ permissioned entities
- Cryptographically sealed
  - Once block is sealed it can't be tampered, deleted, copied, and edited

Blockchain – Salient Features

- Near Real time
- Distributed Trust (No Intermediary)
- Irreversibility and Immutability (Eventually Consistent)
- Smart contracts
- Cryptographic guarantees
- Distributed Ownership (Publicly Verifiable)
- Tamper Resistant
- Pseudonymity

Consensus in Blockchain

- Consensus is established using the blockchain
  - Which keeps records of previous transactions
  - Proof-of-work which makes changing historic records prohibitively costly
- Correctness is guaranteed by protocol rules
- Owner can be identified using public key cryptography

List of Blockchain Platforms

- Bitcoin Core
- Ethereum Blockchain
- Infosys EdgeVerve Blockchain Framework
- Hyperledger from Linux Foundation
- Intel - Sawtooth Lake
- Chain
- Multichain
- OmniLayer
- Blockstream
- Scale Chain
- Stratis Platform
- Eris – by Monax
- Ripple (Google funded digital currency)
- BigchainDB (Database on Blockchain)
- Openchain

Types of Blockchain

- **Public Blockchain** (Anyone can read/write data in public Blockchain) – Eg. Bitcoin, Ethereum, etc

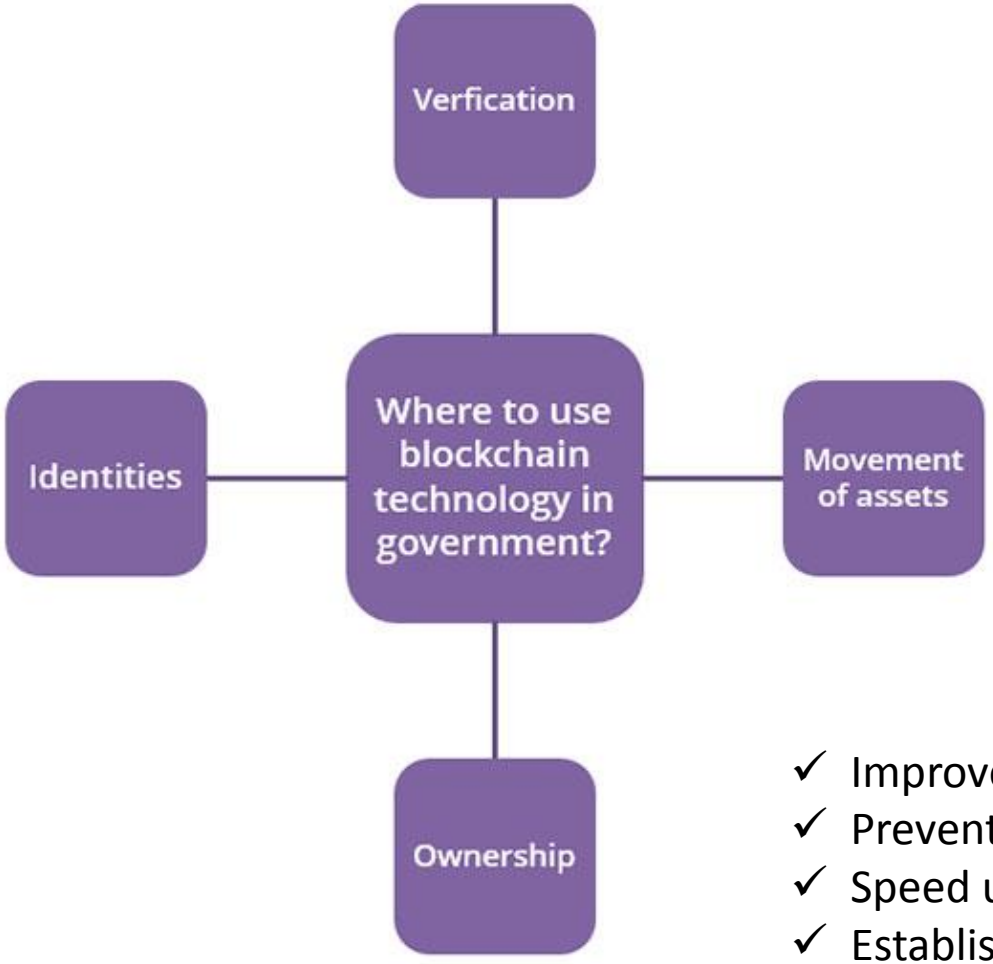
- **Private Blockchain** (Write permissions are kept centralized to one organization. Read permissions may be public or restricted) – Eg. Multichain, Blockstack

- **Consortium Blockchain :** Consensus process is controlled by a pre-selected set of nodes; for example, one might imagine a consortium of 15 financial institutions, each of which operates a node and of which 10 must sign every block in order for the block to be valid. The right to read the blockchain may be public, or restricted to the participants.

Adoption in India - Application Domains

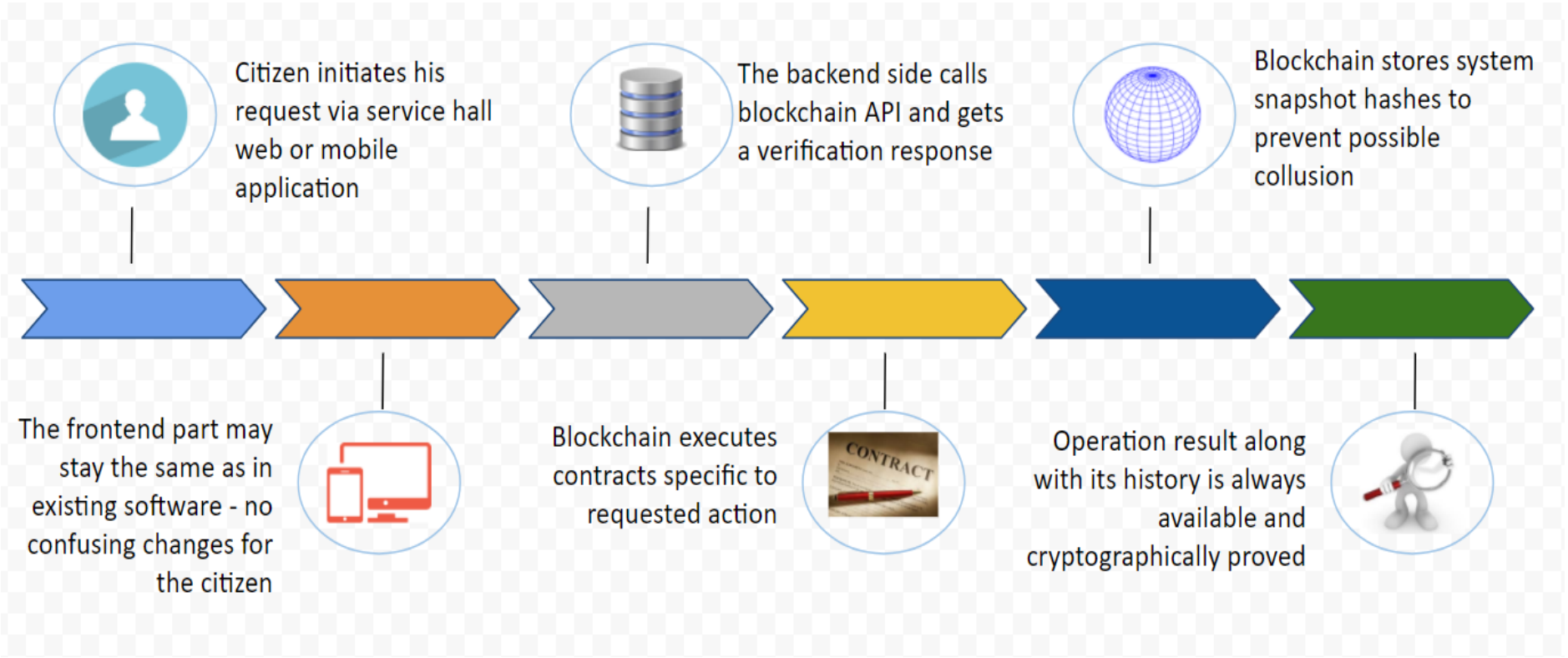
- Governance
- Banking and Finance
- Cyber Security
- Healthcare
- Media
- Smart cities
- Judiciary
- Insurance …

Blockchain applicability in Government



- ✓ Improve transparency
- ✓ Prevent fraud
- ✓ Speed up transactions
- ✓ Establish trust

Blockchain Registry - How does it works



Government and Blockchain Adoption

- Across Globe, Government organizations are exploring the use of blockchain technology to improve operations and citizen services.
- According to a recent survey conducted by IBM and the Economic Intelligence Unit, Government interest in blockchain is high:
  - 9 in 10 government organizations plan to invest in blockchain for use in financial transaction management, asset management, contract management and regulatory compliance by 2018
  - 7 in 10 government executives predict blockchain will significantly disrupt the area of contract management
  - 14 percent of government organizations expect to have blockchains in production and at scale in 2017

Global Scenario

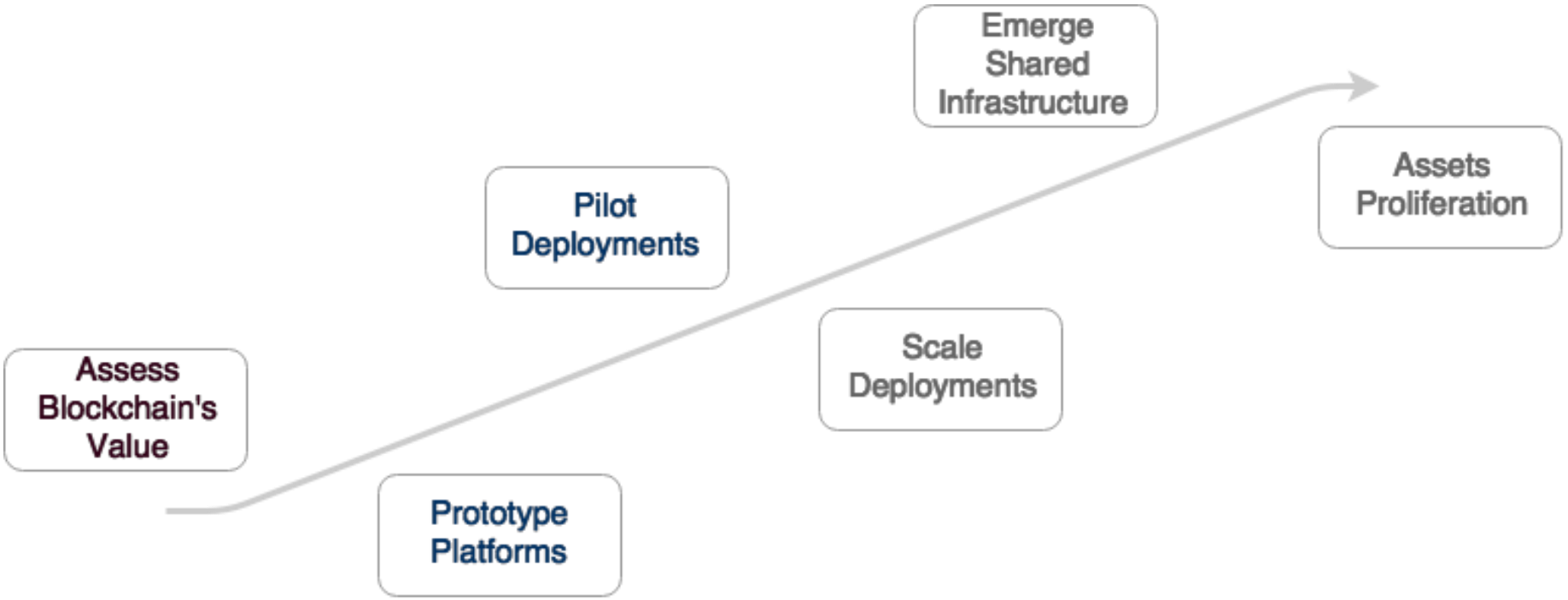
- Governance & Industry
  - UAE have strategic plan to make all Government documents secured on Blockchain by 2020
  - Sweden Land Registry aim to demonstrate the effectiveness of the blockchain at speeding land sale deals
  - IBM is utilizing Blockchain for IoT (ADePT Project)
  - Central securities depository of the Russian Federation (NSD) announced a pilot project to explore the use of blockchain-based automated voting systems
  - The Ethical and Fair Creators Association uses blockchain to help startups protect their authentic ideas.
- Research and Academic
  - IEEE Security & Privacy on the Blockchain
  - First ACM Workshop on Blockchain, Cryptocurrencies and Contracts (BCC'17)
  - ACM Asia Conference on Computer and Communications Security (ASIACCS) 2017

Standards

- ISO/TC 307 Blockchain and electronic distributed ledger technologies is proposed

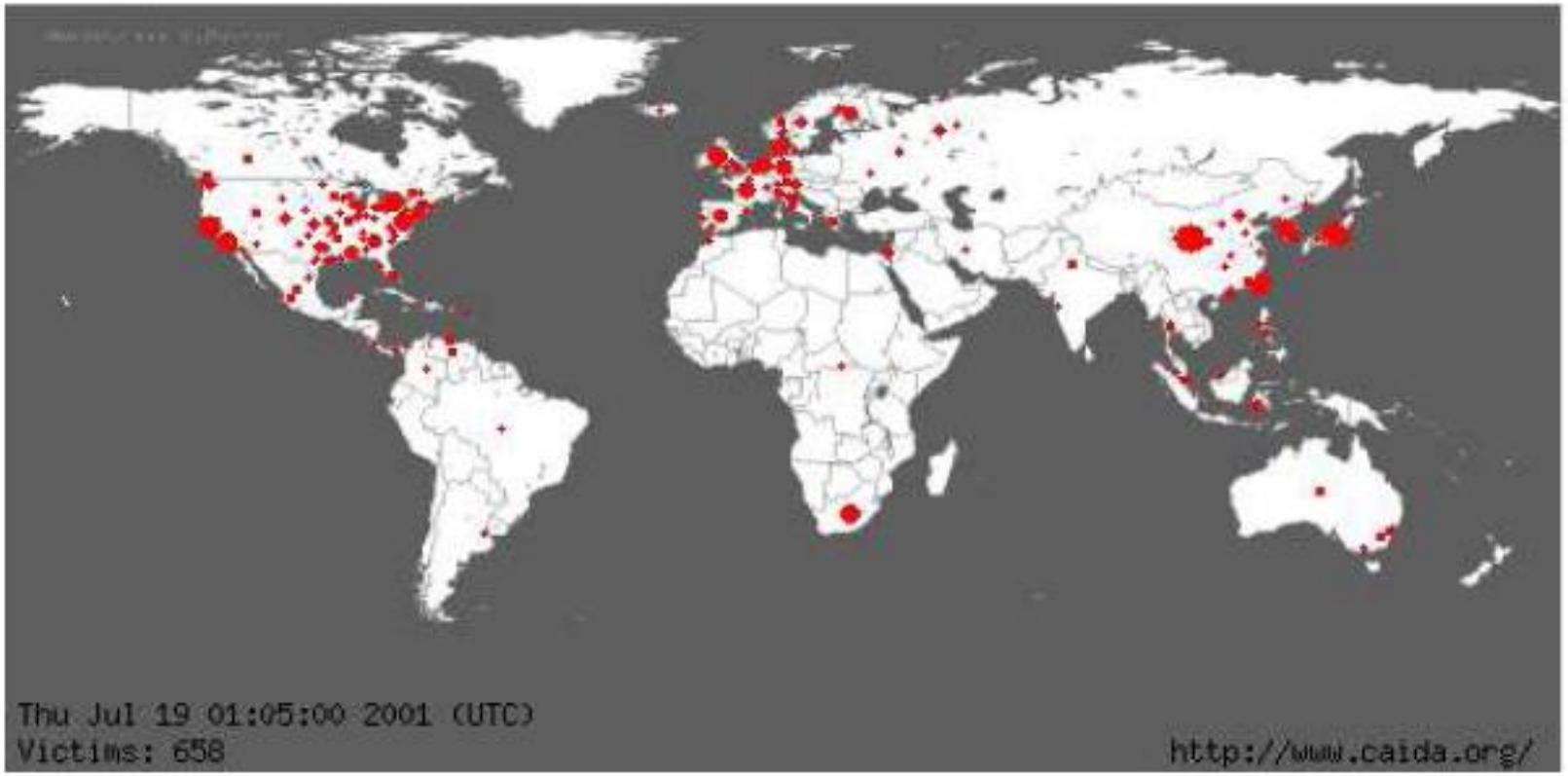
- XBRL (US Consortium for Business Reporting Standard) and ConsenSys (Ethereum startup) is developing standards for creating Blockchain-based tokens

Roadmap for Blockchain Applications



Cyber Security

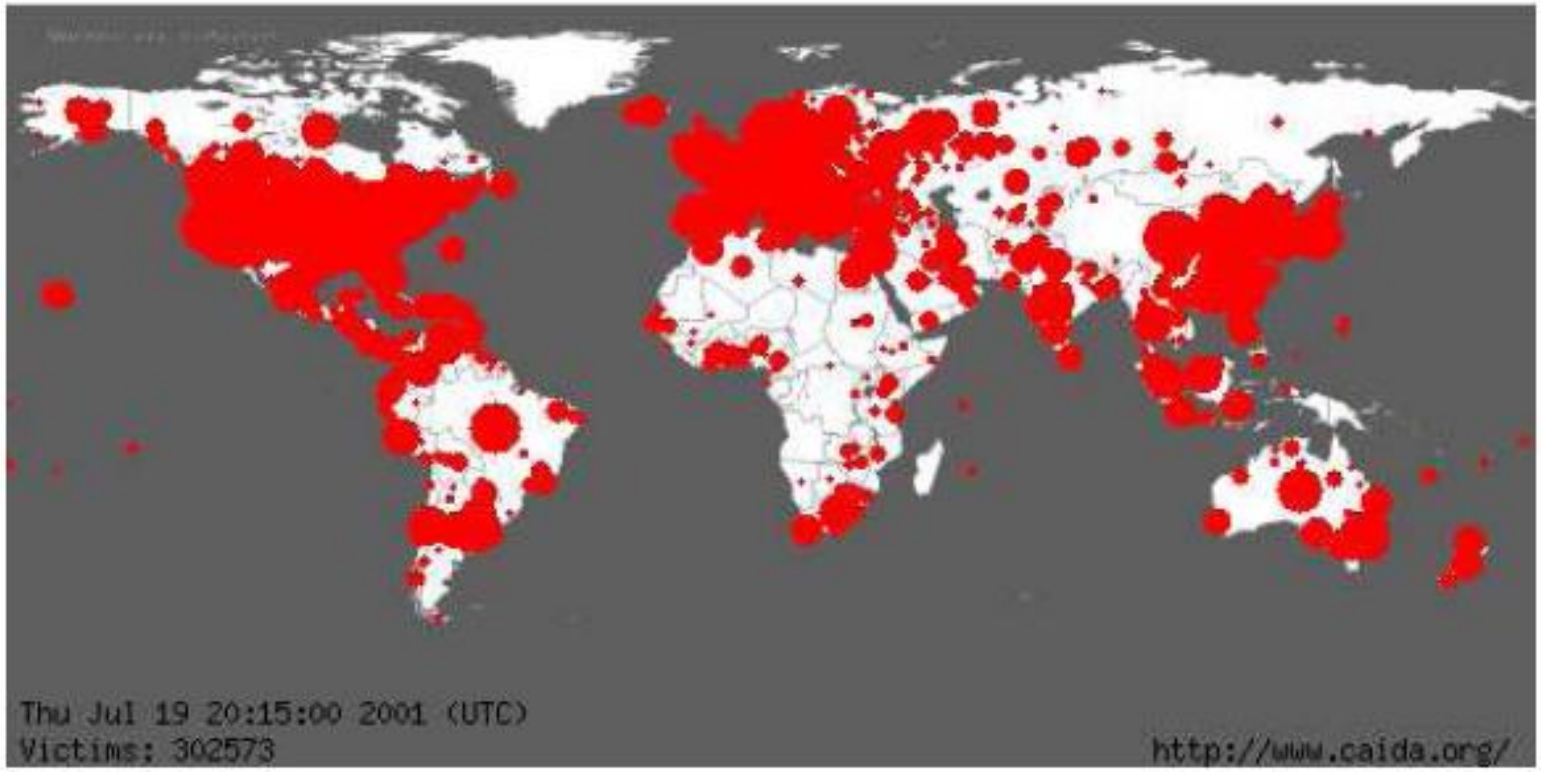
Code Red Worm



July 19 01:05:00 2001

19 Hours Later

Code Red Worm



July 19 20:15:00 2001

CyptoLocker Ransomware

- **CryptoLocker** is a ransomware Trojan which targeted computers running Microsoft Windows.

- It propagated via infected email attachments, and via an existing botnet.

- When activated, the malware encrypts certain types of files stored on local and mounted network drives using RSA public-key cryptography, with the private key stored only on the malware's control servers.

WannaCry Ransomware

- One of the biggest cyber attacks in history.

- The **WannaCry** ransomware attack has hit about 150 countries globally, including Russia and the US. Infected computers were running on older versions of Microsoft operating systems like XP.

- The ransomware locks user's devices and prevents them from accessing data and software until a certain ransom is paid to its creator. In this case, cyber criminals have demanded a fee of about $300 in crypto-currencies like Bitcoin for unlocking the device.

- **WannaCry** propagates using EternalBlue, an exploit of Windows' Server Message Block (SMB) protocol. This is used to compromise windows machines, load malware, and propagate to other machines in a network. The attack uses SMB version 1 and TCP port 445 to propagate.

Petya

- **Petya** targeted Windows machines.

- Infecting the master boot record that displays the ransom note. Encrypts file system table MFT. Prevents from booting. Original Petya does not encrypt files one by one. Variants encrypt the first MB of files.

- May be using EternalBlue.

Other Major Breaches in Recent Times

- The **2011 PlayStation Network attack** was the result of an "external intrusion" on Sony's Playstation Network in which personal details from approximately 77 million accounts were compromised and prevented users of PlayStation 3 and Playstation Portable consoles from accessing the service.

- **Operation Aurora** exploited zero-day vulnerability in Microsoft Internet Explorer.

- **Mirai** is a malware that turns networked devices running Linux into remotely controlled "bots" that can be used as part of a botnet in large-scale network attacks. It primarily targets online consumer devices such as IP cameras and home routers. Launched DDoS attacks.

Other Major Breaches in Recent Times

- **Stuxnet** exploited four previously unknown vulnerabilities. First virus to include code to attack Supervisory Control and Data Acquisition (SCADA) systems. Duqu and Flame were in similar lines.

- **Google Is Fighting A Massive Android Malware Outbreak** -- Up To 21 Million Victims.

- **Heartbleed** in OpenSSL's implementation allows attackers to read portions of the affected server's memory, potentially revealing users data, that the server did not intend to reveal.

ComputerWeekly.com

Add your search term here SEARCH

RSS Email Newsletters

HOME | IT MANAGEMENT | NETWORKS AND COMMUNICATIONS | SOFTWARE | HARDWARE | RESEARCH | JOBS

Desktop Software

Send to a friend Print

Trojans offer new online banking threat

Posted: 18:38 02 Mar 2006
Topics: Viruses & Virus Protection | Security

BOOKMARK

MessageLabs has warned that cyber criminals are surfing into online banks alongside customers to steal their money in response to the increased adoption of stronger authentication.

Instead of stealing user names and passwords, the new 'bank-stealing Trojans' wait until their would-be victim has logged into their bank account, then transfer their money out.

The bank-stealing Trojans are programmed to work with specific online banking websites, and typically arrive in an email with an apparently innocent web link - for example, to an online greeting card. If the user clicks on it, they will download an executable that installs itself into their browser and then waits until he or

RELATED CONTENT

CW Articles | Web Content

- Twin Trojans use PowerPoint to spread
- Briefs: Vulnerabilities found in Trend Micro, Firefox browser
- Online banking popularity soars
- Does Staroffice offer business a real alternative to Microsoft?
- Online banking usage grows 174%

FEATURED BLOG

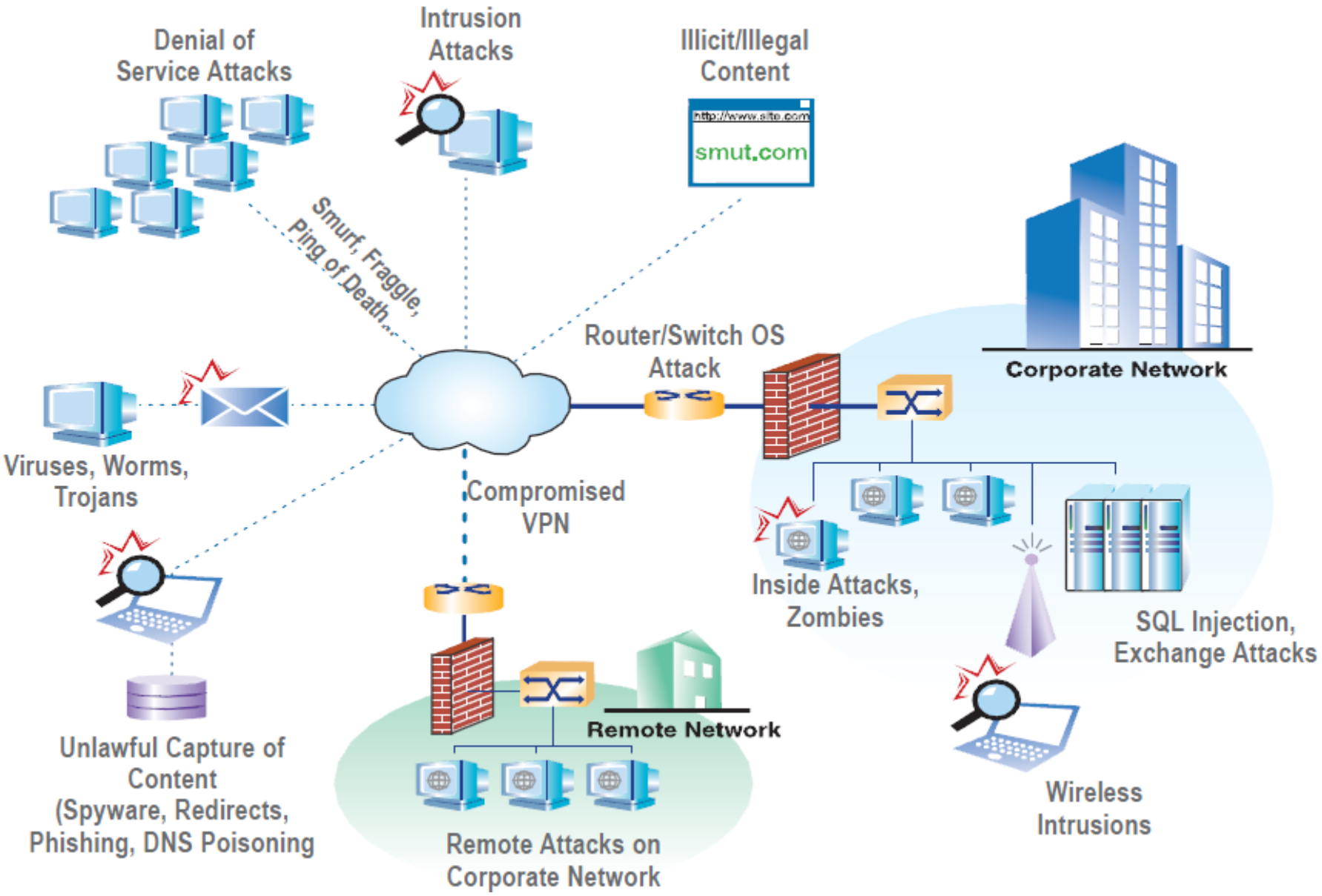
Predicting the outcome of events

Security breach or breakdown of system due to security issues can lead to

- Loss of new business opportunity
- Loss in existing business
- Loss of credibility
- Losing competitive edge over the competitor

All these ultimately result in monetary losses

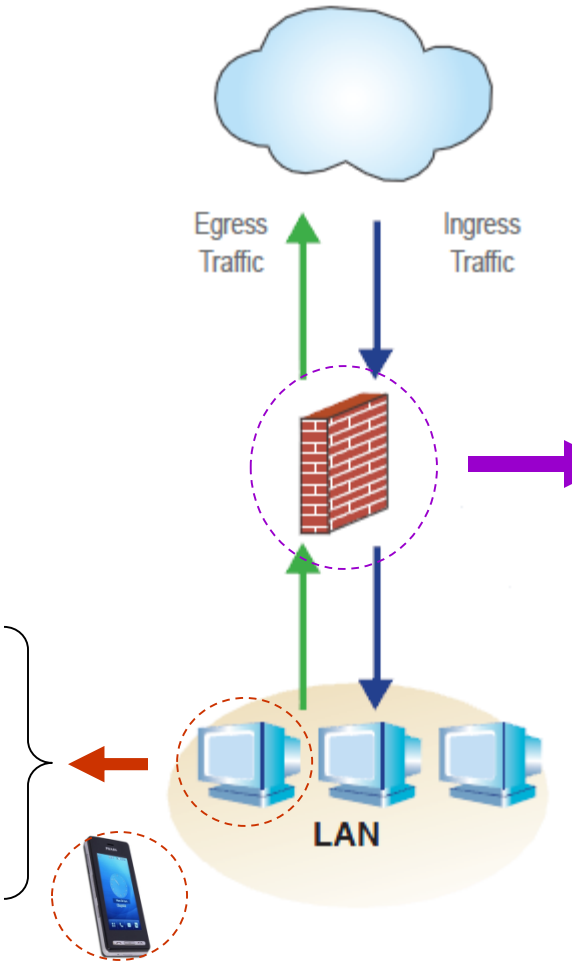
Computer Network - Security Threats



Core Pillars of Information Security

- Confidentiality – only allow access to data for which the user is permitted
- Integrity – ensure data is not tampered or altered by unauthorized users
- Availability – ensure systems and data are available to authorized users when they need it

Security Deployment



- ✓ Anti Spyware
- ✓ Anti Virus
- ✓ IPS
- ✓ VPN
- ✓ UTM
- ✓ Threat Intelligence

End Point Security Management

- ✓ Anti Virus (Signature, Behavior & heuristic based)
- ✓ Desktop Firewall
- ✓ App Control, Device Control
- ✓ Host IDS
- ✓OS Hardening
- ✓Trusted Execution Environment

Vulnerability/Patch/Alarm Cycle

Evolution of Cyber Attacks

- Cyberattacks have evolved in complexity and sophistication since 1988 (with Morris Worm).
- Worms and viruses to advanced persistent threats and certificate-based attacks.
- Cybercrime costs the global economy over $400 billion annually.
- Juniper research prediction
  - Rapid digitization of consumers' lives and enterprise records will increase the cost of data breaches to $2.1 trillion globally by 2019

Blockchain Technology in Cyber Securtiy

- As cybercrime is becoming more sophisticated, so too is the field of cyber security.

- Efforts are made to protect computer systems and the information from various security threats.

- **Blockchain technology** will become **very common in enabling cybersecurity** in the near future.

Why Blockchain for Cyber Security?

- Blockchain can provide the transparency and auditing
  - Include user identity security, transaction and communication security and the protection of critical infrastructure
- Helps to realize more efficient and secure software development and supply chain risk management
- Enables us to make the most use of shared online services whereas eliminating the potential security and privacy issues

Blockchain Features relevant to Cyber Security

- Resolving Trust
- Transactions
- Transparency
- Accountability
- Immutability

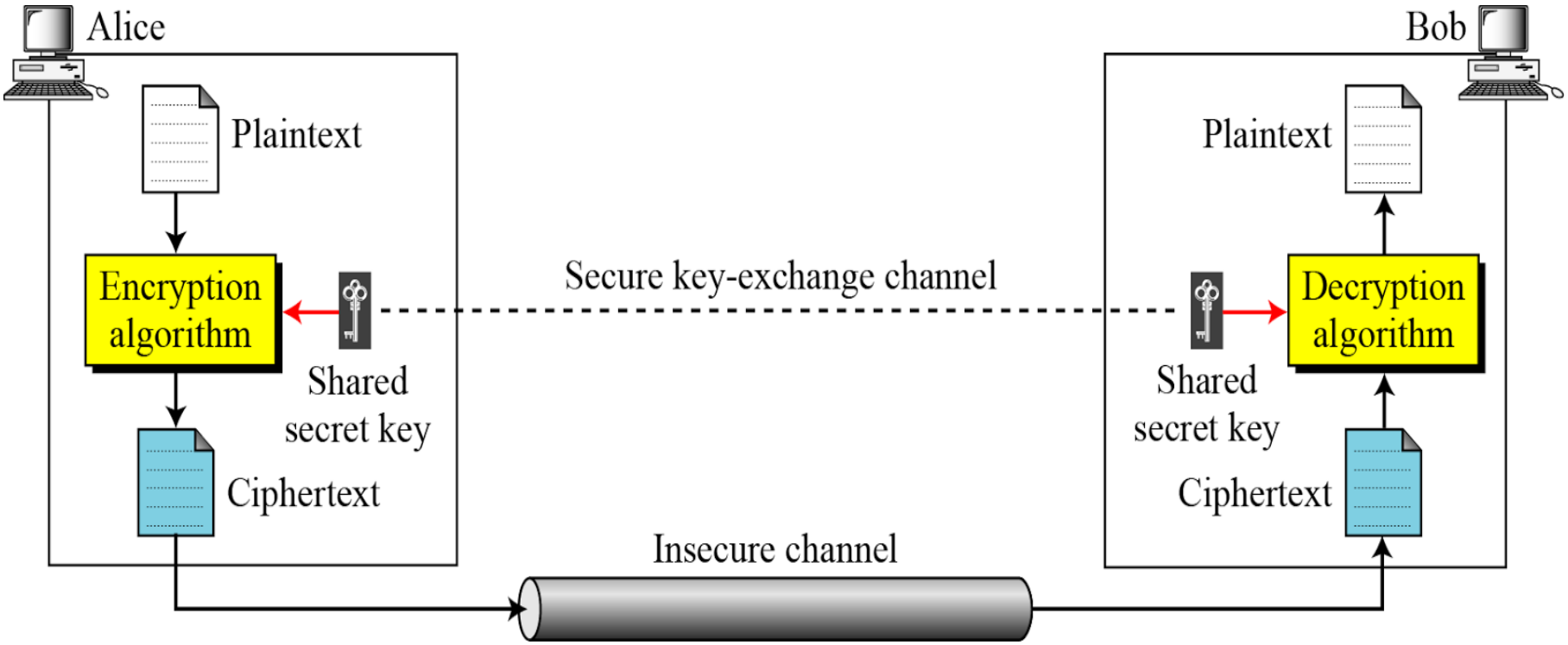
Need for Authentication

- Authentication
  - process by which an account is confirmed to belong to or be associated with a particular owner.

- Robust authentication process is required if secure transactions are to successfully take place between a large number of parties.

- If a transaction takes place without prior authentication of the parties involved, leads to man-in-the-middle kind of attacks.

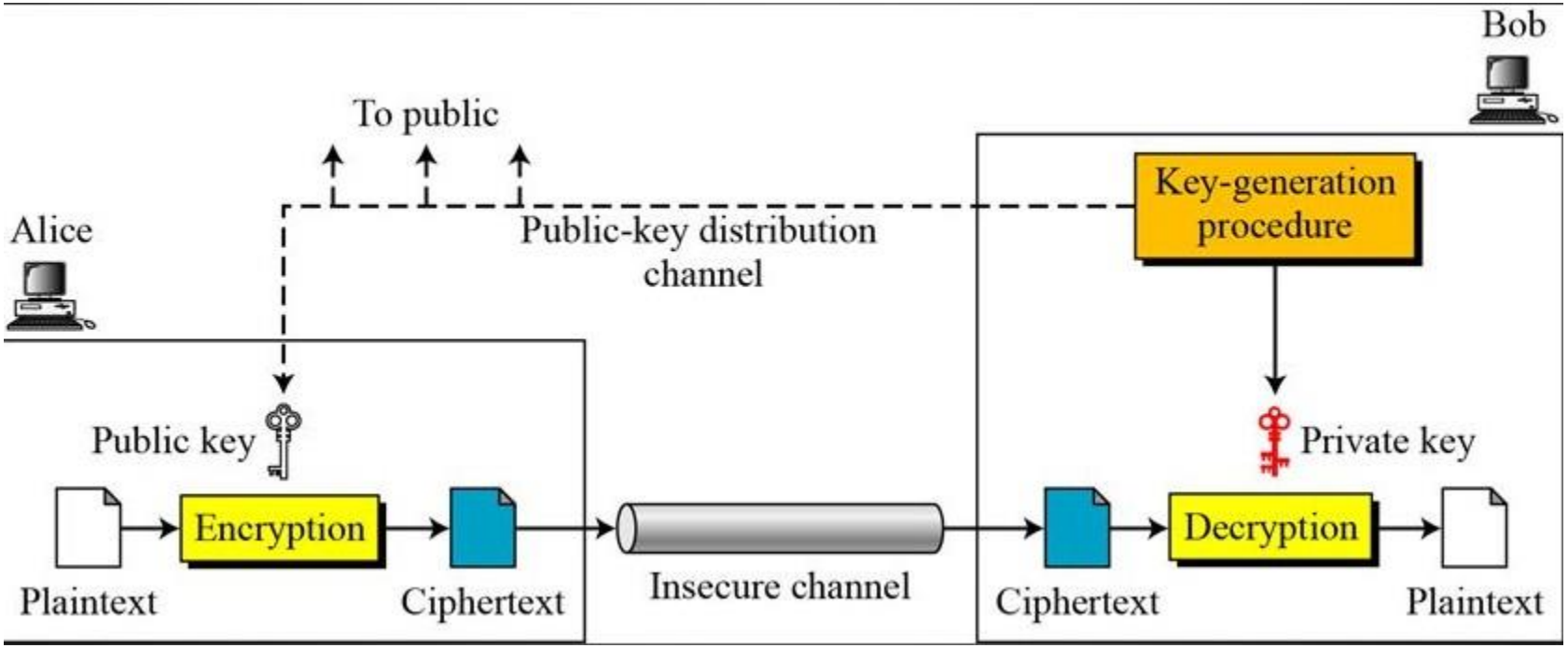
Symmetric Key Algorithms



Symmetric Key Algorithms

- Both parties need to share the key using secure channel.
- It is not scalable for users wishing to transact with multiple parties given the need to agree on a different symmetric key with each different party.
- It is not secure for use with untrusted parties, given that the other party can provide others with the key.

Public Key Cryptographic Algorithms



Public Key Cryptographic Algorithms

- Public-key cryptography enables parties to securely send and receive data from one another
- Limitations
  - It does not authenticate that a public key is truly associated with a user
  - User's public key is available to everyone, no guarantee that data is coming from the presumed sending party

Trust Models (Managing Public Keys)

- Web of Trust
  - Certified Entities are people
  - Theoretically simple and resistance to compromise
  - Dependency on people and lack of dedicated central management
  - Revocation becomes complicated

Trust Models (Managing Public Keys)

- Certificate Authority (CA)
  - A Certification Authority (CA) is a trusted third party issues digital certificates.
  - No dependency on people
  - Scalable
  - Procedures in place for revocation
  - It creates a single point of failure which can have terrible consequences when compromised

Certificate Authority Failures

- VERISIGN
- TRUSTWAVE
- DIGINOTAR

Blockchain based PKI

- Need:
  - Webs of Trust is not scalable
  - CAs are potential central points of failure in PKI
- Blockchain has implicit transparency and auditing features and eliminates the need for central trusted third party
- If PKI is maintained on a blockchain, single computer is replaced by a group of connected computers making it more robust and trustworthy

Blockchain based PKI – Ongoing Efforts

- POMCOR
  - Involves CAs. It stores a hash of the certificate in a blockchain ledger.
  - Revoked hashes are stored on a second blockchain ledger.
  - A user wishing to authenticate another party will confirm that their certificate is included in the first ledger, and also not included in the revoked ledger.
  - Pomcor has also developed the concept of a 'rich credential', which can be used to identify a user. It requires users to present a password, their private key, and biometric data such as voice or facial structure.

Blockchain based PKI – Ongoing Efforts

IOTA

- Eliminates the central point of failure.
- Transactional settlement and data integrity layer for the Internet of Things.
- Tangle - which overcomes the inefficiencies of current Blockchain designs and introduces a new way of reaching consensus in a decentralized peer-to-peer system.
- Tangle requires that all users algorithmically choose two previous transactions to essentially *mine* in order to complete one of their own transactions, thus making Tangle an extremely scalable blockchain-based authentication solution.
- Verification process is decentralized amongst the users, removing the risk of a central point of failure.

Blockchain based PKI – Ongoing Efforts

- CERTCOIN
  - It completely decentralized and without a single point of failure.
  - When new domain names are purchased through Certcoin, the purchaser is directly provided public and secret keys once the transaction is posted. Transactions are posted with transaction fees, incentivizing miners to include their information in the blockchain.
  - User's public key being hashed into a block.
  - Certcoin is also a highly scalable solution

Logging and Integrity Management (Provenance) for Cloud using Blockchain Technology

- Verifiable supply chain of data which can provide history and traced back towards accountability. Includes verifying the data at rest.

- The ability of all users holding account on cloud to verify the transactions gives assurance to end user especially while using the third party cloud service provider.

- Provide clear audit trail for data transactions which helps to detect data breaches / forensic analysis.

- Protects from various cyber security threats such as code injections, Advanced Persistent Threats (APTs), Zero-day exploits etc.

IoT Privacy and Security Challenges

- Heterogeneity in device resources
- Multiple attack surfaces
- Centralized control
- Scale
- Context specific risks
- Poor implementation of security / privacy mechanisms in off-the shelf products

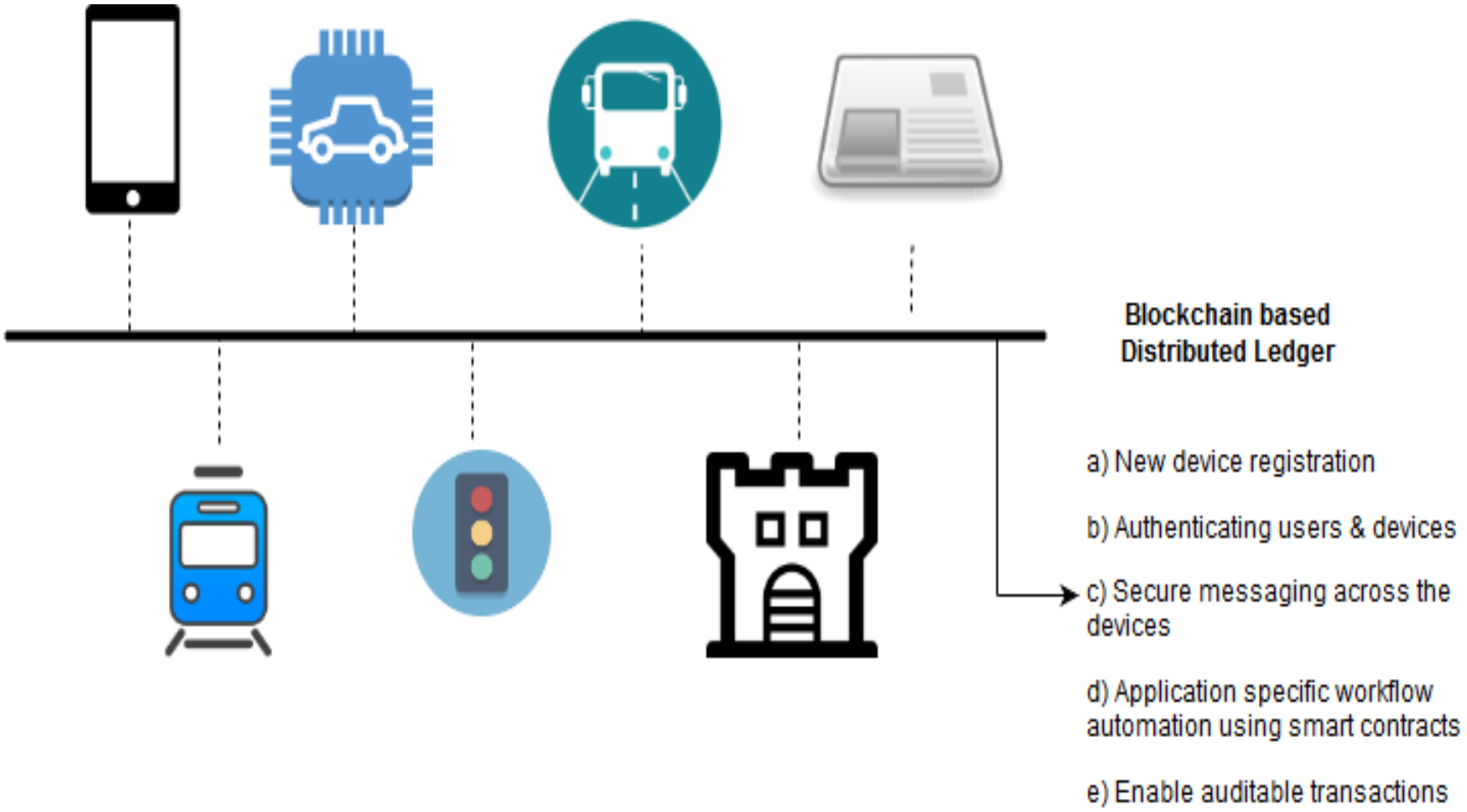
Need for a new approach to IoT security - away from the current centralized model.

Decentralized IoT Networks and Blockchain Technology

- Decentralized approach must support three fundamental functions:
  - Peer-to-peer messaging
  - Distributed data and file sharing
  - Autonomous device coordination

- Blockchain technology is the missing link to settle scalability, privacy, and security concerns in IoT

Decentralized IoT Networks and Blockchain Technology



Decentralized IoT Networks and Blockchain Technology

- Blockchain technology can be used in tracking billions of connected devices
- Enable the processing of transactions and coordination between devices
- Decentralized approach would eliminate single points of failure
- More resilient ecosystem for devices to function
- The cryptographic algorithms used by blockchains, would make consumer data more private.

Prevention of DDoS Attacks

- **Centralized vs. decentralized**
  - Current applications / services use centralized servers that can result in DDoS.
  - A decentralized platform allows users to rent out their bandwidth
    - which can then be pooled to allow for substantially greater amounts of data processing, greatly reducing the risk of DDoS success.

Distributed DNS

- DNS Protocol was originally designed with no security protection in place.
- DNSSEC added a layer of trust on top of DNS by providing authentication, but it still did not address issues such as DoS/DDoS attacks
- Blockchain-based DNS alternatives (Namecoin and Blockstack) - is a promising approach to build decentralized, secure and human-friendly naming systems

Anti Malware Solutions using Blockchain Technology

- BitAV: Fast Anti-Malware by Distributed Blockchain Consensus and Feedforward Scanning
- Decentralised firewall for malware detection
- Malware detection using blockchain consensus

Protection from Supply Chain Attacks

- Dependence on foreign supply chains
- Blockchain based solutions can be used to secure the supply chains
- Enabling forensics to detect malicious activity

Conclusion

- Blockchain has promising applications in Cyber Security
- Challenges to be addressed
  - Security for Blockchain
  - Standards
  - Bandwidth, Computational power and storage
  - Choosing for right applications

Endpoint Security Solutions @ C-DAC

- M-Kavach
  - www.cdac.in/mkavach
- USB Pratirodh
  - www.cdac.in/usbpratirodh
- AppSamvid
  - www.cdac.in/appsamvid
- Browser JSGuard
  - download from chrome and mozilla repositories
- Application and Device Control
  - Enterprise version
- Hardened Android

Thank You