Information Security Education & Awareness
Ministry of Electronics and Information Technology
Government of India

InfoSec
Newsletter
Mar-Apr 2019

BLOCKCHAIN TECHNOLOGY

सी डैक
CDAC
प्रगत संगणन विकास केन्द्र
CENTRE FOR DEVELOPMENT OF ADVANCED COMPUTING
इलेक्ट्रॉनिकी और सूचना प्रौद्योगिकी मंत्रालय की वैज्ञानिक संस्था, भारत सरकार
A Scientific Society of the Ministry of Electronics and Information Technology, Government of India
Plot No: 6&7, Hardware Park Sy. No.1/1, Srisailam Highway Raviryal (V & GP), Via Ragsanna guda, Maheshwaram (M), Ranga Reddy District, Hyderabad - 501510Telangana(India)
Nalanda Building, No. 1 Shivabagh Satyam Theatre Road, Ameerpet, Hyderabad - 500016, Telangana (India)

InfoSec
Newsletter
Mar-Apr 2019

CREDITS

Honorary Professor. N Balakrishnan
(IISc, Bangalore)
Prof. Sukumar Nandi
(IIT, Guwahati)
Prof. V Kamakoti (IIT, Madras)
Prof. M S Gaur (SVNIT, Jaipur)

Design & Technical Team
Ch A S Murty
K Indra Veni
K Indra Keerthi
P S S Bharadwaj

Action Group Members
HoD (HRD), MeitY
Shri.Sitaram Chamarthy (TCS)
Prof. M S Gaur (MNIT, Jaipur)
Prof. Dr.Dhiren R Patel
(NIT Surat)
Representative of Chairman
(CBSE)
CEO, DSCI (NASSCOM)
Representative of Prasar Bharati,
Member of I & B
Shri U Rama Mohan Rao
(SP, Cyber Crimes, CID,
Hyderabad, Andhra Pradesh)
Shri S K Vyas, MeitY

Compiled by
E Magesh, Director
G V Raghunathan
Ch A S Murty
M Soumya
M Jagadish babu

From C-DAC
E Magesh, Director

Acknowledgement
HRD Division
Ministry of Electronics &
Information Technology

Supported by
For Virus Alerts,Incident & Vulnerability Reporting
certin
Handling Computer Security Incidents

Message from
E Magesh
Director, C-DAC Hyderabad

'Blockchain' the new and upcoming technology has gained a strong foothold around the world with respect to the potential it has in reforming mainstream industries including retail, banking, healthcare, finance, logistics, and others. Leading IT companies, Banks, Industries, State and Central government are striving to set a mark in the online space by using blockchain technology. Even government is exploring various initiatives to incorporate the technology to bring more visibility into governance. As a distributed ledger technology, blockchain guarantees enhanced security, greater transparency, increased efficiency, improved traceability, and reduced costs. Blockchain can become a history-altering technology that will lead our country forward.

At present we are living in a world were Internet has become a prime necessity and this online world keep introducing a multitude of threats, sophisticated cyber attacks and also raises concern over the security and privacy of digital information we hold. With blockchain, many of the issues may be fixed mainly because of the security it offers. But any technology has weak points, and the blockchain is no exception. Just as blockchains have unique security features, they also have unique vulnerabilities and in current scenario these vulnerabilities are mostly theoretical.

The newsletter 'Blockchain Technology' helps the reader to understand the concept behind blockchain and also look at the various attack vectors and how blockchain can save our privacy before it disappears. Hope this newsletter will help in creating awareness about the challenges issues and benefits of using blockchain technology which will be a major player in the digital transformation of our country.

Connect us with /informationsecurityawareness
Follow us at /infosecawa
Subscribe us at /informationsecurityawareness
Follow us at /infosec_awareness

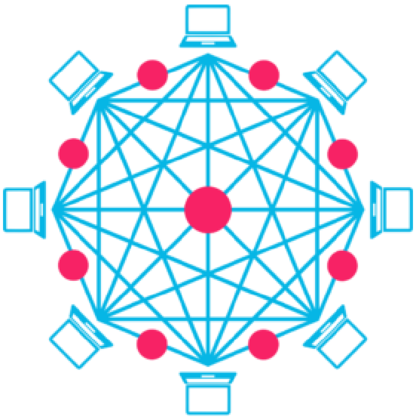
BLOCKCHAIN TECHNOLOGY

What is a Blockchain?

A blockchain is, in the simplest of terms, a time-stamped series of immutable records of data that is managed by cluster of computers not owned by any single entity. Each of these blocks of data (i.e. block) are secured and bound to each other using cryptographic principles (i.e. chain).

Blockchain Technology

Blockchain technology is defined as a distributed ledger system which is used to record data/ transactions across multiple computers. It makes it difficult for any type of data breaches, identity thefts, cyber-attacks or foul play in transactions. This ensures that the data remains private and secure.



Blockchain technology has seeped into every sphere of lives from banking to healthcare and beyond. By removing much of the human element from data storage, blockchains significantly mitigate the risk of human error, which is the largest cause of data breaches.

Blockchain Technology records transactions in Digital Ledger which is distributed over the Network thus making it incorruptible.

In short, Blockchain is explained as follows

- It is a decentralized database which stores information in the form of transactions
- It can be public or private
- Stored data is Immutable (Data once recorded cannot be changed)
- Highly secure (Because owned by multiple computers)
- Data gets recorded via consensus-based algorithms
- Uses cryptography (for verifying the data & sender)
- Generally, exist over peer-to-peer network

"Blockchain is a general agreement-based secure decentralized public database which stores information immutably over peer-to-peer network"

Trust of Blockchain

Blockchain enhances trust across a business network through the following five attributes:

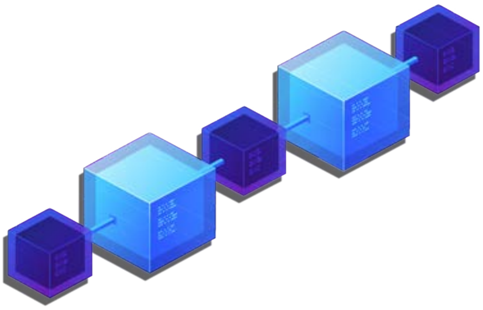
- **Distributed:**The distributed ledger is shared and updated with every incoming transaction among the nodes connected to the Blockchain. All this is done in real-time as there is no central server controlling the data.
- **Secure:** Every transaction is signed by end-user, which allows for the verification using public key and trusted certificate of the end user.
- **Transparent:** Because every node or participant in Blockchain has a copy of the Blockchain data, they have access to all transaction data or data of their interest. They themselves can verify the identities without the need for mediators.
- **Consensus-based:**All relevant network participants must agree that a transaction is valid. This is achieved through the use of consensus algorithms.
- **Flexible:** Smart Contracts which are executed based on certain conditions can be written into the platform. Blockchain Network can evolve in pace with business processes.

Benefits of Blockchain Technology

- **Time-saving:** No central Authority verification needed for settlements making the process faster and cheaper.
- **Cost-saving:** A Blockchain network reduces expenses in several ways. No need for third-party verification. Participants can share assets directly. Intermediaries are reduced. Transaction efforts are minimized as every participant has a copy of shared ledger.
- **High-security:** No one can tamper with blockchain data as it is shared among millions of participants. Cybercrimes and fraud can be minimized by the use of blockchain technology.

The following are three principal technologies that combine to create a blockchain

1. Public Key cryptography and Hash Algorithms
2. A distributed network with a shared ledger
3. An incentive to service the network's transactions, record-keeping and security.



Application domains of Blockchain Technology

Blockchain technology was primarily invented for bitcoins (a leading digital virtual currency). In bitcoin application, every user is allowed to connect to the network, send new transactions to it, verify transactions, and take part in the competition to create new blocks, known as mining. Blockchain being a distributed ledger has many other applications in finance industry. More specifically finance industry is gazing at Blockchain technology to improve efficiency and transparency. It may help customers with faster payments and at the same time financial institutions may look for transparency in the system. But, in financial industry also it is not limited to making and receiving payments. For example, NASDAQ has started block chain based system for market which connects institutional investors with companies that are not listed on exchange (for issuance, transfer and management of private company securities). Blockchain can benefit financial industry in various ways such as Initial booking of the trade, calculation of the premium paid, payment of the premium, calculations of accrued interest for the fixed and floating legs of the trade on each, coupon date, payment of interest on each coupon date, foreign exchange revaluation entries during the course of the trade, termination of the trade and also for payment of various taxes.

Blockchain technology has potential in other industries as well. It has applications in Governance, healthcare, security, automobiles, media, travel, hospitality, energy, smart cities etc.

Specific applications include tracking taxpayer money, online voting, tracking database records for different Governance applications, smart contracts, smart payments, music payment & licensing, decentralized Internet of Things (IoT), authenticity of a review, notary, Supply-Chain Communications & Proof-of-Provenance, Rural Payments, Corporate Audits, Patient Data Management and Global Wallets.

Blockchains Aren't Unhackable

However, powerful as blockchains may be, they are not immune to attack. Any technology has weak points and attack vectors, and the blockchain is no exception. Here we will explore the various vectors of attack (in order of increasing threat) and take a look at some examples of each from the short but exciting history of cryptocurrency so far.

Sybil Attack

A Sybil attack is an attack in which a huge number of nodes on a single network are owned by the same party and attempt to disrupt network activity through flooding the network with bad transactions or manipulating the relaying of valid transactions.

These attacks are theoretical so far and for the most part, may never be seen, as one of the fundamental design decisions made when developing a cryptocurrency system is how to prevent Sybil attacks.

Bitcoin prevents them through its Proof-of-Work algorithm, requiring nodes to spend resources (in the form of energy) to receive coins, thereby making owning the vast majority of nodes very expensive. Different projects handle Sybil-resistance differently, but nearly all handle it.

Routing Attack

A routing attack is an attack made possible by the compromise or cooperation of an Internet Service Provider (ISP). While it's technically possible to run a Bitcoin (or other coins) node anywhere in the world, the current reality is that nodes are relatively centralized right now in terms of the ISPs that carry the internet traffic to and from.

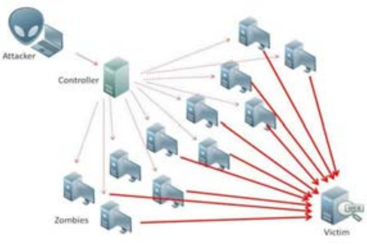
According to research done by ETHZurich, 13 ISPs host 30% of the Bitcoin network, while 3 ISPs route 60% of all transaction traffic for the network. This a major point of failure if an ISP were to be compromised to corrupted.

A routing attack works by intercepting internet traffic being sent between Autonomous Systems, top-level nodes in the architecture of the internet, of which there are few enough to intercept with relative ease. This is a phenomenon seen commonly, even daily, on the internet in the wild and can certainly be used against Bitcoin or other cryptocurrency traffic.

Using this method, a cryptocurrency network could be partitioned into two or more separate networks, exposing either side of the partition to double-spending attacks because they cannot communicate with the entire network to validate transactions. Once coins were spent on one side of the network and goods or services received, the partition could be removed and the side of the network with the shorter chain would be rejected by the network as a whole and those transactions would be wiped out.
As far as we know, this kind of attack has not occurred, and there are steps that can be taken to make coins immune to this behavior.

Direct Denial of Service

A Direct Denial of Service (DDoS) attack is an attempt by bad actors to cripple a server, anything from a website to a Bitcoin node, by flooding it with high volumes of traffic. This is definitely one of the more common attacks seen in the wild, as it's relatively easy to purchase a DDoS attack from any number of disreputable "hackers" or firms out there.



In the case of a website, this looks like a huge volume of requests to the server being sent continuously over a period of time, preventing legitimate requests from receiving the resources they need. In the case of a Bitcoin node, this looks like huge volumes of small or invalid transactions being sent in an effort to flood the network and prevent legitimate transactions from being processed.

Major networks like Bitcoin are constantly under attack from DDoS attempts, but design decisions made in the development of the Bitcoin network act to mitigate the risk of DDoS attempts. In the face of a successful DDoS attack, there is no threat of stolen funds or compromised security, simply a halting of network activity.

Bitcoin's Backlog Blues

However, while not a security risk, this interruption of service can be used for other agendas. There's something of a saga when it comes to "spam" transactions (DDoSing the network with lots of transactions) and Bitcoin that played out from 2015 to 2017.

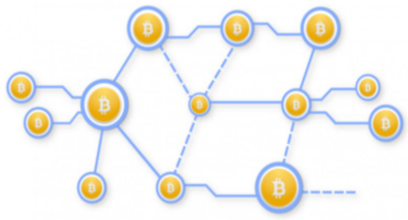
In June of 2015, Coinwallet.eu (a now defunct wallet company), conducted a "stress test" of the Bitcoin network by sending thousands of transactions on the network in an effort to influence the controversial block-size change debate that was raging at that time, stating in their announcement post that they set out "to make a clear case for the increased block size by demonstrating the simplicity of a large scale spam attack on the network."

A month later, in what is called the "flood attack," 80,000 tiny transactions were simultaneously sent on the Bitcoin network, creating a massive backlog that was cleared out only by the efforts of F2Pool, one of the largest mining pools at the time, which dedicated an entire block to combining all of the spam transactions and clearing them.

Over the course of the next year, according to analysis by LaurentMT, the creator of the Bitcoin analytics tool OXT, many thousands or even millions more spam transactions (mostly tiny, useless transactions that could not possibly have been legitimate) were sent out, clogging the Bitcoin UTXO backlog, but these transactions were for the most part ignored by the major mining pools.

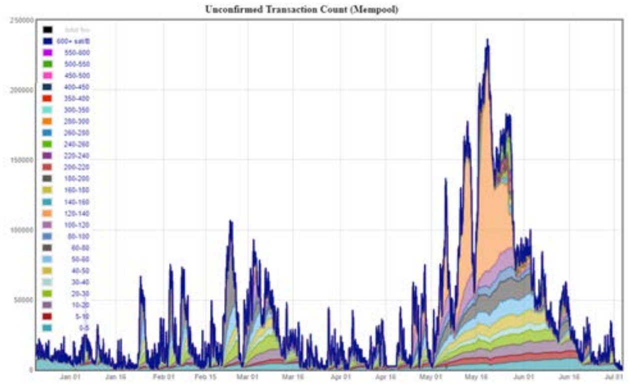
Suddenly, in the second half of 2016 and all right around the same time, the major mining pools at the time began accepting these spam transactions into blocks, reducing the throughput of legitimate transaction just as the block-size debate was ramping up again and many of the pools were rumoured to be siding with the "big-blockers" over the small blockers.

The Bitcoin network has since cleared out this backlog and is humming along, while the big-block fans have moved their attention to Bitcoin Cash, a project that Jihan Wu (founder of Bitmain the largest owner of Bitcoin hashpower by far) is fully supportive of. Do your own research.



51% or Majority Attack

Since the security of a blockchain is directly linked to the computer power building the chain, there is the threat of an attacker gaining control over a majority of the hash power on the network. This would allow the attacker to mine blocks faster than the rest of the network combined, opening the door to 'double-spending.'



Double-spending is a method of defrauding a cryptocurrency that involves submitting transactions to the chain, receiving the good or service that transaction pays for, and subsequently using the majority hashpower to fork the blockchain at a point prior to the transaction. This effectively erases that transaction from the chain history, allowing the attacker to transact with those same coins a second time.

Obtaining a majority of hashpower would

not allow an attacker to create coins, access addresses or compromise the network in any other way, which limits the damage this method enables. The biggest effect of such an attack may well be the loss of confidence in the network that is attacked, and a subsequent plummet in asset price of any token on the network.

This sort of majority attack is very expensive to pull off, and as a result, in reality, only relatively small and low-hashpower coins are susceptible to this attack vector. Major coins like Bitcoin have little to fear from a 51% attack due to the fact that any attacker with the vast majority of hashpower would have more incentive to simply mine all of the blocks and receive the Bitcoin than to attempt to an attack, especially considering the price of their stolen Bitcoin would collapse if the news of an attack got out.

51% in the Wild

One of the more interesting examples of 51% attacks in the wild comes courtesy of a group of hackers that called themselves the '51 Crew.' In the second half of 2016, the 51 Crew began holding small Ethereum clones for ransom, capitalizing on their low hash rates and centralized mining distribution to rent enough hardware to corner the network.

Claiming their "intention is not to wreck a project" and they were doing this just make money, they demanded Bitcoin in exchange for shutting down their operation and leaving the projects in peace. If the demands were not met, they would fork the coin's blockchain to a point prior to large sales the crew had already made on exchanges.

The projects in question, Krypton (now defunct) and Shift (still traded at small volume), both refused to pay the ransom and subsequently had their blockchains forked. The project teams scrambled to shore up network decentralization and make changes to the protocols to prevent such abuses, but not before taking quite a hit.

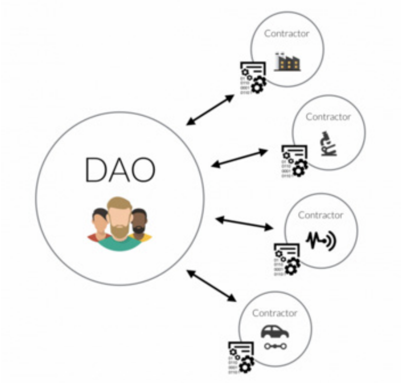
Cryptographic Vulnerabilities

The attacks outlined so far deal mostly in the realm of either double-spending or reduction in network service. The attacks are expensive to pull off and are quickly corrected by the network's own self-repairing features. While they could be real threats to the confidence in a cryptocurrency and result in a minimal loss of funds, they are relatively small potatoes.

As with any computer system or network, the largest attack vector is human error. The major losses of funds seen so far in cryptoland are a result of bugs in the software of the coin itself. Cryptographic errors in the security of cryptocurrencies leave security holes that can be discovered and exploited by sophisticated hackers to undermine a project.

The DAO

Perhaps the most visible example of a hack enabled through shoddy code is the infamous Ethereum DAO hack, so bad it spawned a whole new cryptocurrency and haunts the Ethereum project to this day.



The DAO (Decentralized Autonomous Organization) was a leaderless organization built on top of Ethereum using smart contracts. The idea was to give anyone the ability to invest in the company and vote on projects they wanted to be funded, all managed securely and automatically by the DAO smart contract code.

If you invested in the DAO (by purchasing DAO tokens) and then later decided to pull out, there was a mechanism for this by which you could have your Ethereum returned to you in exchange for your DAO tokens. This is the mechanism called the 'Split Return' that was exploited by a pioneering DAOist on June 17, 2016.

The Split Return is a two-step process: return the proper amount of Ethereum to the token holder triggering the return, then take the tokens and register the transaction on the blockchain to update the DAO token balance. The unknown hack-

er realized that he could trick the system into repeating the first step without moving onto the second, which enabled them to siphon $50million worth of Ethereum out of the DAO and into a separate DAO controlled only by the attacker.
This obviously enflamed the Ethereum community, and a plan to soft-fork and recover the funds was made. A soft fork would have been minimally invasive, backward-compatible and simply 'erased' the DAO hack from the blockchain. Once the plan was made, however, it was realized that it would not fly and a hard fork would be necessary. This was controversial and resulted in the creation of Ethereum Classic (ETC), a continuation of the original Ethereum chain with the DAO hack in place, and Ethereum (ETH), the newly hard forked project that continued to DAO another day.

The Real Threat is Users, Not Hackers

Blockchain technology is robust and promising, and even with all of these possibly attack approaches very few successful attacks have gone down in history. This hasn't prevented vast amounts of money being stolen from users, however.

While the security of most cryptocurrencies remains intact, the security of the wallets, exchanges, and accounts of third-party services around these cryptocurrencies remains almost laughably bad. Millions upon millions of dollars worth of Bitcoin and other cryptocurrencies have been stolen from the compromised accounts of individuals and exchanges over the years.

While the attacks outlined above are mostly theoretical and are being defended against actively, the glaring hole in the security of Bitcoin and any other cryptocurrency is the fact that humans aren't so great at paying attention and being vigilant. Reusing passwords, falling victim to phishing scams, careless website operators and negligent exchange employees continue to be the single most dangerous point of failure when it comes to the health of the crypto economy.

As we move forward, there may well be some blockchain level attacks perpetrated. These may come from huge powers like governments or corporations set on controlling or undermining these promising new means of storing and transferring wealth and value. In the long run, however, attacks like these will only act to strengthen and evolve the technology to be more resistant and robust.

But much more than this, there will need to be great leaps and bounds made in the ease of use and security of consumer crypto products before real adoption can occur. As long as one accidentally shared a password or left open laptop can mean the loss of your life savings, we can't enter a world run on crypto.

Known Hacks on Blockchain

Recent hacks have proven that blockchain is not impregnable.

- **Nicehash hack, Dec 2017 -** Cryptocurrency amounting to $64 million Bitcoin is said to be stolen from cryptocurrency mining marketplace NiceHash, emptying its entire bitcoin wallet.
- **CoinDash ICO hack, July 2017 -** CoinDash, a blockchain start-up, aimed at raising capital for cryptocurrency social trading by selling their digital tokens in exchange for Ethereum. On 17th July, the day of ICO sale, on 3 minutes after the start of the sale, CoinDash website was compromised. The address for sending investments was changed with a fake address and investments were funded to the attacker's account. Around $7.4 million Ethereum was stolen during this hack.
- **Krypton (KR) & Shift (SHF), Aug 2016 -** Attackers targeted Ethereum-based Blockchains as the cryptocurrencies, Krypton (KR) and Shift, both Ethereum type coins using the version of 51% attack. The attackers could exploit the Blockchain with a two-step attack. Overpowering the network with 51% attack to ensure rollback on transactions and spending the coins twice; and employing DDoS nodes to enhance network power. The attack led to the loss of 21,465 KR, $3000 at the time.

- **Steemit, July 2016 -** The Blockchain-based blogging platform, was hacked. Vulnerability on the Web browser front end and not on the cryptocurrency itself led to this attack. Around 250 user accounts were compromised, resulting in the loss $85,000 worth of Steem Dollars and cryptocurrency Steem.

- **The DAO, May 2016 -** Blockchain based venture capital, The DAO – an Ethereum Project, hacked for $60 million.

While most of these occurred on the public blockchain, private blockchain can be vulnerable as well. Blockchain being the most growing technology, there is an increasing need to thinking securing the blockchain.

Blockchain Can Save Our Privacy Before It Disappears

Today, our personal privacy is under siege by veiled government surveillance programs and the countless tech company Trojan Horses. Privacy, per Merriam-Webster, is defined as the quality or state of being apart from company or observation, or freedom from unauthorized intrusion.

Technical innovations in the past twenty years have blurred the lines of "apart from company" and "unauthorized intrusion," and now our personal privacy is under attack from multiple fronts. Our locations are constantly being tracked on our phones, which are borderline inseparable from our bodies. We are under constant surveillance. Social media platforms know more about us than we should be comfortable with. Our sensitive information is floating around and being exchanged for a myriad of unauthorized purposes. Many personal privacy advocates have taken to blockchain and cryptocurrency entrepreneurship to build solutions that address the concerns of our dwindling right to privacy in the digital world.

Technological advancements like blockchain and zero-proof have given the pro-privacy debate a new gust of wind. The beauty of these solutions is that they offer encryption or at least partial obfuscation on a massive scale.

Privacy coins such as Monero and Zcash give us the freedom to transact without being tracked, but this could come at the prohibitively high cost of empowering and enabling criminal activity.

Blockchain-based browsing and social media platforms like BAT, Steemit, and Sapien offer an escape from a manipulative data-mining browsing and social experience.

References

https://blockgeeks.com
https://coincentral.com
https://www.aujas.com
https://www.codementor.io/

Cryptocurrency Mining

Cryptocurrency mining, or cryptomining, is a process in which transactions for various forms of cryptocurrency are verified and added to the blockchain digital ledger

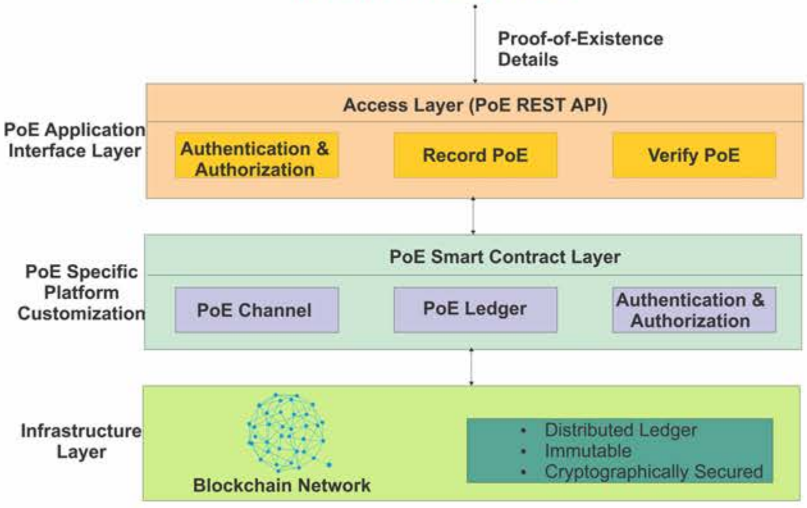
Blockchain based
Proof of Existence as a Service (PoEaaS)

PoE as a Service

What is Proof Of Existence (PoE)?

PoE calculates the cryptographic digest of digital artefact and stores in the Blockchain along with the timestamp. It allows verifying the existence of digital artefact's hash on the blockchain. This proves the existence of digital artefact at a point of time when it was recorded on blockchain.

Architecture



Proof-of-Existence Details

PoE Application Interface Layer
Access Layer (PoE REST API)
Authentication & Authorization
Record PoE
Verify PoE

PoE Specific Platform Customization
PoE Smart Contract Layer
PoE Channel
PoE Ledger
Authentication & Authorization

Infrastructure Layer
Blockchain Network
- Distributed Ledger
- Immutable
- Cryptographically Secured

C-DAC Blockchain based Proof Of Existence(PoE) Platform

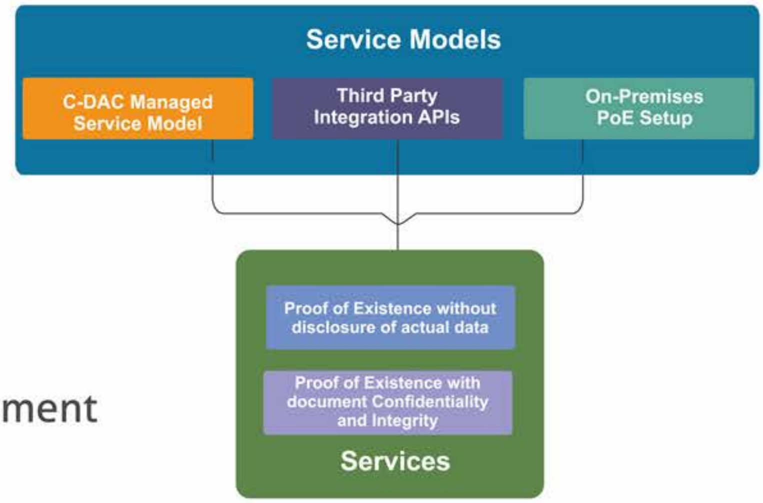
Benefits of PoE

1. Proves document Ownership without revealing actual data
2. Record time stamp & proves digital artefact exists at a certain moment of time
3. Certify the existence of document without the need of a Central Authority
4. Ensures document Integrity
5. Ensures that timestamp and hash of the documents cannot be tampered retroactively

Potential Use Cases of PoE

- Educational Applications
- MoUs / Agreements
- Driving Licenses
- Birth / Death Certificates,
- Sale Deed and Land Records
- Health Records
- Employee Service Records
- Log Management
- Enterprise Document Management
- And many more .....

PoE Service Models



Service Models
C-DAC Managed Service Model
Third Party Integration APIs
On-Premises PoE Setup

Proof of Existence without disclosure of actual data
Proof of Existence with document Confidentiality and Integrity
Services

For demo and queries mail us at cdacchain@cdac.in

सीडैक CDAC | प्रगत संगणन विकास केन्द्र
CENTRE FOR DEVELOPMENT OF ADVANCED COMPUTING
इलेक्ट्रॉनिकी और सूचना प्रौद्योगिकी मंत्रालय की वैज्ञानिक संस्था, भारत सरकार
A Scientific Society of the Ministry of Electronics and Information Technology, Government of India

Plot No. 6 & 7, Hardware Park, Sy No. 1/1, Srisailam Highway, Pahadi Shareef Via (Keshavagiri Post)
Hyderabad - 501510

MALWARE TIMELINE - 2019

Popular malware seen in 2019, I have uploaded APK files for all the entries that I could on my Github repository.

January

- **Zazdi Botnet -** Spyware that spreads via Facebook profiles and Youtube descriptions
- **Anubis dropper -** This dropper comes with motion detection capabilities
- **Masquerading malware -** This malware disguises as T V remote an other apps

February

- **Crypto Clipper -** Switches crypto wallet data
- **UFO Cryptominer -** Another cryptominer
- **Malbus -** Legit app started dropping malware after 5 years
- **Farseer**

March

- **Operation sheep -** Harvesting user data
- **SimBad -** Rogue Adware campaign
- **Apex Legends Spyware -** Spyware masquerades as Apex Legends
- **UC Browser Vulnerability -** Allows an attacks to spread malware sing this vulnerability
- **Adware in Gretel AZ -** Pre-installed malware in Gretel phones
- **Adware in beauty apps -** Adware ridden beauty apps
- **A comparative study of Mobile Anti -**Virus Solutions
- **Fake banking apps**
- **Brazilian Android RAT**
- **Fraud Financial Apps**
- **Persistent malware -** Just removes icon instead of the whole app
- **Comebot**
- **Gustuff -** CryptoTrojan
- **Exodus -** A two stage spyware
- **Another link**

April

- **Xloader -** New version of this threat
- **Gustuff targets Australia -** Another instance of Gustuff attack
- **Malware that sends WhatsApp messages**
- **Crypto banking Ransomware**
- **Sauron Locker**
- **StealJob -** State sponsored malware
- **Gretel pre-**installed malware
- **DrWeb Infection Ads**
- **Jio Offers -** Spreads via messages like a Worm
- **Adware TsSdk -** An aggressive adware component
- **Anubis strikes again -** With new downloaders
- Another Link
- **Preamo -** An adware clicker campaign

For more details
Full list - https://t.co/psh90rufGn
Download samples - https://t.co/2ukouM0Q0t

CERT-In Vulnerability Note CIVN-2019-0062

Denial of Service Vulnerability in Juniper Junos

Software Affected

- Juniper Networks SRX5000 Series:
- 12.1X46 versions prior to 12.1X46-D82;
- 12.3X48 versions prior to 12.3X48-D80;
- 15.1X49 versions prior to 15.1X49-D160.

Overview

An attacker can exploit this vulnerability to cause a denial-of-service condition, effectively denying service to legitimate users.

Description

A vulnerability exists in Juniper Junos OS due to receipt of a specific packet on the out-of-band management interface fxp0. A remote attacker could exploit this vulnerability by continuously sending a specially crafted packet to the fxp0 interface.

Successful exploit of this vulnerability could allow the attacker to cause the system to crash and restart (vmcore). By continuously sending a specially crafted packet to the fxp0 interface, an attacker can repetitively crash the system (vmcore) causing prolonged Denial of Service (DoS).

Solution

Apply appropriate updates as mentioned

https://kb.juniper.net/InfoCenter/index?page=content&id=JSA10936

References

JUNIPER
https://kb.juniper.net/InfoCenter/index?page=content&id=JSA10936

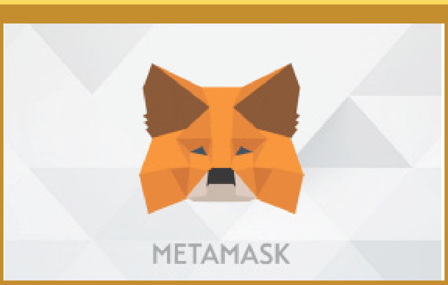
For more details visit:

https://www.cert-in.org.in/s2cMainServlet?pageid=PUBVLNOTES01&VLCODE=CIVN-2019-0062

InfoSec TOOLS

DEVELOPMENT TOOLS

METAMASK



Bring Ethereum to your browser - *https://metamask.io/*
Metamask is a browser extension that allows you to browse Ethereum blockchain enabled websites

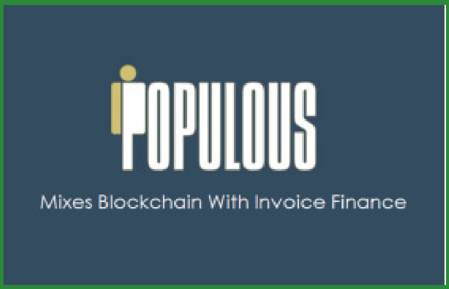
RemixIDE

http://remix.ethereum.org
Remix is a solidity IDE in which one you write code and check for errors right from your browser

Truffle Framework

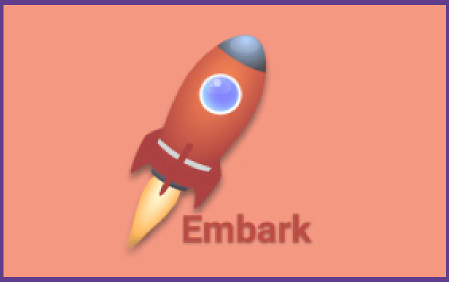
https://truffleframework.com/
The most popular Ethereum development framework - it's a development environment , testing framework and asset pipeline for Ethereum.

Populus



https://populus.readthedocs.io
Populus is a smart contract development framework for the Ethereum blockchain.

Embark



https://embark.status.im/
A framework which allows to easily develop and deploy DApps. It integrates with the EVM blockchains, IPFS, Whisper and Orbit.

Web3j

https://github.com/web3j/web3j
Web3j is a lightweight , reactive and typesafe java and Android library to use with smart contracts and integrate with clients on the Ethereum network

GanacheCLI

https://truffleframework.com/ganache
GanacheCLI (previously Testrpc), a NodeJS package, is a fast and customizable blockchain emulator. It simulates the Ethereum network on a single computer and allows you to make calls to the blockchain without any of the hassles of running a real Ethereum nod

SECURITY TOOLS

Vyper

https://vyper.readthedocs.io
Vyper is a contract-oriented, pythonic programming language that targets the Ethereum Virtual Machine (EVM). It aims for Security, Language and compiler simplicity and Auditability

Smartcheck

https://tool.smartdec.net/
Automatically checks Smart Contracts for vulnerabilities and bad practices – it highlights them in the code and gives a detailed explanation of the problem

Securify

https://securify.chainsecurity.com/
A security scanner for Ethereum smart contracts. Its an online service which takes your code, scans online and projects the analysis.

Mythx

https://consensys.net/
Mythx is an open source Ethereum smart contract and dApp (decentralized app) security analysis engine and platform that integrates with several commonly used IDEs.

सी डैक
CDAC

InfoSec CONTEST

InfoSec QUIZ

1. Bitcoin is based on ________ Blockchain?
   a.Private c.Public
   b.Public Permissioned d.Permissioned

2. What is not a benefit of Blockchain?
   a.Immutability c.Scalability
   b.Security d.Centralized control

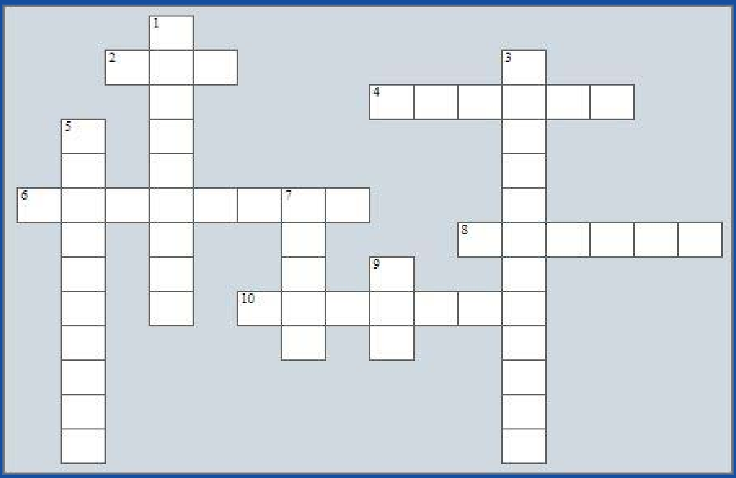
3. Blockchain is a ___________________?
   a.Distributed Ledger c.Exchange
   b.Centralized Ledger d.Digital Currency

4. Where is cryptocurrency stored?
   a.Digital Wallet c.Floppy Disk
   b.Bank Account d.File

5. What is a node in Blockchain?
   a.Type of Crypto Currency c. Exchange on the Blockchain
   b.Computer on a Blockchain network d.Platform

6. Which hashing algorithm is popularly used in Blockchain?
   a.MD5 c.RIPEMD
   b.SHA family d.MD2

Logon to
www.digitalsuraksha.in
www.infosecawareness.in
to participate in
InfoSec Contest and win prizes



InfoSec CROSSWORD

Across

2. 51% majority attack is very expensive to pull off, relatively only small and _________ hashpower
4. Name a Blockchain based social media platform
6. ________a blockchain start-up, aimed at raising capital for cryptocurrency social trading by selling their digital tokens in exchange for Ethereum.
8. Unauthorized access to Block chain is not possible through permissions and cryptography which shows the _______attribute of block chain
10. Who is the founder of bitmain the largest owner of Bitcoin hashpower

Down

1. Data gets recorded via _______________based algorithms
3. No one can tamper with block chain data as it is shared among millions of participant. This indicates ________ about the block chain technology
5. _________is a general agreement-based secure decentralized public database which stores information immutably over peer-to-peer network
7. Name the attack in which a huge number of nodes on a single network are owned by the same party and attempt to disrupt network activity through flooding the network.
9. The _________was a leaderless organization built on top of Ethereum using smart contracts.

INFORMATION SECURITY AWARENESS WORKSHOP

Master trainers training program@ JKBOSE Srinagar

Awareness Program for CISF officers@Airport Hyderabad

Awareness Program @ Rangath, Andaman and Nicobar Islands

Awareness Program for around 70 teachers@Delhi

RELEASE OF INFOSEC DEPOT -2019

The First annual Magazine of ISEA Phase II 'INFOSEC Depot -2019 was released during National Apex Committee meeting by Mr. Ajay Prakash Sawhney, Secretary, Ministry of Electronics & Information Technology (MeitY) on 22nd April 2019. The magazine is showcased as an outcome of collaborative efforts of Centre for Development of Advanced Computing (C-DAC) along with implementing agencies focused in the area of Information Security. This magazine provided a platform for researchers, academicians, and industry experts to share the knowledge, research outcomes and experiences. The magazine is featuring articles in emerging concepts and trends in information security, technological challenges, cyber threat perception and analysis, security practices, approaches in software development and implementation, solutions and trend analysis

To share tips / Latest News, mail us to

isea@cdac.in

About ISEA

Looking at the growing importance for the Information Security, Ministry of Electronics & Information Technology has identified this as a critical area. Information Security Education and Awareness (ISEA) Project was formulated and launched by the Govt. of India. One of the activities under this programme is to spread Information Security Awareness among children, teachers, home users, IT and non-IT professionals throughout the country. C-DAC Hyderabad has been assigned the responsibility of executing this project by Ministry of Electronics & Information Technology, Government of India. As part of this activity C-DAC, Hyderabad has been preparing Information Security Awareness material, coordinating with Participating Institutes (PI's) in organizing the various Information Security Awareness events etc.,

About C-DAC

C-DAC established its Hyderabad Centre in the year 1999 to work in Research, Development and Training activities embracing the latest Hardware & Software Technologies. The centre is a Knowledge Centre with the components of Knowledge Creation, Knowledge Dissemination and Knowledge Application to grow in the areas of Research & Development, Training and Business respectively. The R & D areas of the centre are e-Security, Embedded Systems, Ubiquitous Computing, e-Learning and ICT for Rural Development. The centre has developed over a period of time a number of products and solutions and has established a number of labs in cutting edge technologies. In line with these R&D strengths, the centre also offers Post Graduate level diploma courses. Centre is also actively involved in organizing faculty training programs. The centre regularly conducts skill based training and information security awareness programmes.

BOOK POST

For queries on Information security

Call us on Toll Free No.

1800 425 6235

between 10.00 AM to 6.00 PM
or give us a missed call
we will call you back within 24 hrs

ISEA Whatsapp Number for Incident Reporting

+91 9490771800

Between 9.00 AM to 5.30 PM

Subscribe us on

https://www.youtube.com/c/InformationSecurityEducationandAwareness

Follow us on

https://twitter.com/InfoSecAwa

Connect us with

https://www.facebook.com/infosecawareness

Ministry of Electronics and Information Technology (MeitY)
Government of India

सी डैक
CDAC
www.cdac.in

प्रगत संगणन विकास केन्द्र
CENTRE FOR DEVELOPMENT OF ADVANCED COMPUTING
इलेक्ट्रॉनिकी और सूचना प्रौद्योगिकी मंत्रालय की वैज्ञानिक संस्था, भारत सरकार
A Scientific Society of the Ministry of Electronics and Information Technology, Government of India

Plot No. 6 & 7, Hardware Park, Sy No. 1/1, Srisailam Highway,
Pahadi Shareef Via Keshavagiri (Post), Hyderabad - 501510, Telangana(India)

Nalanda Building, No. 1 Shivabagh Satyam Theatre Road,
Ameerpet, Hyderabad - 500016, Telangana (India)