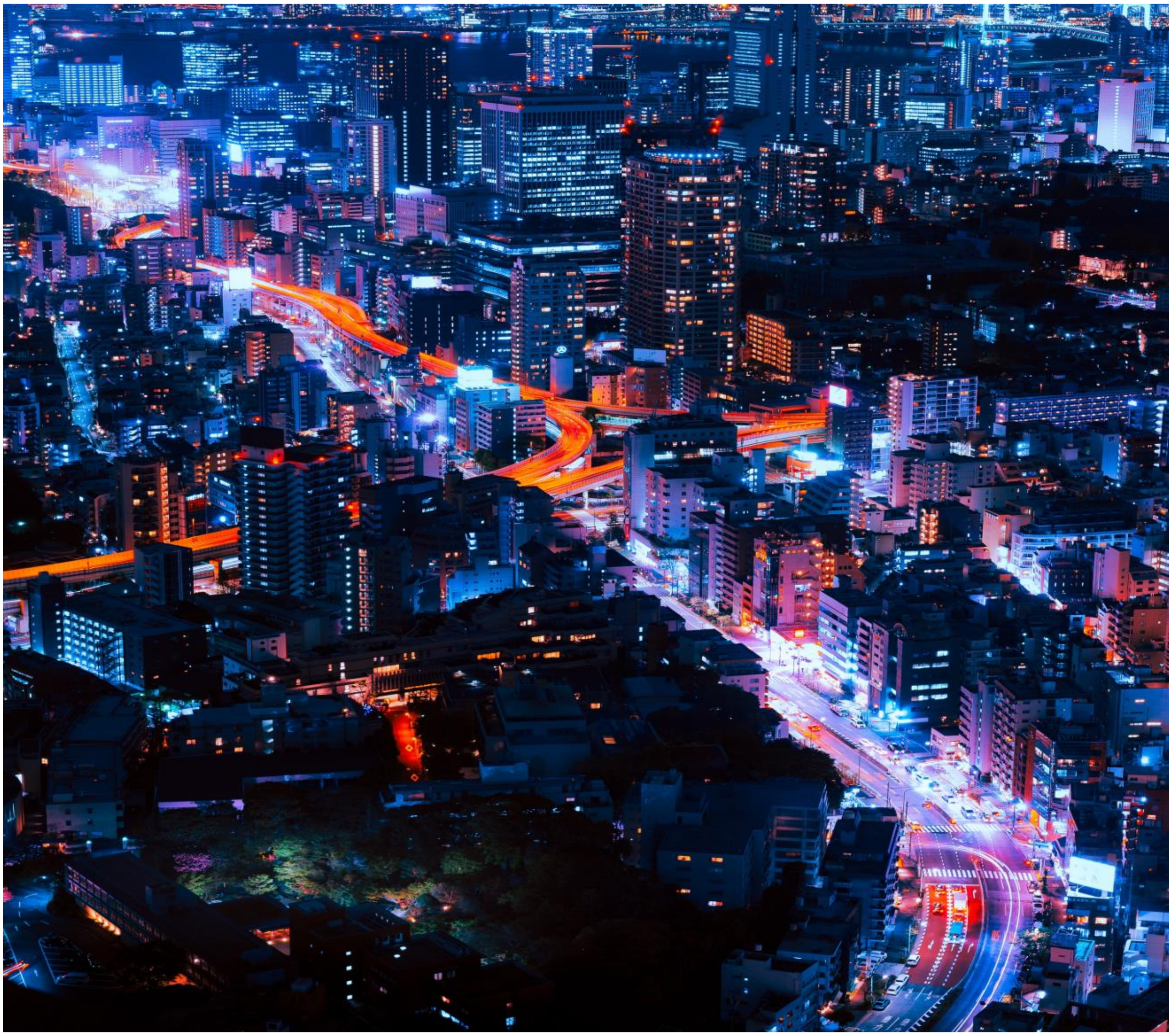
# Blockchain Audit/Assurance Services



# Blockchain Audit/Assurance Services

## INTRODUCTION

### About US

Ecom Infotech I Ltd is a Mumbai based company practicing in Cyber Security related services. We specialize in AICPA SSAE18 SOC Reporting, Cloud and Data Security, Security Analytics, SCADA, IoT and Blockchain Audits. Our team members come with 10-15 years of Cyber Security experience having worked with well-known names.

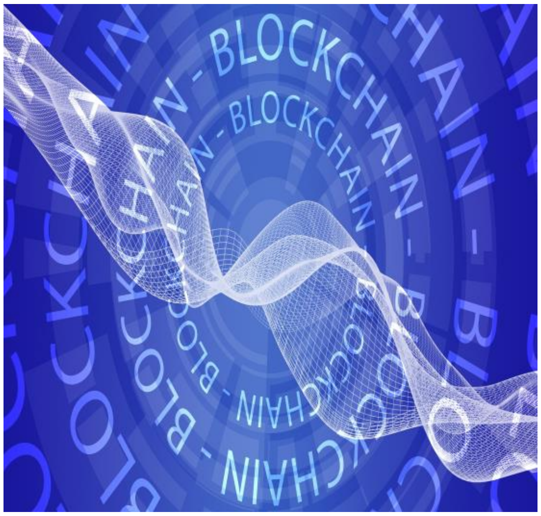
### About Blockchain

Based on the Public Key Encryption (PKE), Blockchain is a distributed database that maintains a continuously growing list of records called blocks that are secured from any kind of tampering and revision efforts. Each block contains a time stamp and a link to the previous block. A blockchain consists of blocks that hold batches of valid and approved transactions. Each block includes the hash of the prior block in the blockchain linking the two. The linked blocks form a chain, which is called a blockchain.

Blockchain is the foundational technology on which the popular bitcoin and other cryptocurrency platforms are built and is a technology that efficiently organizes and secures data so that it can reduce the cost and complexity of transactions to a great extent.

Smart contract implementations are based on blockchains. They are used more specifically in the sense of general purpose computation that takes place on a blockchain or distributed ledger. A popular framework used for smart contracts is Ethereum. Smart contracts are not necessarily related to the classical concept of a contract but can be any kind of computer program. With smart contracts, a program enforces the contract built into the code.

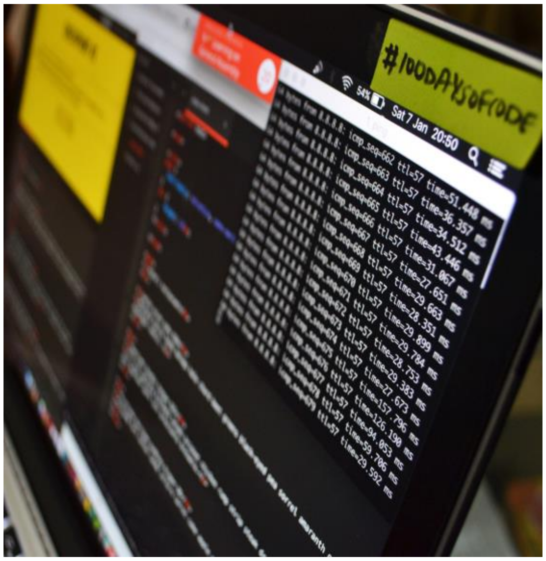
## CHALLENGES WITH BLOCKCHAIN



While blockchain technology is very efficient with respect to transactions, there are concerns about the security of blockchain-based transactions. These vulnerabilities cloud exist in the permissioned blockchain ecosystem. Some of discovered issues are:

**Blockchain implementations could be hacked like any other platform/ protocol.** If someone chooses to save their bitcoin and private keys on an Internet-connected device, they can be stolen. Once private keys are stolen, it does not matter how secure the blockchain architecture and encryption features are to hackers. Incidents like this have occurred in the past, for example the Ethereum attack in June 2016 in which US $150 million was lost.

**Blockchain nodes can be infected by malware**. This has been proven through a POC software that was demonstrated by Interpol at Black Hat Asia in March 2015. This POC software was morphed into malware that could circumvent the blockchain used by bitcoin and introduced data unrelated to transactions into the blockchain. Researchers have also demonstrated that botnets have the ability to send messages utilizing the bitcoin network. **Fujacks Trojan,** a botnet backdoor, has successfully proven that it can remotely control infected computers that are nodes in a blockchain, collect information, and install other malware or tools into the blockchain.

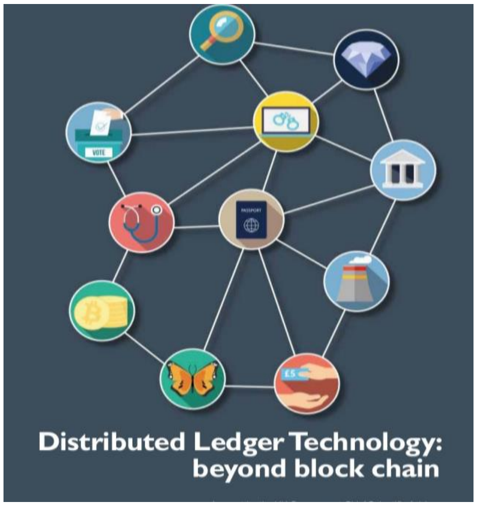


**Securing Keys**. Banks and other organizations have concerns about transactions' confidentiality, securing private keys and the strength of cryptographic algorithms used in blockchain-based transactions.

**Regulation.** Any blockchain transaction is dependent on trust between two or more counterparties. Many people use cryptocurrencies at exchanges and trust the exchange will look after them. Many money exchange firms may not fully regulated entities. They may not offer assurance on the transfer of digital currencies.

**Smart Contracts**

A blockchain-based smart contract is visible to all users of said blockchain. However, this leads to a situation where bugs, including security holes, are visible to all yet may not be quickly fixed. Such an attack, difficult to fix quickly, was successfully executed on The DAO in June 2016, draining US$50 million in Ether while developers attempted to come to a solution that would gain consensus. The DAO program had a time delay in place before the hacker could remove the funds; a hard fork of the Ethereum software was done to claw back the funds from the attacker before the time limit expired. Issues in Ethereum smart contracts, in particular, include ambiguities and easy-but-insecure constructs in its contract language Solidity, compiler bugs, Ethereum Virtual Machine bugs, attacks on the blockchain network, the immutability of bugs and that there is no central source documenting known vulnerabilities, attacks and problematic constructs.



# NEED FOR BLOCKCHAIN AUDITS (DEMAND)

**Increasing Attacks against Blockchain**

As blockchain technology continues to both positively and negatively disrupt global industries, we must be diligent about the security implications. As we’ve seen, cybercriminals will find creative ways to reach their goals. Although the blockchain has been well researched and answers many questions regarding decentralized trust, it does not address the security of users or the applications that connect to its network. Insecure wallets lead to theft of cryptocurrencies. Attackers have used old techniques in new ways with success, such as the dictionary attacks against Bitcoin private keys. Even traditional phishing attacks can work to gain access to wallets or computer resources. To provide assurance for Blockchain implementations **we need a Cyber Security Audit.**

### Due Diligence

Government regulators are struggling to keep up with and understand the legal implications of losses due to cyberattacks. Businesses must also be diligent. Blockchain technology is attracting a lot of interest for solving various business needs beyond decentralized payments. Entire automated businesses are being built using smart contracts. Retailers and others are looking into blockchain to manage their inventories. The medical industry is examining ways to manage medical documents. The number of successful and impactful attacks against exchanges extends well beyond the confines of this report and should serve as a warning. It is not enough to implement and use new technologies without performing a **tailored risk assessment.**

**Governance**

As industries research and implement their own blockchains, we can expect cybercriminals to deploy a combination of known and yet unknown techniques to compromise them. Without a clear understanding of where the risks are you may place undue trust in your blockchain implementations. As we've seen, mistakes are easy to make. Users are even harder to control and can negatively contribute to the risk. We need to learn from recent events to make better decisions for securing our technologies for tomorrow. It is therefore important for us to have an appropriate **Governance model for implementing and monitoring the blockchain deployment.**

> **“Lack of structured blockchain governance is an important challenge in maintaining data in a blockchain.”**

## BlOCKCHAIN AUDIT ENGAGEMENTS

**Some of the use cases for Blockchain Audits could be:**

- Smart Contract Code Reviews
- Permissioned blockchain Implementation Audits
- Evaluate Controls implemented as intended using blockchain
- Operating effectiveness of the blockchain implemented controls
- Vendor organizations may require a Third-Party Audit for Vendor Due Diligence
- Provide an Auditors independent opinion about controls at the organization to Management, Stakeholders and other concerned parties

## Typical SCOPE OF WORK (SOW)

We conduct our assurance engagement against established standards used by our auditors to assess the internal controls of a blockchain deployment. The control objectives and criteria vary based on the scope of the engagement and client operations. The relationship between the organization deploying the blockchain and the purpose it serves must be viewed to help determine the controls that should be included in the engagement. Hence our engagements are usually risk based. In addition, the impact of the blockchain technology adapted in financial areas for the organizations financial statements will also be the determining factor as to whether required controls whether covered in the scope of the engagement. The following are some areas of control activities that may be generally included in the SOW:

- Logic of the PKE deployment
- Security of the Keys
- Vulnerability Assessments/ Penetration Testing
- Physical and environmental security
- Network security (firewalls, intrusion prevention)
- Change management
- Data retention and storage
- Disaster recovery / business continuity
- System documentation

**Specific services for Auditing/Consulting on Blockchain**

**Ciustomized Blockchain Governance Framework**

**Customized Blockchain Risk Management Frameowork**

**Continuous compliance provides low risk**

**Integerate with other assurance programs or audits**

**Comprehensive Assurance that address Privacy**

**Provides a high reliability  Seal of a licensed CPA FIRM**

## OUR OTHER CYBERSECURITY ASSURANCE SERVICES

- AICPA SSAE18 SOC Reports
- Cloud and Data Security
- Privacy compliance such as GDPR
- Security Analytics and SOC as a Service
- SCADA and Industrial Cyber Security
- Smart Infrastructure Security

# OUR PROJECT EXECUTION METHODOLOGY

### Key steps in Blockchain Audit/Assessment Engagement

| Plan | Deliver | Access | Report |
|---|---|---|---|
| Understanding the client entity and environment | Understanding and verifying documentation of existing internal controls | Evaluate Samples | Evaluate additional info |
| Define scope, expectations and project roles | Perform Walkthrough | Analyse Samples for effectiveness | Request clarifications |
| Readiness Assessment if required | Assess Risks | Request additional info | Report is drafted through inputs from the audit team and the client management |
| Kick off meeting with Stakeholders | Identifying the control objectives and controls in place | | Issue draft report |
| Preliminary interviews / questionnaires conducted to gain understanding of requirements | Conduct Interviews | | Incorporate Management comments and Issue final report |
| Client information request list prepared and distributed | Request Samples | | Ongoing support |
| Analysis of client-prepared information performed and client feedback provided | Validation of the implementation of controls | | Answer questions to Management and User Auditors |
| Project timeline (including estimates of client hours) / plan created | Test results communicated and exceptions are resolved, if possible | | |
| Update Plan based on client discussions | | | |

# VALUE DELIVERY

Knowing how much extra value and assurance an audit report can deliver, many clients find that it makes sense to take steps to ensure a more successful outcome, including hiring experts who are skilled in helping organizations be more thorough and thoughtful in how they approach their engagement. Preparing for a Blockchain based engagement is a matter of clear thinking and smart planning. Working with cyber security specialized consulting specialists such as ours, helps you dig into areas such as cloud security, data security and privacy, incident response and much more.

We provide end to end process for Blockchain Audit Engagements. With the rapid Cloud adaption and increased use of IoT, Big Data and Analytics, Cloud Security and Privacy concerns are on the rise. We can conduct integrated engagements with existing best practices to evaluate your environment and to reduce the duplicate efforts and save costs for you.

**Some of the advantages of working with us are:**

A
- End to end process for Blockchain Audit/Assessment Services
- Project management methodology consistently applied to each engagement

B
- Efficient service delivery with minimal disruption to operations
- Our engagements are executed by senior experienced professionals

C
- 15 years of Information Security & Cyber Security experience
- Reduced time to complete assignments

D
- Licensed CPA Firm & Security Professionals to execute projects & provide attest reports
- Prompt services with engagements completed in record time

E
- Ongoing support. We are with you whenever you need us
- Our services are competitively priced than BIG names to provide higher ROI

**To discuss your specific need please email info@ecominfotech.biz**

**Disclaimer**: The content contained in this document is only for information and should not be construed as an advice or an opinion. The rules are subject to change and for the latest information please visit the official websites. In no way we are responsible for the information contained in this document as a result of its/her/his use or reliance on the information. A formal Scope of Work shall be signed which should be referred to for any specific services offered.