Using Blockchain Cryptography Technology for Fraud Prevention

Skills and expertise to help you increase your knowledge in the field of digital technologies

TLC Education & Training Services

About this workshop

Fraud in any organization or company is not a problem that should be ignored. In addition to being costly, it can decrease employee morale and create an unstable business environment as well as undermine business and consumer relationships.

According to a study by the Association of Certified Fraud Examiners, the typical organization loses five percent of revenues to fraud each year. Unfortunately, fraud in a business can go undetected for a long time and is often hard to uncover.

Blockchain can be used to fight and prevent fraud in a business network. One of the major components that determines the value of Blockchain is its ability to share data in a fast and very secured way without any one entity having to take responsibility for safeguarding the data. In this one day workshop we will see how an enhanced security is a leading benefit of Blockchain technology.

A study made by F5 shows that an average of **232.2 million** malicious login attempts made per day with a **0.05** success rate that translated to **116,106 successful account takeover attacks every day**, with an average of **$400 stolen** from each account.

In 2020, PwC has published a report on worldwide blockchain adoption, which finds that 84% of organizations are experimenting with the technology.

By the end of this course, you'll be able to:

- Describe the underlying economics of innovations based on Blockchain as an disrupting technology.
- Blockchain industry Use Cases and how Blockchain addresses data security.
- The role of cryptography to secure transactions using different algorithms.

Prerequisites:

Participants attending this course should be familiar with basic Information Technology (IT) concepts, business challenges and the role of general system wide infrastructure technologies and their applications. The course assumes that learners have zero knowledge of Blockchain technology.

What's the Future of Blockchain in the Business World and related challenges?

- As per a PwC report, **77%** of the financial institutions are anticipated to embrace blockchain technology as a core part of their in-production system or process by the end of 2020.
- Gartner forecasts that blockchain technology will generate an annual business value of around **USD 3 Trillion** by **2030**.
- Financial crime is becoming a greater threat for banks, business institutions, and individuals to handle and control.
- Regulators and financial authorities are challenged to introduce new strategies to **detect** and **prevent** financial crime using Digital Technologies and draw a distinction between **fraud** and **financial crime**.
- Review why applications following generalized security framework, traditional approach to security and enterprise security are struggling hard to protect data and why Blockchain is the only solution stands out as a most secure platform today.

Unit 1 – Blockchain for Fraud Prevention

- Understanding Distributed Systems – System of Records (SOR), System of Engagement (SOE), and System of Interactions (SOI).
- Risk Defined – Three Categories of Risks.
- Understand Financial crime or fraud.
- Financial Compliance Vs Financial Crime and Fraud.
- Types of Frauds in Banking and Financial Services Industry.
- The difference between automated and human-driven fraud.
- Fraud and financial crime – A small Industry backdrop.
- Challenges to combat Financial Crime in Financial Domain.
- Cyber profile of Fraud and Financial Crime – An illustrated Example.
- Understand why crime pathways are converging, blurring traditional distinctions among cyber breaches, fraud, and financial crimes.
- The Process of Fraud Detection System.
- Types of inherent risks attached with Blockchain.
- How Blockchain Technology can Prevent Fraud?
- Understand how enhanced security is a leading benefit of blockchain technology.
- Can Blockchain eliminate all Frauds?
- Blockchain for Traceability and Key Traceability Concepts.
- How AI and Machine Learning can turn the tide of fraud.
- The Process of Fraud Detection System.
- How Blockchain Prevent Identity Theft?
- Benefits of Blockchain – The business value summary.
- Top 11 ways poor Cybersecurity can harm your security hygiene.
- 10 Key steps to Cybersecurity.
- Questions you should ask your Cloud Services Provider.
- What you need to remember – Cybersecurity.
- Unit 2 Assessment.

With the advancement of online payments in various products and services, the likelihood of credit card fraud has risen compared to the decades-long history of credit cards. When blockchain systems' immutability meets smart contracts, third-party removal and decentralization could be met as a high level of security.

Confidence and trust in fraud prevention and security technologies is a must. Merchants are expected to have fraud-proof solutions in place. Customers are expected to protect their personal data. Issuers and acquirers are trusted with verification and authorization management.

Which Fraud Types Can Blockchain Detect?

Financial Fraud

Financial transactions are generally complex transactions. Some aspects such as the collateral requirement between the parties, the time required for reconciliation or settlement, currency differences cause the complexity. Some of these processes may require multiple human interactions at certain steps. Thus, the risk of fraud in financial transactions is high. Thanks to blockchain technology, it becomes much easier to detect suspicious behaviors. Because using blockchain, you share the recorded data in real-time and update the data with the approval of all parties who have access to the data.

Using Blockchain Cryptography Technology for Fraud Prevention

Skills and expertise to help you increase your knowledge in the field of digital technologies

TLC
Education & Training Services

Target Audience for this course

- CIO, CDO, CISO, CTO, or any other CXO, Director IT, GM IT, Senior Managers, Business Technology Leaders, Digital and Technology Team Leaders, Data Analytics and Data Science personals, Data Warehouse Engineers, Application Software Development Teams and Programmers, Enterprise Architects, Project Managers, Business Analysts, Information and Cybersecurity team, SOC Analysts, Risk Professionals and Technical Writers.
- Senior Technology Professionals and Business Technology Leaders who want to upskill their present set of skills in the space of Blockchain Technology.

Financial compliance is now a international concern. The global cost of compliance in the financial sector alone is estimated to be around **$180.9 billion** per year.

Research estimates online fraud losses will exceed **$48 billion** per year by 2023.

45% of banks say their investigations take too long to complete, and **40%** say the investigations result in a high number of false positives, which occur when legitimate transactions that have been mistakenly flagged as fraudulent.

Are you eager to grow your blockchain specialization? Are you willing to acquire blockchain skills and knowledge? If yes, then this is the right time to take this course.

Equally ideal for individuals looking forward to pursuing a professional career in this field.

Identity Fraud

Identity theft is one of the most common fraud methods in e-commerce. Especially in recent years, the prevalence of identity fraud has been increasing rapidly. In the blockchain structure, which works with strong authentication systems, only the people with permission can access the real data as the unique, original version. Also, only a certain party can handle the verification of the transactions to be made. Personal data is safe, and the risk of identity fraud is very low thanks to the secure infrastructure of blockchain.

Supply Change Frauds

Supply chain fraud is a big problem for companies. Due to the network created with the supplier companies, too many people involve in the process and the rate of access to data increases from time to time. Blockchain provides businesses with transparent and easy tracking of products. To update the products, a participant needs verification from all authorized participants. This means that participants are not able to manipulate the products easily.

Unit 2 – The Role of Cryptographic Algorithms in Blockchain

- Understanding the importance of Security.
- Confidentiality, Integrity & Availability – Defined.
- Threat Channel Vector Attack and Attack Progression Model used by Cybercriminals.
- Cryptography Defined.
- Explaining Symmetric and Asymmetric Key Cryptography.
- A High-level Comparison between Public and Private Key.
- Symmetric Vs Asymmetric Encryption Illustration.
- End–to–End Encryption Explained .
- Algorithms used in Blockchain Technology.
- Define SHA-256, ECC and RIPEMD-160 Cryptography Algorithm.
- Hashing and Blockchain relationships.
- Hashing – An Example of online SHA-256 Hash Calculator.
- Properties of Cryptography Hash.
- Establishment of Trust through consensus and cryptography.
- Importance of Digital Signatures and Nonrepudiation.
- Cryptography and Encryption Checkpoint and key differences.
- Understanding Digital Wallets and Types of Digital Wallets.
- Maintaining a Wallet Security.
- Blockchain Security Reference Architecture and Security Model.
- Blockchain literacy gaps – The Challenge.
- A Blockchain network is only as secure as its infrastructure.
- Unit 2 Assessment.

When done right, Blockchain can eliminate these vulnerabilities:

Real-time monitoring: Timestamps fix a traceable timeline, featuring the how, who, when, and where of accountability.

Real identities: Each block (account, credit card, transaction) is linked to a real person or company. Identities cannot be hidden or buried in paperwork.

Eliminate third-party approval: Blockchain relies on 51% approval of those involved in the transaction. Third-party approval is not required or permitted. Only those in the chain can access and approve.

Paper is replaced with digital data: Proof of purchase, approval records, receipt of items, and other payment data is stored in the blockchain. The merchant, issuer, acquirer, and customer all have access to the same secure data—saving time and money in the event of a chargeback representment

This course will be delivered by **Certified Blockchain Expert – Blockchain Council**.

Detail Information

Course Code : TN315
Course Duration : 1 Day Workshop
Course Location : TLC, Online and Customer On-site.
Terms & Conditions :100% payment in advance.
Course Deliverable: Comprehensive Student Guide and Course Certificate

For additional information, please write to us at: info@tlcpak.com

Opportunities are made, not found