CYBERSECURITY CENTRE *of* EXCELLENCE
A joint initiative of DSCI & Government of Telangana

DSCI
PROMOTING DATA PROTECTION
A NASSCOM® Initiative

SecureDApp

WHITEPAPER

SMART CONTRACT SECURITY

ENHANCING TRUST IN DECENTRALIZED PLATFORMS

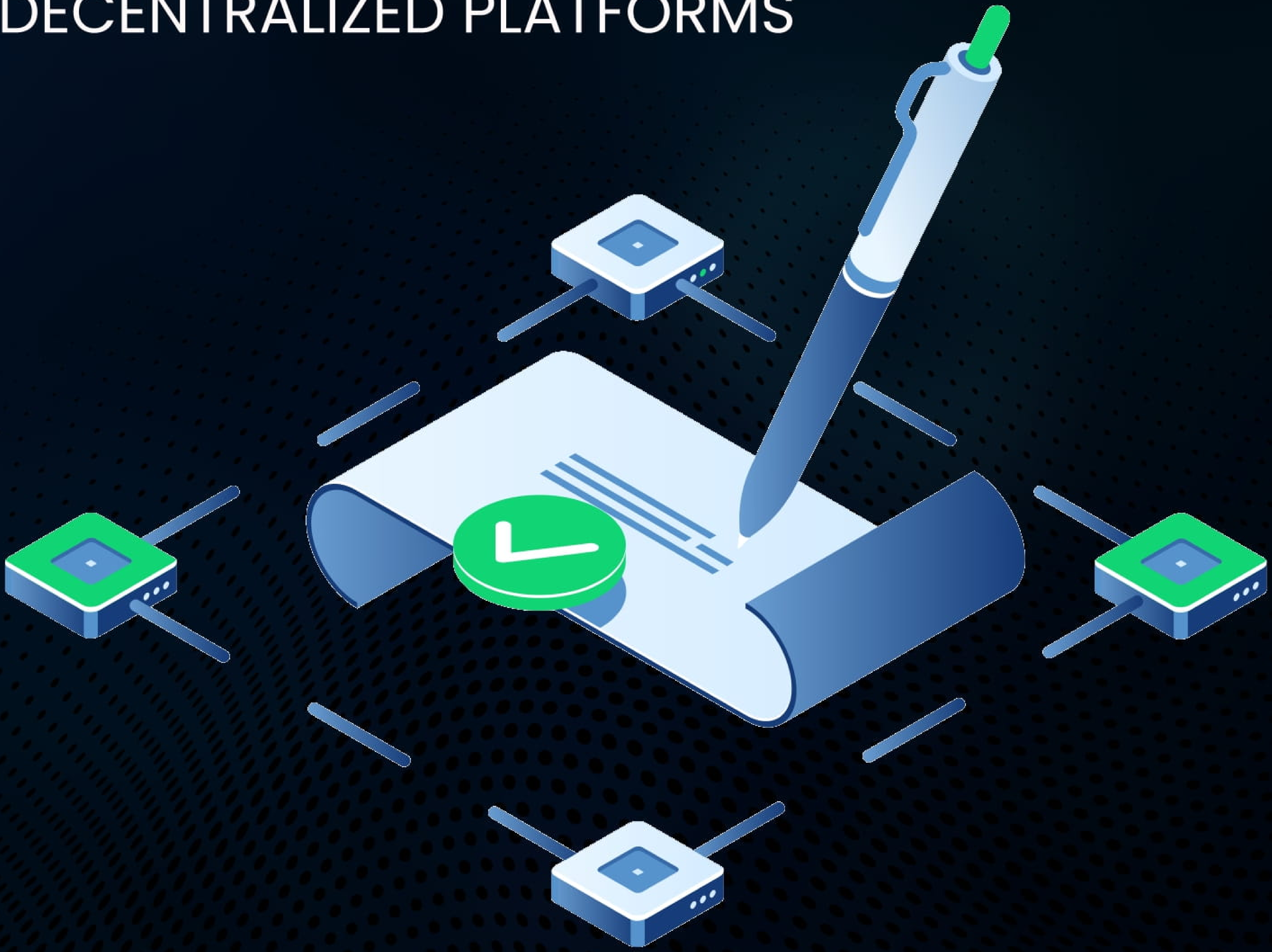


Table of Contents

Executive Summary:

Blockchain technology is presently reshaping the economy and the social mechanics of the internet. In its essence, blockchain is an electronic register, a distributed database in which information is stored in computers and not owned by anyone. This decentralised nature of block chain means that once information or a piece of data has been placed in the block it cannot be altered or erased. This characteristic makes blockchain reliable and shareable in that the content of the storage once created cannot be altered. Compared to conventional systems for collecting and dealing with large volumes of data, blockchain relies on consensus over all nodes, which removes the need for extra steps and power from middlemen, thus boosting effectiveness.

In fact, the security provided by blockchain is another area in which it has become increasingly relevant. While in a centralised system an attack on a database can wipe out all the data and valuables, in a blockchain changing data is near to impossible for wrong doers as they would have to change it on all the nodes of the network. Blockchain adds another layer of security to this by virtue of the ledger transparency that it offers. The participants in the blockchain have the same copy of data; that is, transactions are clear and conspicuous; this is suitable for the financial and healthcare sectors.

Blockchain is a relatively new technology; Bitcoin is the first digital currency created based on a decentralised ledger called Blockchain from which other uses have developed. In recent years, blockchain is being utilised in various sectors apart from the finance domain. Today it is a cornerstone of Web3, a new decentralised web. Web1 allowed users to read content in a passive manner but Web2 brought interactivity with Web2 property managers like Google, and Facebook among others holding a lot of data. Web3 aims to reset users' power by offering decentralised applications (dApps) that operate through greater, distributing nodes rather than central hosts. This shift has been most profound in the money market where through decentralised finance (DeFi), people can buy, sell, lend, and borrow without going through an intermediary financial house. Web3 and blockchain are also used in the sectors including healthcare, supply chain, and government services because decentralisation helps to combat fraudsters.

One major feature on blockchain is the smart contract. Smart contract is a digitalized contract which executes the terms of the agreements in the blockchain technology. Unlike most agreements that may require the intervention of third parties such as banks or lawyers, once the substantive terms of a contract are fulfilled then the contract fulfils the agreement. For example, in real estate sales, upon payment being made, the smart contract implementation may insert the title deed into the buyer’s name. Such contracts bring efficiency, as the time and money needed for conventional approaches are minimised, In addition, due to their placement on the blockchain, the contracts cannot be altered and are, therefore, highly transparent. But they come with certain risks. As the code corresponds to the smart contract, any mistake or weakness in the code can be manipulated, and therefore security checks are important to embrace the smart contracts.

Blockchain technology solutions are on the rise in various industries and sectors across the world. In finance, it helps to make cross-border payments even cheaper and faster; in healthcare, for instance, it is already in use for securely storing patient information – it will protect the patient data from being breached and violating the data protection laws. Blockchain also adds value in supply chain management by allowing organisations to trace products from their source to the consumer to try to eliminate forgery. Blockchain is being considered by governments to replace traditional voting systems to deliver transparent, and more importantly, immutable election outcomes. In real estate, blockchain is a process of using electronic ledgers to manage property ownership records, and the buying and selling processes eliminate third-party agents or paperwork.

Blockchain’s capability is not just limited to what it is being used for today. Looking at the future evolution of Web3, blockchain should stay central for the management of individual data, for the decentralisation of the control of the user’s experiences, and innovative business models. More processes are to be automated through smart contracts, and more applications are to decentralise our interactions with the internet and with each other. Blockchain has all the attributes that can bring revolution in industries throughout the world in the future including security, transparency and decentralised systems.We also look at future trends such as AI and quantum computing as well as give examples of organisations who have been able to effectively mitigate these risks. Last but not least, we explain how SecuredApp stands out from the competition in addressing smart contracts’ security challenges and how our solutions can help organisations adapt to this new reality.

Introduction:

Smart contracts are dependent on a complex technological environment that supports the essence of their operation and protection. In their essence, smart contracts are pieces of code written to execute on the basis of a certain blockchain like Ethereum. This infrastructure has several components that have made smart contracts both effective and weak in equal measure.

The first one is the launch of a blockchain platform and the corresponding application. Blockchain is the distributed ledger that stores all transactions and all contract implementations. Because no individual or organisation has direct access to the blockchain, the latter is highly protected and transparent. Due to the combination of decentralised peers, each transaction is discussed and checked by multiple participants (nodes), so once the contract is set, it remains unchangeable.

The next is the code of a smart contract which is written in programming languages, such as Solidity which is used in Ethereum. This is a donor work description which contains provisions of the contract that has been made as well as the circumstances under which it will be implemented. For instance, upon confirmation of delivery, some contract may trigger an automatic payment. Unlike conventional applications, once the code is written and launched on the blockchain, it cannot be altered, which preserves an agreed-upon representation. But this immutability also makes it possible for bugs or vulnerabilities in the code to be with the system forever so care must be taken when writing the code.

Another important factor is Oracles – these provide off-chain data (data and information that is outside the blockchain system). Oracles have this role because smart contracts sometimes require data from the real world such as stock prices or weather conditions to execute a contract. Nevertheless, that brings certain risks, as the data provided by oracles can be manipulated, and this can create intentions for non-desirable or even fraudulent contract executions.

It is only by having a glance of the technical underlying of smart contracts will one be in a position to have a broad understanding of the strengths that can be accorded to smart contracts as well as the weaknesses that may come along with smart contracts but needs to be sealed off for the success of the whole process.

Why is Security Critical?

Smart contracts are innovations in digital transactions, which, however, pose great threats to security. Smart contract code, once launched on the blockchain, remains fixed and may have numerous exposed weaknesses that enemies can take advantage of endlessly and cause great financial and image damage.

Presently, the use of blockchain is gradually increasing in India for various government projects, and, therefore, security must be a priority. For Instance, the Government of Maharashtra employs the use of blockchain in an effort to safely protect land registry, which helps in conducting safe property deeds. In the same manner, in the Government of Telangana the use of blockchain has been applied to land registries as a way of minimising fraudulent activities and ownership issues.

At the national level, National Payments Corporation of India (NPCI) introduced Vajra Blockchain Platform which aims to enable secured interbank transactions simultaneously, Ministry of Electronics and Information Technology (MeitY) is driving National Blockchain Strategy envisaged to cover various sectors including healthcare, education and supply chains.

For such crucial government operations and citizen information, it becomes important to protect smart contracts to preserve the national interests and continue trust on the blockchain technologies.

Current Security Landscape

According to Gartner, nearly 20% of all enterprise blockchain applications will face major security breaches by 2025 due to inadequate security measures. Recent data from Chainalysis shows that $3.8 billion was lost in cryptocurrency hacks in 2022, with a substantial portion attributed to smart contract vulnerabilities.

Purpose of This Whitepaper

This whitepaper is intended to give an overview of the security issues of smart contracts and to give recommendations to minimise these threats. In this paper, we will discuss the trends observed in recent years, typical weaknesses, and recommendations for smart contracts' protection, as well as a thorough analysis of the solutions implemented in SecuredApp.

Current Landscape of Smart Contract Security

Recent trends and developments

- Growing Adoption of Smart Contracts: Despite blockchain's potential still remains unclear, smart contracts are already rapidly being implemented. For instance, in what decentralized finance applications? They facilitate the execution of specific financial operations without the participation of middlemen by means of a script. However, there is the dark side to this fast uptake in that such systems are vulnerable to attack since flaws found in the code are leveraged once the systems are live. Criminals can take advantage of vulnerabilities in the code of smart contracts and lead to the theft of funds of exchange disruptions.

- Emergence of New Attack Vectors: With the increase of use of smart contracts, the attack methods also increase. For example, flash loan attacks that leverage the DeFi system's features of its immediate lending include manipulating the token prices in under milliseconds, leading to certain losses. Another frequently encountered kind of attack is reentrancy where hackers take advantage of calls made within a contract to siphon money from a contract before the original function call is over.

- Increased Regulatory Focus: Global governments have begun targeting blockchains as the technologies continue to gain more popularity to meet legal requirements both in finance and data protection. However, poorly developed designs allow for some exploitations including oracle manipulation, or governance attacks in which hackers control some blockchain systems. For instance, the implementation of blockchain technology for the public schemes in India, especially the records of land, it becomes imperative for the government of the country to ensure that they come up with the strict security features on the intervention of tampering or accessing the records by unauthorized persons.

Latest Data and Statistics

Source	Statistic
Gartner	By 2025, 20% of blockchain applications will face security breaches.
Chainalysis	$3.8 billion lost in cryptocurrency hacks in 2022.
IBM Security	The average cost of a breach in the financial sector is $5.85 million.
Bridgecrew	50% of DeFi smart contracts contain at least one critical vulnerability.
Elliptic	Reentrancy attacks account for 35% of DeFi platform losses.

Major Issues in Blockchain Environment

- **Lack of Standardization:** Currently, there are no standard guidelines that are followed when developing smart contracts, thus the security of the smart contracts is not uniform.

- **Complexity of Smart Contract Code:** Smart contracts are becoming more complex, and that is why their auditability and security become more challenging.

- **Open-Source Nature:** Although transparency is one of the characteristics of blockchain, it also enables the attackers to analyse the code of the smart contract and find vulnerabilities.

Classification of Common Vulnerabilities

A

Code Bugs and Inadequacies : Surely it is understood that even slightly different incorrect code in smart contracts can lead to ASTONISHING financial loss. For instance, in 2016, the DAO counterpart was hacked through a code weakness, enabling the attackers to siphon about 3.6m Ether or approximately $70m. Specific pattern they have identified as problematic are unfixed return values, integer overflow/underflow, and improper or absent exception handling, all of which endanger the integrities of smart contracts.

B

Reentrancy Attacks : This kind of an attack involves a feature where a contract can be called several times before the initial execution gets complete. The former helps those attackers who withdraw more than they initially planned. One example is the dForce protocol that was exploited in 2020 with reentrancy issues which caused the platform to lose $25 million. It also showed the impact of insecure coding resulting into repeated contract calls as the attack was executed.

C

Oracle Manipulation : They free-ride or dispense real-world information to the smart contracts (e.g., prices). If an oracle becomes corrupt it is sad to note that any attacker can twist the data and thus perform other undesired contract executions. The bZx protocol has fallen victim to an oracle manipulation attack twice in 2020, with the hackers making away with $900,000. It shows the importance of safety and decentralised oracles to avoid the sharing of fake data that can misguide the user community.

D

Inadequate Security Audits : Such smart contracts leave the possibility of various attacks unaddressed even if they provide all the benefits of automating business processes. Sometimes audits are not conducted because of a lack of funds or simply a lack of knowledge about the importance of such actions; thus, projects can be exploited. Lack of proper audits can obscure a number of critical issues and make serious vulnerabilities exposed to hacking attacks common in many contracts.

Some of the typical issues that can be found in smart contracts include

Common Vulnerabilities in Smart Contracts and case explain how it was exploited

1 Code Bugs and Inadequacies

Vulnerability: Some of the minor codings include unchecked return values, inadequate integers, overflow/ underflow and wrong exceptions that result in extreme effects. These problems are ubiquitous because of the smart contracts and the blockchain properties of being immutable.

Case Study: The DAO Hack occurred in 2016 – Through a simple code exploit of the DAO's smart contract, ETH $70 million was drained.

Impact: This attack incurred humongous losses of money and paved the way for a contentious hard fork as a measure to regain the lost fund.

2 Reentrancy Attacks

Vulnerability: It happens when a function of a smart contract is invoked several times before the first call has even started, enabling attackers to steal the money or change the contract's status.

Case Study: dForce Protocol Attack (2020) — Hackers took advantage of the reentrancy bug, and looted $25 million from the dForce protocol within a few minutes.

Impact: It dealt a severe blow to its reputation by bringing into focus two vital functions that need to be central to smart contract building – function and state.

3 Oracle Manipulation

Vulnerability: Oracles are intermediaries between smart contracts and the real world to supply data but, when manipulated, can give out wrong information to cause smart contracts to behave unusually.

Case Study: bZx Protocol (2020) — the protocol was hacked twice by means of oracle manipulation aimed at the manipulation of the price feeds and the subsequent theft of $900,000.

Impact: Such situations highlighted the problems with the use of centralized oracles and increased the demand for fresh decentralized ones to avoid them.

4 Inadequate Security Audits

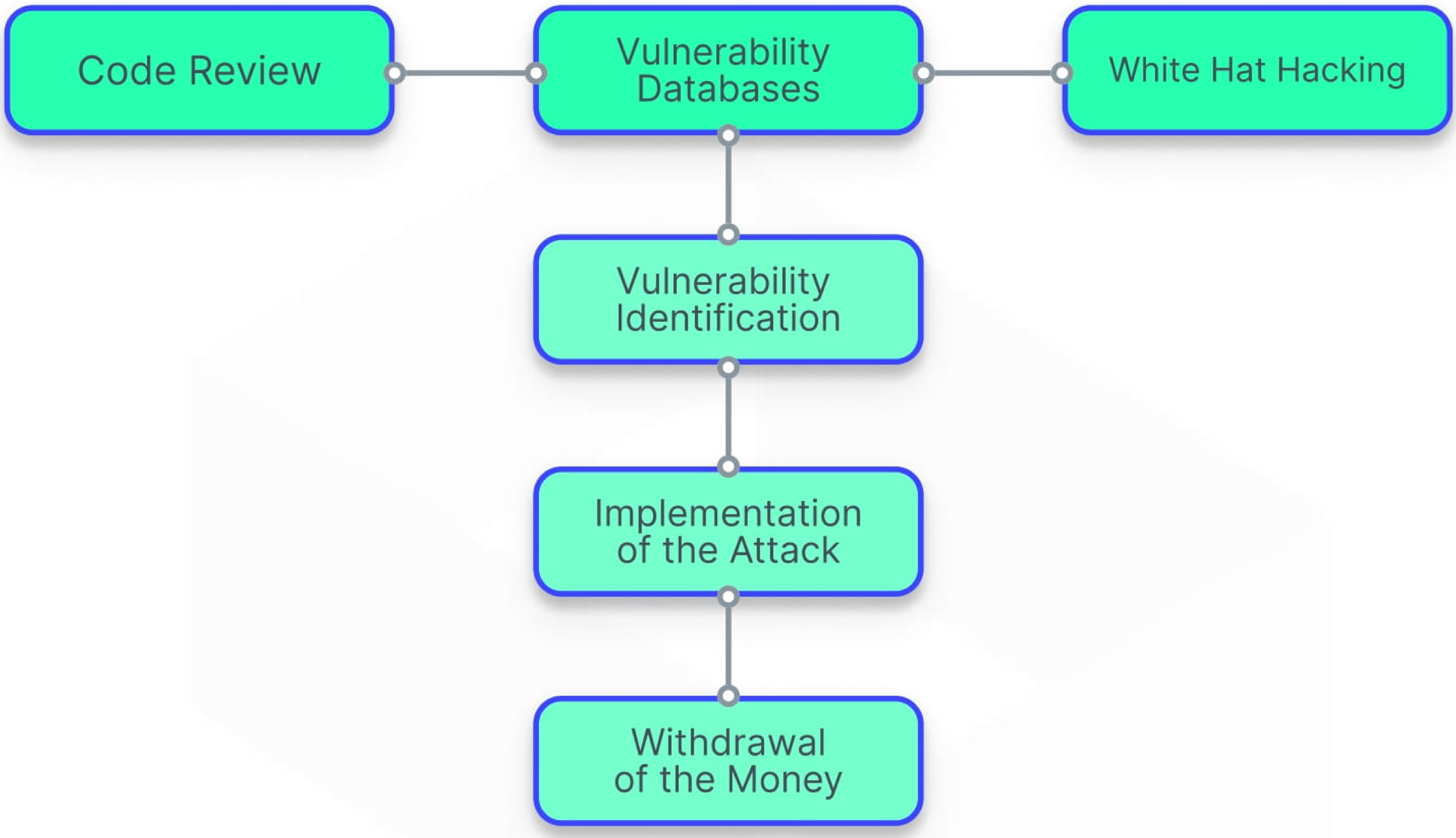
Vulnerability: Not enough security auditing hampers the smart contracts for known and unknown vulnerabilities to be discovered and utilized. Sadly, most project managers avoid doing audits due to the time constraints, or lack of funds, putting themselves in a vulnerable position to attack.

Case Study: Many DeFi projects were hacked because the audit was basic or superficial. A good example we can see is the Poly Network Hack (2021) which was a severe case of poor auditing, which led to a vulnerability that was exploited to steal over 600 million dollars, making it the largest DeFi hack to date.

Impact: This not only leads to mismanagement of resources in the form of financial losses but also erodes the confidence individuals place in decentralised systems hindering the influx of block chain technologies.

Decoding the Smart Contract Attack Lifecycle

Code review + Vulnerability Databases + White Hat Hacking [Vulnerability Identification] → [Exploitation Strategies Development] → [Implementation of the Attack] → [Withdrawal of the Money].



- **Discovery of Vulnerability:** Attacker finds out that there is a loophole in the smart contract.
- **Exploitation Planning:** A plan on how to take advantage of the weakness is then formulated.
- **Attack Execution:** Performs the attack in order to control the contract.
- **Funds Withdrawal:** Moves the stolen money, sometimes using mixers to hide the sources of the money.

Impact of Smart Contract Hacks

Assessment of Major Attacks on a Case-by-Case Basis

DAO Hack (2016):

The Decentralized Autonomous Organization (DAO) was an experiment on the Ethereum platform to enable people to vote on proposals using a decentralised platform. However, the DAO had a vulnerability in its smart contract code: a recursive function. This enabled a hacker to continuously initiate the withdrawals before the contract realized it had no money left, stealing approximately 63,000 Ether or roughly $70m at the time.

The attack had split the Ethereum community since the recovery of the stolen Ether needed the operation known as a "hard fork", which essentially is branching off the existing blockchain. This fork created two versions of Ethereum: Ethereum (Ether) and Ethereum Classic.

dForce Protocol Attack (2020):

dForce was an incorporated decentralized finance platform providing lending and borrowing solutions. In April 2020, hackers were able to breach it because of weakness in the management of functions within the contract. Due to this vulnerability, an attacker can continuously call the withdrawal function before the contract can update the balance and as result $25million was drained. This kind of attack called reentrancy attack happens when a contract does not lock its state during execution. Thankfully, most of the stolen funds were recovered most likely because the hacker is identifiable from the wallet addresses.

Ronin Network Hack (2022):

Axie Infinity associated Ronin Network blockchain was attacked, losing a record amount to hackers in terms of blockchain thefts. The hack was on the bridge that links the Ronin blockchain and Ethereum, which is a system that enables the movement of assets between two blockchains. The hackers were able to download the private key of the Ronin's validators, machines that confirm transactions and approved counterfeit withdrawals totaling $620 million. This pointed out significant security issues with cross-chain bridges; where the security is centralized on a selected number of validators. The hack underlined the importance of stronger multi-signature solutions with attention to increased use of decentralized validation solutions and services.

Recent Smart Contract Hacks

Year	Hack	Platform	Type of Attack	Amount Lost	Source
2016	DAO Hack	Ethereum	Code Bug Exploit	$70 million	Chainalysis, Gartner
2020	dForce Protocol Attack	dForce	Reentrancy Attack	$25 million	Chainalysis, IBM
2020	bZx Protocol Oracle Attack	bZx	Oracle Manipulation	$1 million	CipherTrace, Elliptic
2022	Ronin Network Hack	Axie Infinity	Bridge Attack	$620 million	Bridgecrew, Chainalysis
2023	Wormhole Exploit	Solana	Exploit in Smart Contract	$320 million	IBM Security, Elliptic

Industry Insights: Opinions of Leading Analysts

- **Gartner:** Estimates that blockchain security budgets will grow at a rate of 50% year on year until 2025 due to growing smart contract threats.
- **IBM Security:** Suggests that to effectively protect smart contracts, it is necessary to implement the zero-trust security model.
- **Bridgecrew:** Stresses on the fact that security is a constant process and requires constant updates.

BPSC (Best Practices for Securing Smart Contracts)

1 Comprehensive Security Audits

- Perform detailed and separate audit processes using the MythX tool and OpenZeppelin.
- Smart contract code should be updated periodically in order to counter new threats.

2 Employment of Certified Libraries and Development Frameworks

- Use existing libraries to minimise coding mistakes.
- Use secure development frameworks and should avoid using deprecated code.

3 Incorporate Runtime Threat Detection and Mitigation

- Runtime threat detection tools continuously monitor smart contract execution for vulnerabilities, anomalies, and malicious activities, allowing for early identification of potential threats

- By detecting threats in real time, mitigation strategies can be implemented promptly, minimising damage and preventing further exploitation.

4 Implementing Decentralised Oracles

- Always incorporate Decentralised Oracle Networks such as Chainlink to guarantee safe and accurate data feeds.
- It is also important to review and modify the oracle configurations from time to time to avoid being altered.

5 The Multi-Signature Wallets and Secure Access Controls

- This is to ensure that large transactions are authorised by more than one person to minimise cases of fraud.
- Employ RBAC to limit the functions according to users' roles and responsibilities.

6 Establishing Bug Bounty Programs

- Offer incentives to the ethical hackers such that they can help in the identification of the weaknesses.
- Promote program details to get more people to participate and to get the best hackers.

7 Constructing the Secure Development Lifecycle (SDL)

- Ensure that security features are incorporated into the system development life cycle.
- Perform static and dynamic analysis of the smart contract to ensure that the security of the smart contract is checked regularly.

Within today's industry, these best practices are being implemented into organisations' regular practices to utilise smart contracts securely. Blockchain platforms and DeFi projects are already adopting security features on their ecosystem as a part of the standard process in the process of development, with significant firms like OpenZeppelin, Quantstamp, SecureDApp etc. Further, on-chain data and price feed providers such as, Chainlink are emerging as the most common decentralised solution to contain off-chain data manipulation. Multiple signature wallet features and RBAC has been adopted by most organisations in order to improve the security of the transactions. There are some platforms, mainly in the DeFi segment, which stress on the idea of making these wrongdoings weak by giving out white-hat hackers bug bounties. Collectively, these initiatives demonstrate a proactivity on the part of the industry in securing smart contracts so that both parties and organisations engaging in decentralised applications can exercise confidence in the security of the based smart contract.

Practical Applications and Industry Success Stories

Case Study 1: Financial Sector Implementation

Through the cases of smart contracts in the financial industry, it has been realized that auditing and monitoring of such smart contracts significantly reduce the risks. An international bank recently implemented a smart contract auditing solution that enabled monitoring of decentralized finance. The bank was successfully minimizing threats by providing smart contract security features and through preemptive analysis, it reduced its risk factor by 70% during the first half of the year. Smart contracts in the financial sector provide opportunities to carry out large transactions quickly, eliminating third parties and being financially secure from frauds at the same time. Smart contracts should routinely be connected to auditing systems to detect such issues at an early stage, and thereby greatly reduce major money losses.

Case Study 2: Healthcare Industry

Of course, legal requirements and data privacy concern especially in the sector of Healthcare. An example of large-scale healthcare providers was using smart contracts to guarantee the patient records' safety. Such smart contracts allowed access to such information to be controlled and documented to legal regulatory standards such as HIPAA. Therefore, the organization got 100% legal compliance and the reduction of data breaches by 30%. Smart contracts assist in this regard because data access control is automated through the unique properties of blockchain to execute securely and transparently while offering an immutable solution for maintaining patient information.

Case Study 3: DeFi Platforms

Decentralized finance (DeFi) platforms, meanwhile, face a major problem of guarding their smart contracts controlling money transactions from outside influence. Some DeFi platforms depended on decentralized oracle suppliers to get their price feeds and all the other data they required. Price feeds are examples of data that smart contracts need to interact with a real-life action; therefore, protecting these inputs is deemed a priority. Thanks to optimization of decentralized oracles, the platform decreased the number of oracle-based attacks by 50%. Making a link between DeFi and smart contracts, we can define that smart contracts are essential to DeFi as they optimize transactions, while when connected with secure oracles, ensure that the data inputting into the smart contracts is not interfered with externally.

Future Trends in Smart Contract Security

1 The Use of Artificial Intelligence and Machine Learning

- It can be seen that the use of AI-based tools can detect the possible weaknesses quicker than through conventional methods.
- Machine learning models can predict the attack patterns and suggest the possible countermeasures to be taken.

2 Implementing Zero Trust Architecture in Blockchain

- A zero-trust model presumes that there is no trust and that it needs to be established and validated at every level of interaction.
- This model minimises chances of internal threats and unauthorised access.

3 Quantum Computing: In the next frontier, the preparation process is the key in order to succeed.

- Smart contracts are currently secured with encryption methods and the rise of quantum computing can be considered as a threat to them.
- Businesses have to look for quantum-safe cryptography to mitigate risks regarding their blockchain projects in the future.

SecureWatch

SecureWatch is a cutting-edge runtime threat detection and mitigation platform that shields decentralized applications (DApps) from a myriad of vulnerabilities. By continuously monitoring smart contract execution in real-time, SecureWatch proactively identifies and neutralizes potential threats, such as

- Monitor your sensitive functions like transferOwnership, pause, or upgrade
- Alert on potentially dangerous transactions on your contracts
- Respond by executing logic when key events happen
- Know when an unexpected volume of transactions or alerts occur. Etc

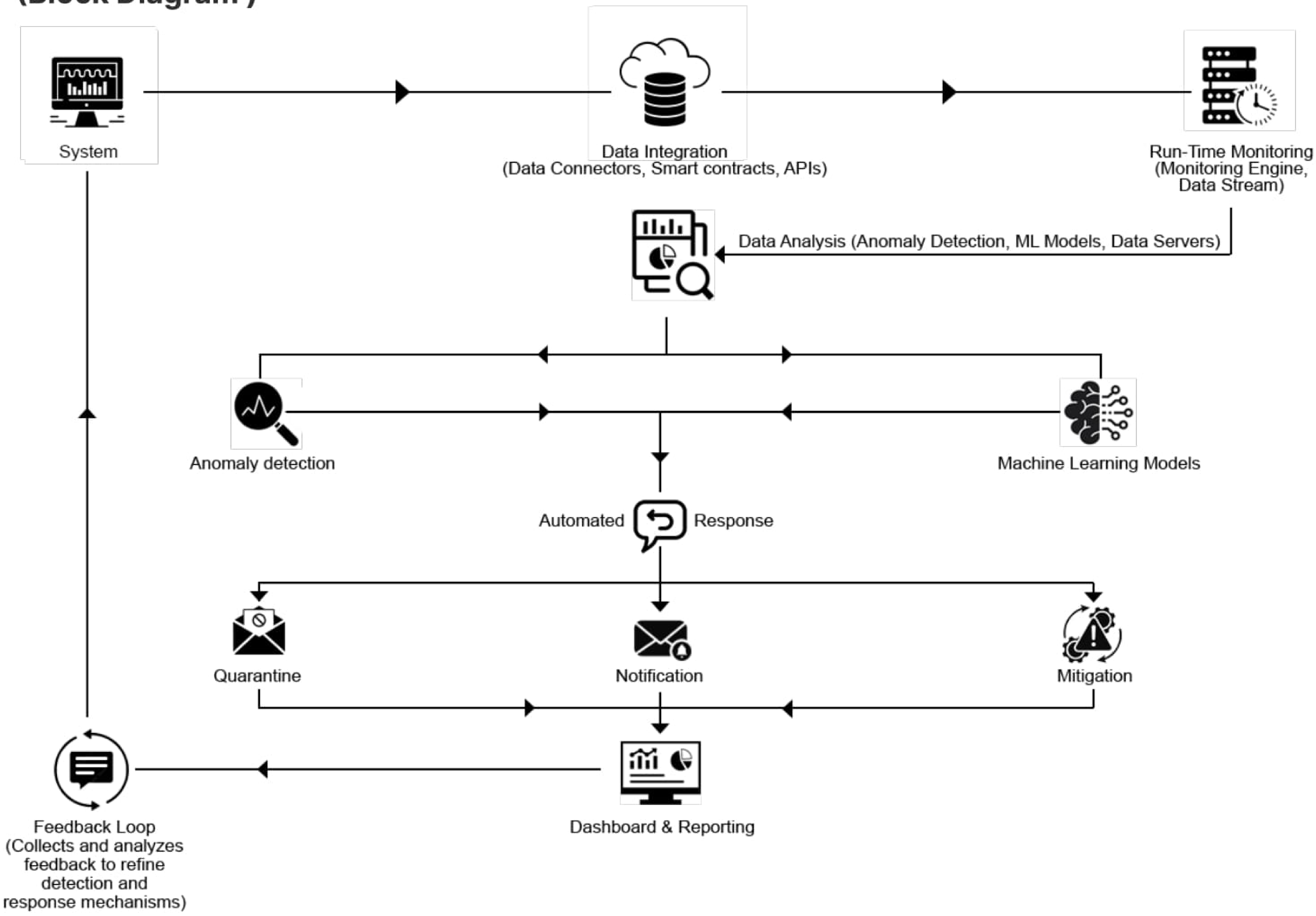
With its advanced mitigation strategies and customizable security profiles, SecureWatch empowers public and private DApp owners to build secure, resilient, and trustworthy applications, safeguarding their investments and fostering user confidence.

What sets SecureDApp apart from other solutions in this field is its holistic, end-to-end approach to smart contract security. While many platforms focus only on static security checks or post-deployment monitoring, SecureDApp integrates real-time threat detection, ongoing vulnerability scanning, and AI-powered threat mitigation. This ensures that threats are not only detected early but also neutralised before they can escalate. Furthermore, SecureDApp offers customizable security profiles that allow businesses to tailor protection strategies to their specific needs, making it both adaptable and scalable. Unlike competitors who rely solely on external audits, SecureDApp combines continuous monitoring with built-in security auditing, offering a comprehensive security solution that evolves with the platform.

Key Benefits of SecureWatch

- **Proactive Security:** Identify and address potential security threats in real-time.
- **User Confidence:** Build trust with your users by ensuring the security of their critical transactions.
- **Compliance Assurance:** Meet regulatory requirements with robust monitoring and reporting features.
- **Scalability:** Grow your business confidently with a scalable and adaptable monitoring solution.
- **Peace of Mind:** Focus on business growth while SecureWatch takes care of transaction security.
- **SecureWatch** – Where Security Meets Simplicity, ensuring the heartbeat of your web applications remains strong and secure.

SecureWatch (System-Integrated Proactive Threat Identification Tool - SIPTIT) (Block Diagram)



Conclusion

Smart contracts are changing the face of digital business leaving behind nothing but benefits in terms of automation, verifiability and cost. Though they present many benefits, these paradigms introduce explicit security threats that require low brass in order to protect the reliability of the underlying blockchain platforms.

Smart contracts are changing the face of digital business leaving behind nothing but benefits in terms of automation, verifiability and cost. Though they present many benefits, these paradigms introduce explicit security threats that require low brass in order to protect the reliability of the underlying blockchain platforms.

This whitepaper has illustrated that the threat for smart contracts is on the rise with billions of dollars at stake due to code errors such as, re-entry attacks, oracle manipulation, and inadequate or superficial security scans. What has been expressed in this document through the statistics and case studies is the evidence of the need for more vigorous security measures. These risks may be avoided by implementing standard procedures such as security audits regarding the platform, using only verified libraries for code implementation, decentralisation of oracle integration, implementation of multi-signature wallets, and the involvement of bug bounty programs.

In the future, using the new advancements including AI, machine learning and quantum residency cryptography were seen as vital applications to improving smart contract security. Still, such technological advancements need to be supported by a strong strategic plan combined with the use of zero-trust environments and a Secure Development Lifecycle (SDLC).

SecuredApp is committed to assisting organisations through these issues with certainty. Our all-encompassing solution includes security assessment supported by Artificial Intelligence, constantly scanning the environment for threats, proper coding of smart contracts and seamless, integrated bug bounty service, so clients get the best of both worlds and a comprehensive service for smart contract protection. Through collaboration with SecuredApp, it becomes possible not only to solve modern threats but also to avoid potential risks that might appear in the future, providing organisations with efficient security of their smart contracts.

SecuredApp is committed to assisting organisations through these issues with certainty. Our all-encompassing solution includes security assessment supported by Artificial Intelligence, constantly scanning the environment for threats, proper coding of smart contracts and seamless, integrated bug bounty service, so clients get the best of both worlds and a comprehensive service for smart contract protection. Through collaboration with SecuredApp, it becomes possible not only to solve modern threats but also to avoid potential risks that might appear in the future, providing organisations with efficient security of their smart contracts.

About Cybersecurity Center of Excellence

The Cybersecurity Center of Excellence (CoE) is a joint initiative of the Government of Telangana and Data Security Council of India (DSCI) to accelerate the cybersecurity momentum and create a conducive cybersecurity ecosystem that nurtures innovation, entrepreneurship and capability building. CoE works with all industry organisations, government agencies, academia and R&D centres and user groups and collaborates with other industry bodies, incubators and accelerators to accomplish its mission. DSCI is a not-for-profit, industry body on data protection in India, set up by NASSCOM®, committed to making cyberspace safe, secure and trusted by establishing best practices, standards and initiatives in cyber security and privacy. DSCI is the apex industry body for Cybersecurity in India.

About SecureDApp

SecureDApp is a leading blockchain security platform that provides a comprehensive suite of tools to safeguard decentralised applications (DApps) from a wide range of threats. By leveraging advanced threat detection, mitigation, and real-time monitoring capabilities, SecureDApp empowers DApp developers to build secure, reliable, and compliant applications. In addition to its robust security features, SecureDApp offers both product-based and hybrid smart contract auditing services and blockchain forensic investigations. This comprehensive approach ensures that DApps are thoroughly evaluated for vulnerabilities and can be effectively protected from malicious attacks, financial losses, and reputational damage.

CYBERSECURITY CENTRE of EXCELLENCE
A joint initiative of DSCI & Government of Telangana

DSCI
PROMOTING DATA PROTECTION
A NASSCOM® Initiative

SecureDApp

Take your security to the next level.

✉ Hello@securedapp.in

☎ +91 9606015868

🌐 www.securedapp.io