iJRASET
International Journal For Research in Applied Science and Engineering Technology



INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 14 **Issue:** V **Month of publication:** May 2026

DOI: https://doi.org/10.22214/ijraset.2026.83044

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538
Volume 14 Issue V May 2026- Available at www.ijraset.com

Cryptocurrency & Blockchain Technology: Types, Mechanisms, Security Threats & Major Hacking Incidents

Mohd Imtiyaz Gaus Shaikh
Master of Computer Applications (MCA), Institute of Distance and Open Learning, University of Mumbai
Dr. Shankar Dayal Sharma Bhavan, Vidyanagari, Santacruz (E), Mumbai - 400 098

Abstract: ***This research paper provides a comprehensive examination of cryptocurrency and blockchain technology two of the most transformative innovations of the 21st century. We explore the foundational principles of distributed ledger technology, the diverse taxonomy of cryptocurrencies, consensus mechanisms, smart contracts, and decentralised finance (DeFi). Additionally, this paper investigates the security landscape of the crypto ecosystem, cataloguing major hacking incidents, attack vectors, and mitigation strategies. The paper concludes with an outlook on future developments and regulatory trends.***

I. INTRODUCTION

The emergence of Bitcoin in 2009, introduced by the pseudonymous Satoshi Nakamoto, marked the beginning of a new paradigm in digital finance. At its core, Bitcoin introduced a peer-to-peer electronic cash system that eliminates the need for trusted intermediaries such as banks and payment processors. This was made possible by blockchain technology a distributed, immutable ledger that records all transactions across a network of nodes. Since then, the ecosystem has expanded dramatically. Thousands of cryptocurrencies have been created, each with distinct goals and underlying technology. Blockchain has transcended finance and found applications in supply chain management, healthcare, voting systems, digital identity, and more. At the same time, the enormous value locked in these systems has attracted malicious actors, resulting in billions of dollars in losses from hacks, exploits, and scams.

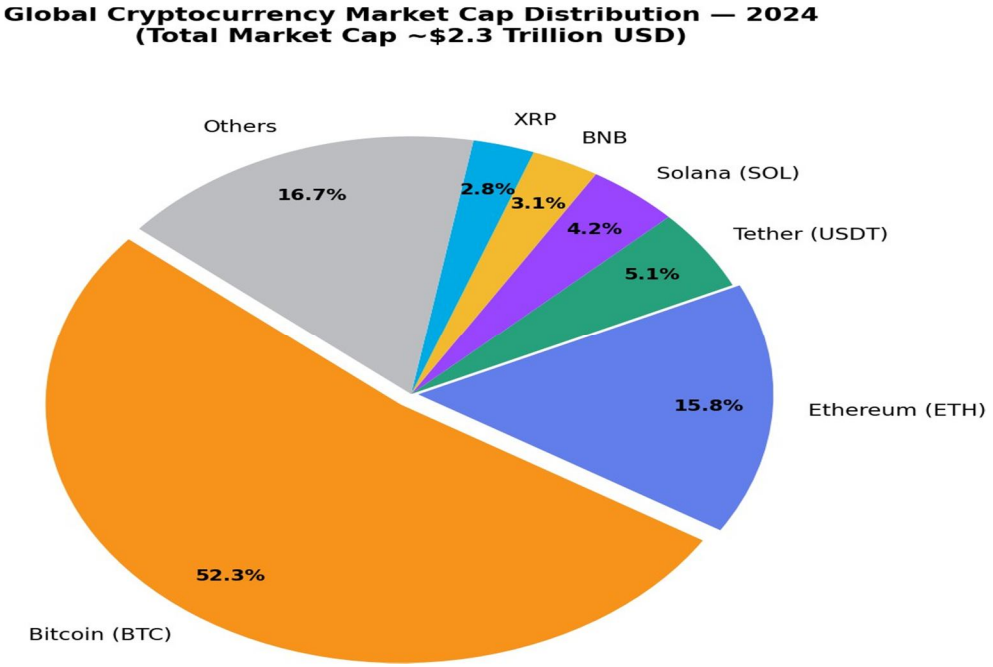


Figure B: Global Cryptocurrency Market Capitalisation Distribution 2024 (~$2.3 Trillion Total)

This paper aims to provide a rigorous, structured overview of this rapidly evolving landscape.

©IJRASET: All Rights are Reserved

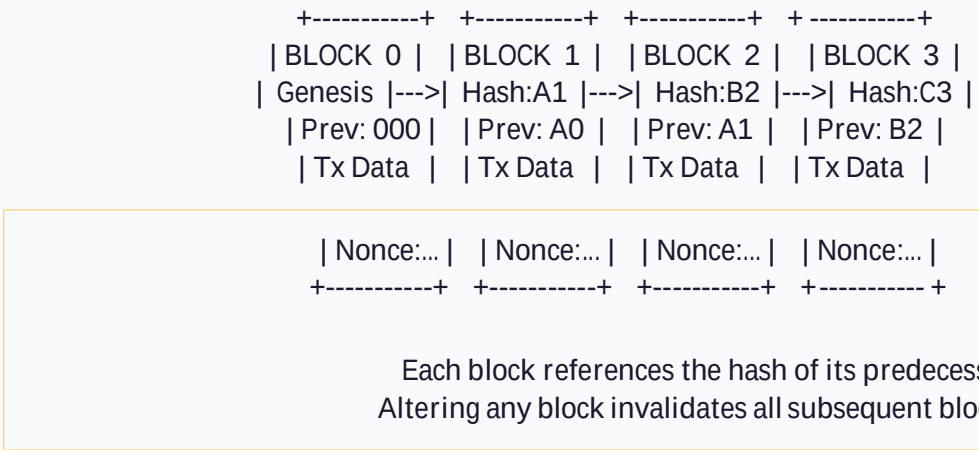
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538
Volume 14 Issue V May 2026- Available at www.ijraset.com

II. BLOCKCHAIN TECHNOLOGY: FOUNDATIONS

A. What is a Blockchain?

A blockchain is a type of distributed ledger technology (DLT) in which data is stored in a chain of blocks. Each block contains a cryptographic hash of the previous block, a timestamp, and transaction data forming an immutable, append-only record.

FIGURE 1: Blockchain Structure Linked Block Chain



B. Key Properties of Blockchain

1) Decentralisation: No single authority controls the chain; nodes share governance.
2) Immutability: Once confirmed, data cannot be altered without consensus.
3) Transparency: All transactions are publicly verifiable on public blockchains.
4) Security: Cryptographic hashing (SHA-256, Keccak-256) ensures data integrity.

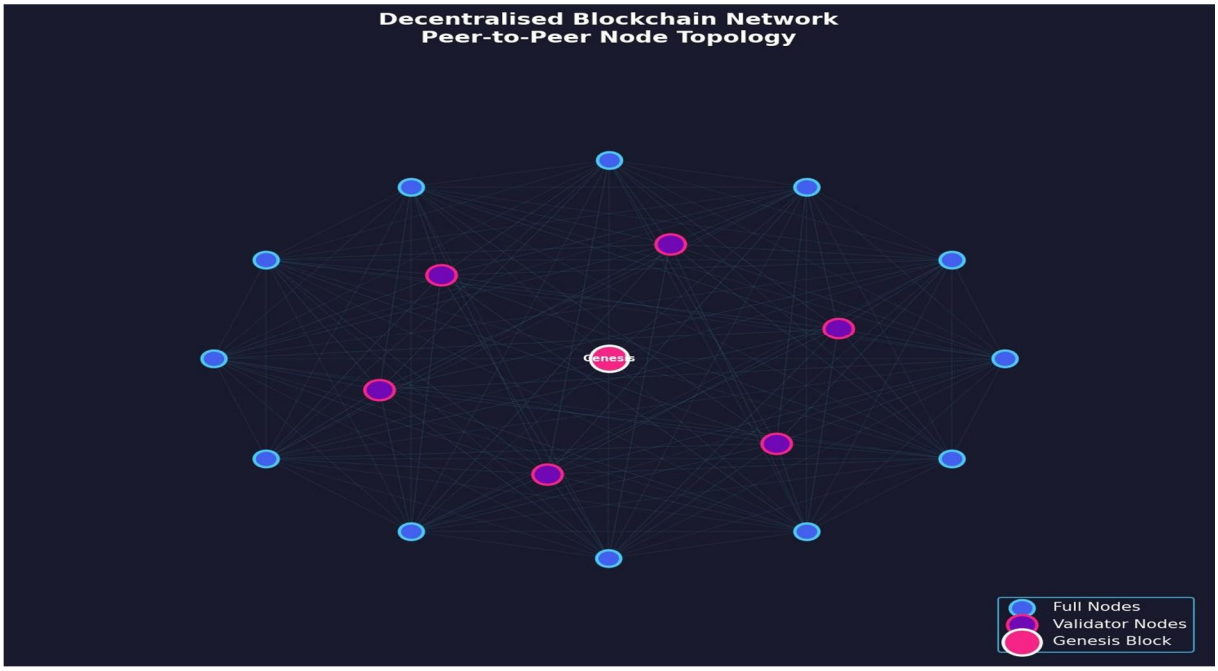


Figure C: Decentralised Peer-to-Peer Blockchain Network Every Node Holds a Full Copy of the Ledger

5) Consensus: Nodes agree on the state of the ledger via consensus protocols.

©IJRASET: All Rights are Reserved

C. Consensus Mechanisms

Consensus mechanisms are protocols that allow distributed nodes to agree on the validity of transactions without a central authority.

Mechanis m	Description & Examples
Proof of Work (PoW)	Miners compete to solve computational puzzles. Winner adds the next block. High energy consumption. Used by Bitcoin, Litecoin, Ethereum
Proof of Stake (PoS)	Validators are chosen based on the amount of cryptocurrency staked. Energy-efficient. Used by Ethereum (post-Merge), Cardano, Solana.
Delegated PoS (DPoS)	Token holders vote for delegates who validate blocks. High throughput. Used by EOS, TRON.
Proof of Authority (PoA)	Approved, known validators sign blocks. Used in private/permissioned chains (Hyperledger, VeChain).
Byzantine Fault Tolerance	Consensus achieved even if some nodes fail or act maliciously. Used by Tendermint, Cosmos.

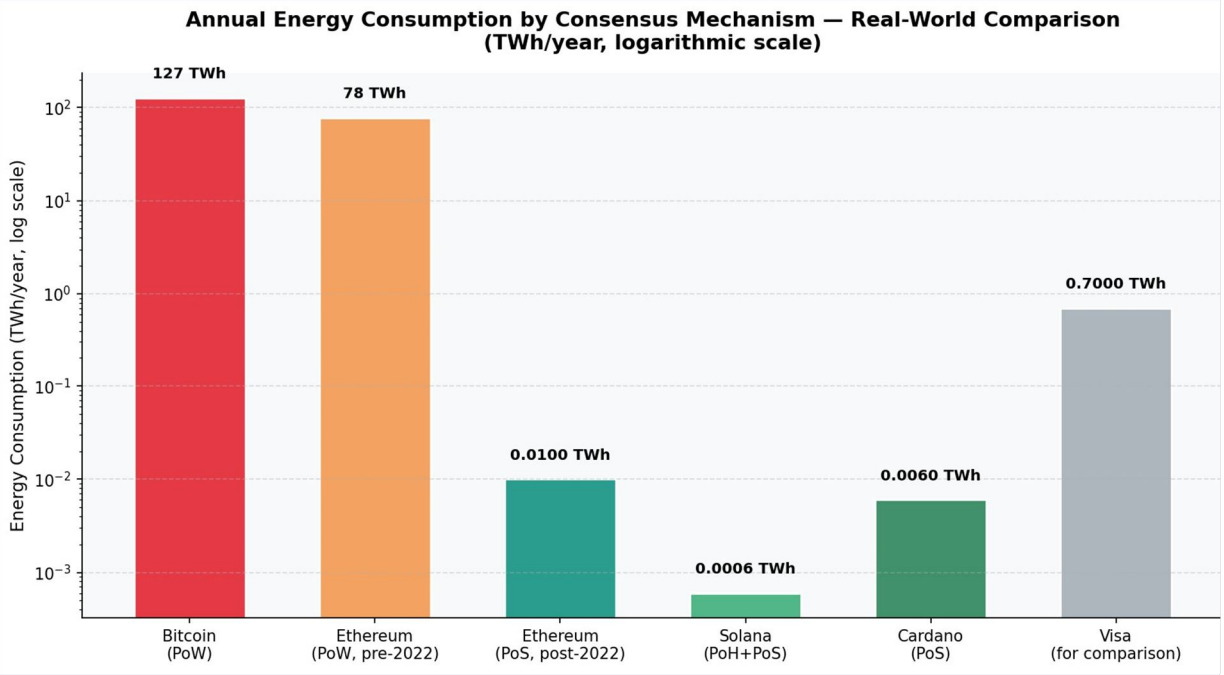


Figure D: Annual Energy Consumption by Consensus Mechanism Real-World Data (TWh/year, Log Scale)

FIGURE 2: Proof of Work vs Proof of Stake Comparison

PROOF OF WORK	PROOF OF STAKE
Miners race to solve SHA-256 puzzle	Validators are randomly selected (weighted by stake)
Winner broadcasts block	Validator proposes block
Network verifies solution	Other validators attest
Block added, miner rewarded	Block added, validator rewarded
Energy: Very High (~127 TWh/yr)	Energy: Very Low (~0.01 TWh/yr)
Security: Battle-tested	Security: Economic penalties (slashing)

D. Smart Contracts

Smart contracts are self-executing programs stored on a blockchain. They automatically enforce and execute the terms of an agreement when predefined conditions are met without requiring intermediaries.

Example: A smart contract for a loan: if the borrower repays the principal + interest by block 18,000,000, the collateral is automatically released. If not, the collateral is transferred to the lender.

III. TYPES OF CRYPTOCURRENCIES

The crypto ecosystem has evolved far beyond a simple digital currency. Today, cryptocurrencies span a wide spectrum of functions and technical designs.

A. Bitcoin (BTC) Digital Gold

Bitcoin is the first and most widely adopted cryptocurrency. Created by Satoshi Nakamoto in 2009, it operates on a Proof of Work consensus mechanism with a fixed supply of 21 million BTC. Bitcoin is primarily regarded as a store of value and a hedge against inflation often referred to as 'digital gold'.

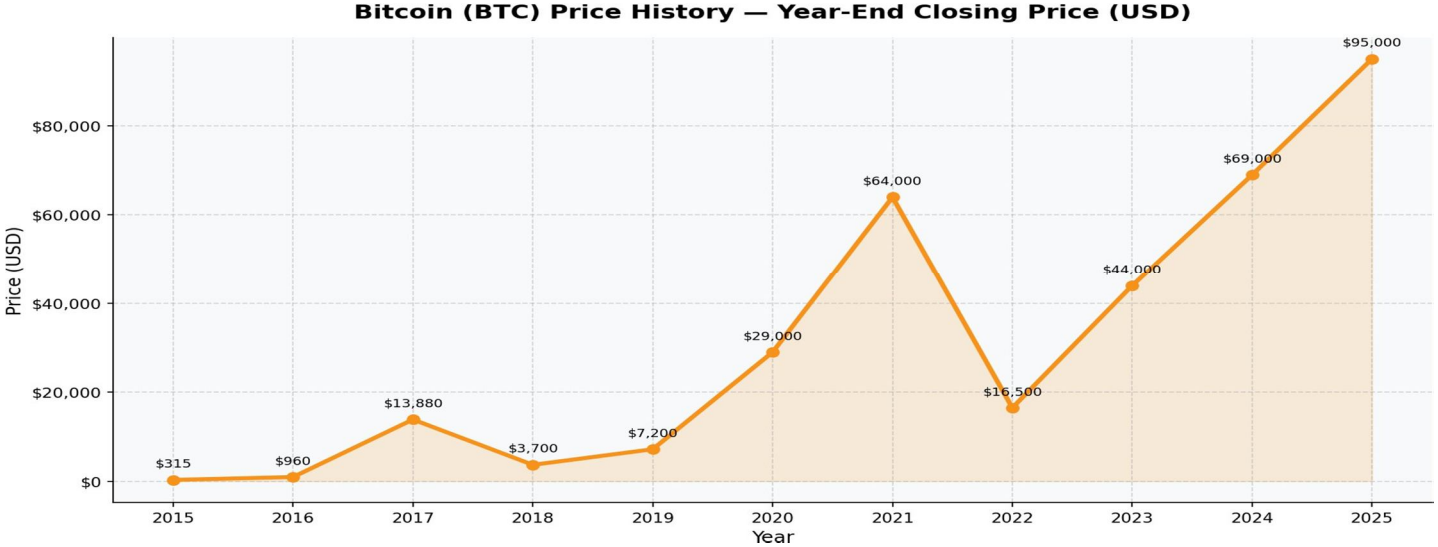


Figure A: Bitcoin (BTC) Year-End Closing Price (USD), 2015-2025 Real-World Market Data

A. Altcoins Alternative Cryptocurrencies

Altcoins are any cryptocurrency other than Bitcoin. They often introduce improvements or alternative use cases.

Altcoin	Key Features
Ethereum (ETH)	Smart contracts, EVM, DeFi hub, post-Merge PoS, ERC-20 tokens.
Litecoin (LTC)	Faster block times (2.5 min), Scrypt PoW, often called 'silver to Bitcoin's gold'.
Ripple (XRP)	Cross-border payments for banks, XRP Ledger, semi- centralised.
Cardano (ADA)	Peer-reviewed development, Ouroboros PoS, strong academic foundation.
Solana (SOL)	High throughput (65,000 TPS), Proof of History, popular for NFTs and DeFi.
Avalanche (AVAX)	Sub-second finality, three-chain architecture (X, P, C chains).

B. Stablecoins

Stablecoins are cryptocurrencies pegged to a stable asset, most commonly the US dollar. They provide price stability while maintaining the benefits of blockchain.

- Fiat-backed: USDT (Tether), USDC backed 1:1 with USD reserves.
- Crypto-backed: DAI collateralised by other crypto assets, governed by MakerDAO.
- Algorithmic: UST (now defunct) maintained peg via algorithmic supply/demand mechanisms.

C. Utility Tokens & Governance Tokens

Utility tokens grant access to a specific product or service within a blockchain ecosystem (e.g., Filecoin for decentralised storage). Governance tokens allow holders to vote on protocol changes (e.g., UNI for Uniswap, COMP for Compound).

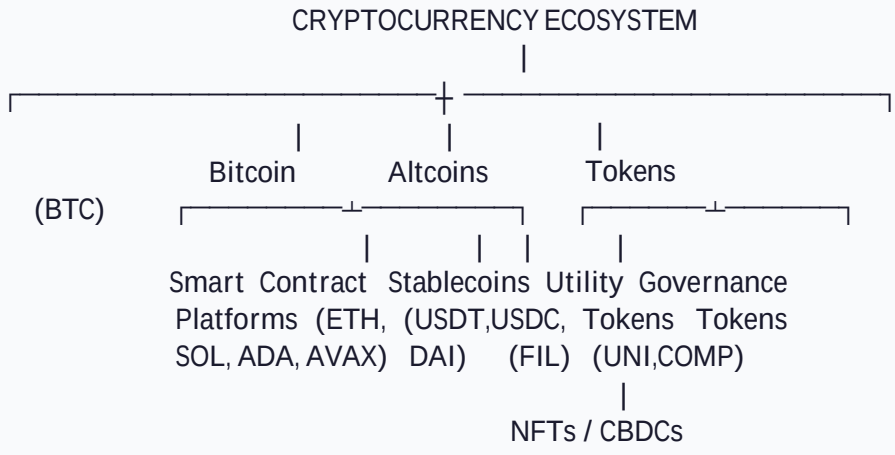
D. Non-Fungible Tokens (NFTs)

NFTs are unique cryptographic tokens on a blockchain that represent ownership of a distinct item digital art, music, in-game assets, or real-world property. Unlike fungible tokens, each NFT has a unique identifier and cannot be replicated.

E. Central Bank Digital Currencies (CBDCs)

CBDCs are government-issued digital currencies built on distributed ledger technology. Unlike decentralised cryptocurrencies, CBDCs are fully centralised and regulated. China's Digital Yuan (e-CNY) and the EU's Digital Euro are among the most prominent examples under development or pilot.

FIGURE 3: Cryptocurrency Taxonomy



ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538
Volume 14 Issue V May 2026- Available at www.ijraset.com

IV. DECENTRALISED FINANCE (DEFI)

DeFi refers to financial services and products built on public blockchains that operate without traditional intermediaries like banks, brokers, or exchanges. Using smart contracts, DeFi recreates and extends financial instruments in an open, permissionless, and transparent manner.

A. Core DeFi Components

- Decentralised Exchanges (DEXs): Platforms like Uniswap and Curve Finance allow peer-to-peer token swaps via automated market makers (AMMs).
- Lending & Borrowing: Protocols such as Aave and Compound allow users to earn interest or borrow against collateral.
- Yield Farming: Users provide liquidity to protocols in exchange for token rewards.
- Derivatives: Platforms like dYdX offer decentralised perpetual contracts and options.
- Insurance: Protocols like Nexus Mutual provide decentralised coverage for smart contract exploits.

DeFi TVL: At its peak in late 2021, the Total Value Locked (TVL) in DeFi protocols exceeded $180 billion USD, highlighting the rapid growth and adoption of decentralised finance.

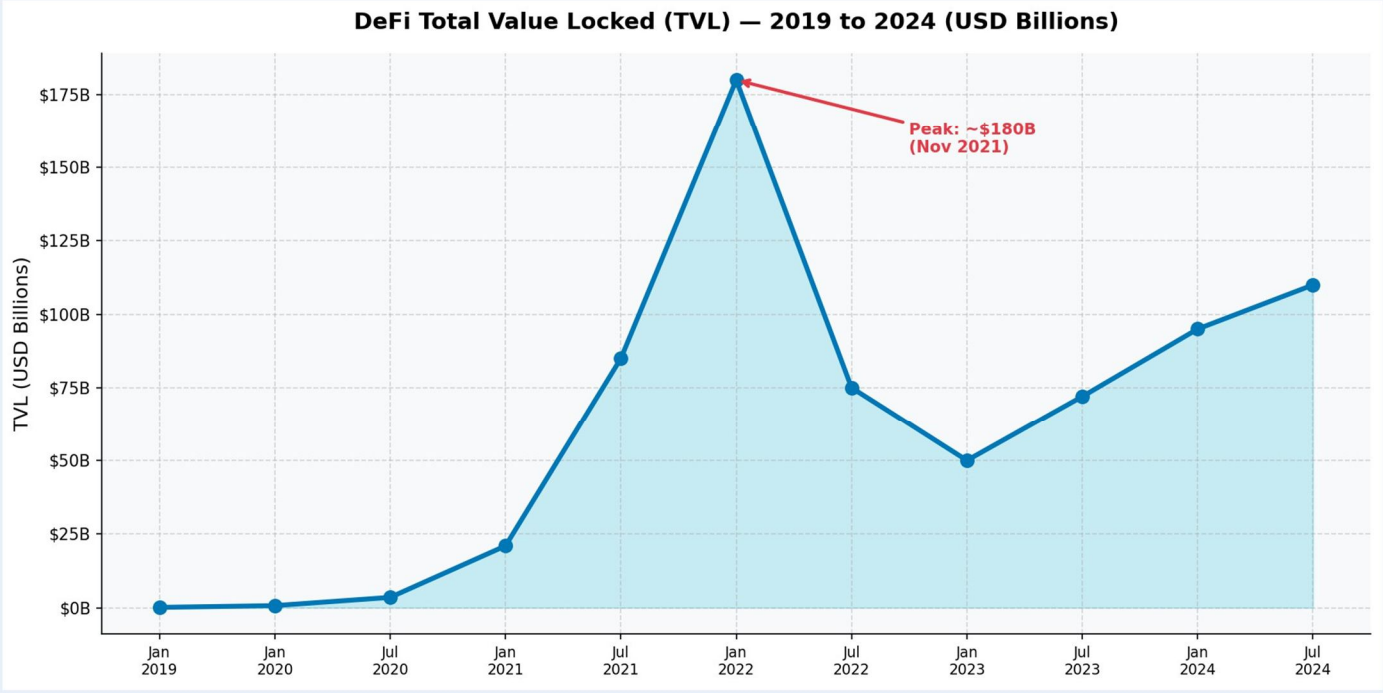


Figure E: DeFi Total Value Locked (TVL) 2019-2024 USD Billions. Peak: ~$180B (Nov 2021)

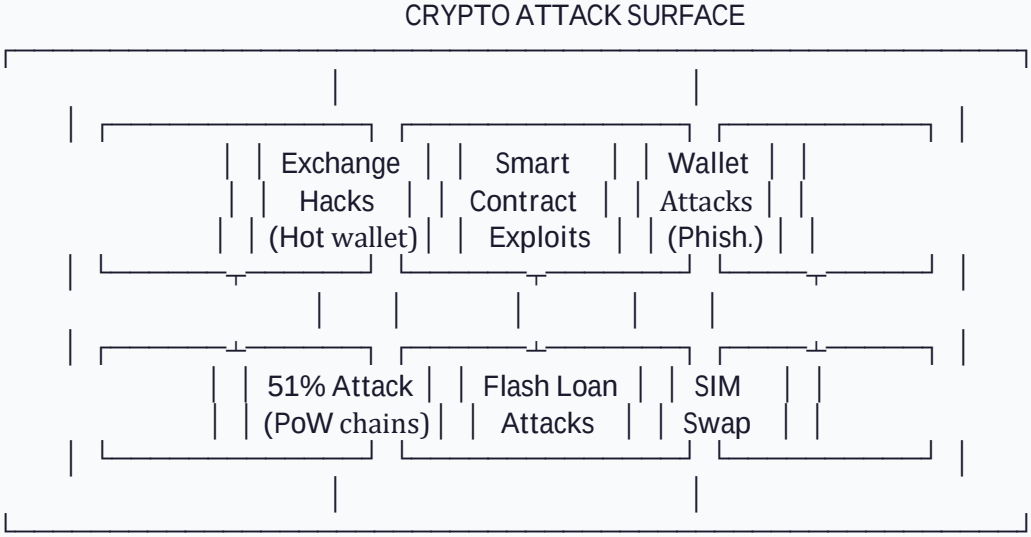
V. CRYPTOCURRENCY HACKING INCIDENTS

The significant value stored in crypto assets has made the ecosystem a prime target for malicious actors. Vulnerabilities exist across multiple layers: exchange infrastructure, smart contract code, private key management, and social engineering.

©IJRASET: All Rights are Reserved

A. Major Attack Vectors

FIGURE 4: Cryptocurrency Attack Surface Overview



B. Types of Attacks

1) Exchange Hacks

Centralized cryptocurrency exchanges (CEXs) are required to maintain a portion of their total holdings in hot wallets wallets that remain persistently connected to the internet in order to facilitate instant withdrawals, high- frequency trading, and seamless liquidity for millions of users around the clock. Because these wallets are always online and often hold hundreds of millions, sometimes billions, of dollars worth of digital assets, they represent one of the most lucrative and high-profile targets in the entire cybersecurity landscape. Unlike traditional banks, which benefit from decades of regulatory oversight, insurance schemes, and battle-tested infrastructure, many cryptocurrency exchanges particularly smaller or newer ones have historically operated with immature security frameworks. This creates a dangerous gap between the sheer volume of value being stored and the level of protection surrounding it. Attackers exploit this gap through multiple vectors. Weak security practices such as inadequate access controls, poor password policies, absence of hardware security modules (HSMs), or failure to enforce multi-factor authentication on critical internal systems can give adversaries a foothold into the exchange's backend infrastructure. Once inside, navigating toward hot wallet credentials or private keys becomes a matter of persistence and privilege escalation.

Unpatched software presents an equally serious threat. Exchanges rely on complex, multi-layered technology stacks including web servers, trading engines, wallet management systems, and third-party APIs. A single unpatched vulnerability in any one of these components can serve as an entry point. The history of cryptocurrency is littered with catastrophic exchange breaches that underscore just how costly these security failures can be. The most iconic case remains Mt. Gox, once the world's largest Bitcoin exchange, handling over 70% of all global Bitcoin transactions at its peak. Between 2011 and 2014, attackers silently and systematically drained approximately 850,000 Bitcoin worth around $450 million at the time, and an almost incomprehensible sum by today's valuations directly from its hot wallets. What made the Mt. Gox breach particularly alarming was not just its scale, but its invisibility. The theft went undetected for years, largely due to the exchange's failure to conduct regular audits, reconcile wallet balances, or implement even rudimentary transaction monitoring. By the time the breach was publicly acknowledged in February 2014, the damage was total and irreversible. Mt. Gox filed for bankruptcy shortly after, leaving hundreds of thousands of users with devastating losses and triggering one of the first major crises of confidence in centralized crypto infrastructure. A similar pattern of negligence unfolded with Coincheck in January 2018, when Japanese exchange lost approximately $534 million worth of NEM tokens in what became one of the largest single exchange hacks in history. Investigators found that Coincheck had stored nearly all of its NEM holdings in a single hot wallet, without the protection of multi-signature authorization a basic security measure that requires multiple approvals before any transaction can be executed. The exchange had reportedly been aware of its security shortcomings but had failed to act on them in time, once again demonstrating that awareness without action is no defense at all.

The Bitfinex hack of 2016 offered yet another case study in the dangers of flawed implementation. Attackers exploited a vulnerability in the exchange's multi-signature wallet architecture a system that was ironically designed to enhance security and made off with nearly 120,000 Bitcoin, valued at approximately $72 million at the time. The breach raised serious questions about the security of third-party custody solutions and whether exchanges fully understood the systems they were deploying to protect user funds. The infamous Binance hack of 2019 took a more sophisticated approach. Rather than exploiting a single vulnerability, attackers orchestrated a patient, multi-stage campaign that combined phishing techniques and custom malware to quietly harvest API keys and two-factor authentication codes from a large number of user accounts over an extended period. When they finally struck, they executed a single, precisely coordinated withdrawal of over 7,000 Bitcoin approximately $40 million in one transaction, carefully structured to pass Binance's automated risk checks. The attack was a stark reminder that even well-resourced, security-conscious exchanges with robust infrastructure can fall victim to adversaries who are willing to invest time, creativity, and patience. More recently, the Bybit hack of February 2025 set a chilling new benchmark, with attackers widely attributed to the North Korean Lazarus Group stealing approximately $1.5 billion in Ethereum, making it the largest exchange hack ever recorded. What distinguished this attack was its sophistication: the hackers did not breach Bybit's systems directly. Instead, they compromised the Safe multisig wallet interface used by Bybit's signers, manipulating the transaction display so that internal approvers unknowingly authorized a malicious smart contract that transferred control of the funds to the attackers. It was a masterclass in supply chain deception, exploiting human trust in familiar interfaces rather than attacking underlying code.

Taken together, these incidents paint a consistent and sobering picture: whether through years of silent drainage, negligent architecture, implementation flaws, sophisticated social engineering, or supply chain manipulation, hot wallets remain the Achilles' heel of centralized exchanges. The consequences extend far beyond the exchange itself users lose funds with little to no legal recourse, market confidence erodes, token prices crash, and the broader perception of cryptocurrency as a safe store of value is repeatedly undermined.

2) Smart Contract Exploits

Smart contracts are immutable once deployed, meaning bugs cannot easily be patched. Attackers exploit logic errors, re-entrancy bugs, integer overflows, and oracle manipulation to drain funds from DeFi protocols.

Re-entrancy attacks represent one of the oldest and most destructive classes of smart contract vulnerabilities, made infamous by the catastrophic DAO hack of 2016. In a re-entrancy attack, a malicious contract repeatedly calls back into the vulnerable contract before the initial execution has finished essentially withdrawing funds in a rapid, recursive loop before the contract's internal balance is ever updated. The DAO hack exploited precisely this flaw, draining over $60 million worth of Ether and ultimately forcing a controversial hard fork of the Ethereum blockchain to recover the funds a decision that split the community and gave birth to Ethereum Classic. Despite being one of the most well-documented vulnerabilities in the history of DeFi, re-entrancy attacks continue to resurface. The Cream Finance hack of 2021 demonstrated that even experienced development teams can inadvertently reintroduce this vulnerability when integrating complex, composable protocols, resulting in losses exceeding $130 million.

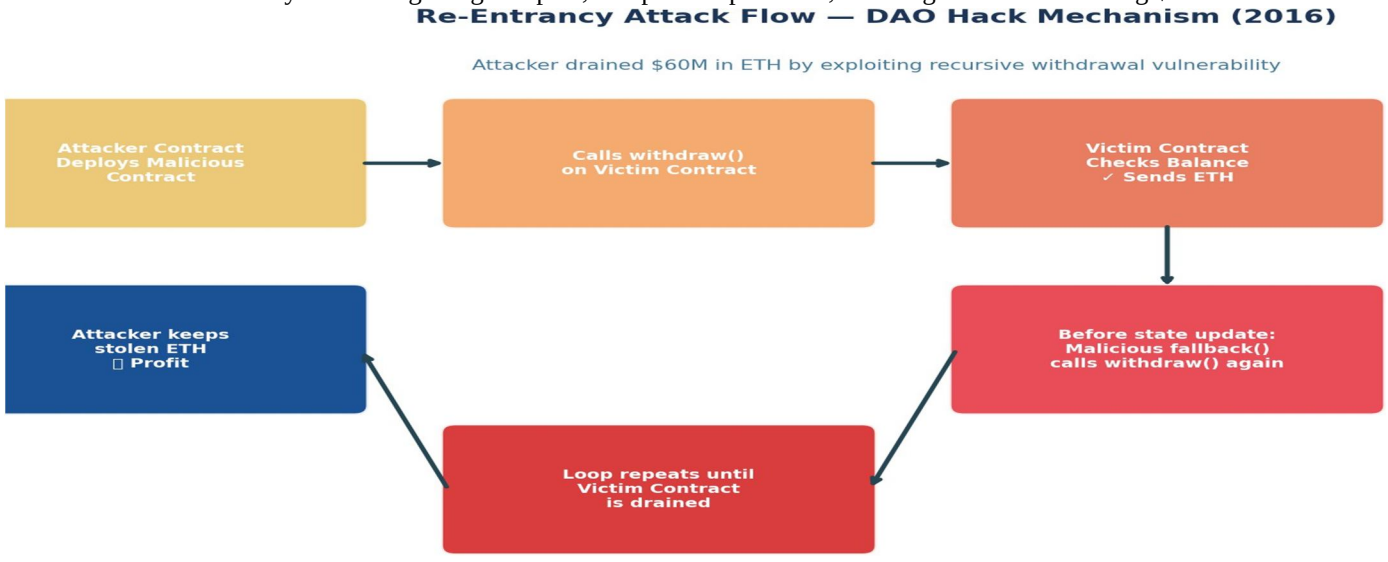


Figure G: Re-Entrancy Smart Contract Attack Flow DAO Hack Mechanism (2016, ~$60M Drained)

Oracle manipulation has emerged as one of the most sophisticated and frequently exploited attack vectors in modern DeFi. Smart contracts, by design, cannot access real-world data on their own they rely on external data feeds called oracles to retrieve asset prices, interest rates, and other critical inputs.

When these price feeds are insufficiently decentralized or can be temporarily influenced, attackers exploit the gap between the manipulated on-chain price and the true market value. Flash loan attacks have supercharged this vulnerability dramatically by borrowing enormous sums of capital within a single atomic transaction at zero upfront cost, attackers can artificially inflate or crash the price of a thinly traded asset on a decentralized exchange, trick a lending protocol into issuing a vastly over-collateralized loan, and vanish with the proceeds all within a single block. The Mango Markets exploit of 2022 is a stark illustration of this, where an attacker used their own capital to manipulate the price of MNGO tokens, artificially inflated their collateral value, and borrowed approximately $117 million against it before the protocol could react.

Integer overflows and logic errors, while less cinematic than flash loan attacks, are equally dangerous and often more difficult to detect during routine code reviews. An integer overflow occurs when an arithmetic operation produces a value that exceeds the maximum size the variable can hold, causing it to wrap around to an unintended number a flaw that can be weaponized to mint unlimited tokens, bypass balance checks, or unlock funds that should be inaccessible. Beyond raw arithmetic bugs, broader logic errors flaws in the fundamental business rules encoded into the contract can be just as devastating. The Euler Finance hack of March 2023, which resulted in losses of nearly $197 million, stemmed from a logic flaw in its donation mechanism that allowed an attacker to create an artificial bad debt position and systematically drain multiple asset pools. What makes these vulnerabilities particularly dangerous is that, unlike traditional software, there is no patch button once a smart contract is live on the blockchain, its code is permanent.

Developers can deploy upgraded contract versions or implement emergency pause mechanisms, but only if such features were built in from the start, and only if the team identifies the flaw before an attacker does.

3) 51% Attacks

To understand why this is so dangerous, it is essential to first grasp how Proof of Work consensus actually functions. In a PoW blockchain, miners compete to solve computationally intensive cryptographic puzzles, and the first to succeed earns the right to append the next block to the chain.

The network collectively agrees that the longest valid chain the one with the most cumulative computational work behind it represents the true and authoritative transaction history. This mechanism works as intended when no single participant controls enough mining power to consistently outpace the rest of the network. The moment that assumption breaks down, the entire foundation of trustless consensus begins to crumble. When a malicious actor accumulates majority hash rate, they gain the ability to secretly build an alternative version of the blockchain in private commonly referred to as a shadow chain while the rest of the network continues building on the legitimate one. The attacker can simultaneously spend their cryptocurrency on the public chain, and once their shadow chain surpasses the honest chain in length, broadcast it to the network, effectively erasing those original transactions and returning the spent coins to their own wallet the essence of a double-spend attack.

Smaller Proof of Work blockchains are disproportionately exposed to this threat for a straightforward economic reason the cost of attacking a network is directly tied to the total hash rate required to achieve majority control. On Bitcoin, amassing 51% of the global hash rate would require billions of dollars in specialized ASIC hardware, infrastructure, and electricity, making any attack economically irrational. On smaller chains, however, the required investment is a fraction of that cost. The rise of hash rate rental marketplaces such as NiceHash has made it possible for attackers to temporarily rent enormous mining power for just a few thousand dollars, execute a targeted attack within hours, and disappear before the network can respond dramatically lowering the barrier to entry and transforming 51% attacks from theoretical concerns into repeatable, low-cost exploits.

The real-world toll has been both frequent and severe. Ethereum Classic (ETC) suffered multiple 51% attacks in 2020, with one attacker reorganizing over 7,000 blocks and rewriting more than two days of transaction history.

Bitcoin Gold (BTG) was successfully attacked in both 2018 and 2020, with attackers double-spending an estimated $70,000 and $72,000 respectively across the two incidents. Beyond direct financial damage, these attacks trigger a systemic loss of trust when exchanges and merchants can no longer guarantee transaction finality, the rational response is to require dramatically more confirmations before crediting funds, making the network slow and impractical. Several exchanges have delisted smaller PoW coins entirely following repeated attacks, and in this way a 51% attack does not merely steal funds it can permanently undermine the utility and economic viability of the targeted blockchain.

4) Flash Loan Attacks

What makes flash loans uniquely dangerous as an attack vector is that they fundamentally eliminate the traditional barrier of capital. In conventional finance, executing a large-scale market manipulation requires an attacker to already possess or somehow borrow enormous amounts of capital, creating a natural economic deterrent. Flash loans dissolve this deterrent entirely. By borrowing tens or even hundreds of millions of dollars worth of assets instantaneously, at zero upfront cost and with no credit checks or collateral requirements, an attacker gains the temporary purchasing power of a whale within a single atomic transaction. This borrowed capital is then deployed across multiple DeFi protocols in rapid succession manipulating price feeds, exploiting arbitrage gaps, draining liquidity pools, or triggering cascading liquidations all within the span of a single block, which on Ethereum takes approximately 12 seconds. If any step in the sequence fails, the entire transaction is automatically reversed as though it never occurred, meaning the attacker bears virtually no financial risk while the potential upside remains enormous.

The mechanics of a typical flash loan price manipulation attack follow a well-established pattern. An attacker borrows a massive amount of a target asset, then uses that volume to artificially inflate or crash the price of that asset on a thinly traded decentralized exchange typically one that a lending protocol relies on as its price oracle. Because the lending protocol reads this manipulated price as the current market rate, it becomes temporarily blind to reality, allowing the attacker to borrow far more than they should be entitled to, or to liquidate other users' positions at artificial prices for profit. The bZx attacks of February 2020 were among the first high-profile demonstrations of this technique, where an attacker used a flash loan to manipulate the price of WBTC on Uniswap, tricked the bZx lending protocol into issuing an undercollateralized loan, and walked away with approximately $350,000 in profit across two separate attacks within days of each other effectively announcing to the entire DeFi ecosystem that flash loan exploits were no longer theoretical. The Pancake Bunny exploit of 2021 followed a similar blueprint, with attackers borrowing a massive amount of BNB, using it to artificially pump the price of the BUNNY token, triggering the protocol's own minting mechanism against itself, and draining nearly $45 million before repaying the flash loan and vanishing all within a single transaction.

What makes defending against flash loan attacks particularly difficult is that the vulnerability rarely lies in the flash loan mechanism itself it lies in the protocols that interact with manipulable price sources and fail to account for the possibility of sudden, extreme, and artificial price movements. A protocol that reads its asset prices from a single low-liquidity decentralized exchange, without using time-weighted average prices or cross-referencing multiple independent oracles, is essentially operating with a blindfold that a well- capitalized attacker can exploit at will. The broader lesson the DeFi ecosystem has drawn from years of flash loan exploits is that composability the ability of protocols to freely interact with one another is both DeFi's greatest strength and its most exploitable weakness. Every integration point between protocols is a potential attack surface, and the speed and capital efficiency that flash loans provide mean that attackers can probe and exploit these surfaces at a scale and velocity that was simply not possible before this financial primitive existed.

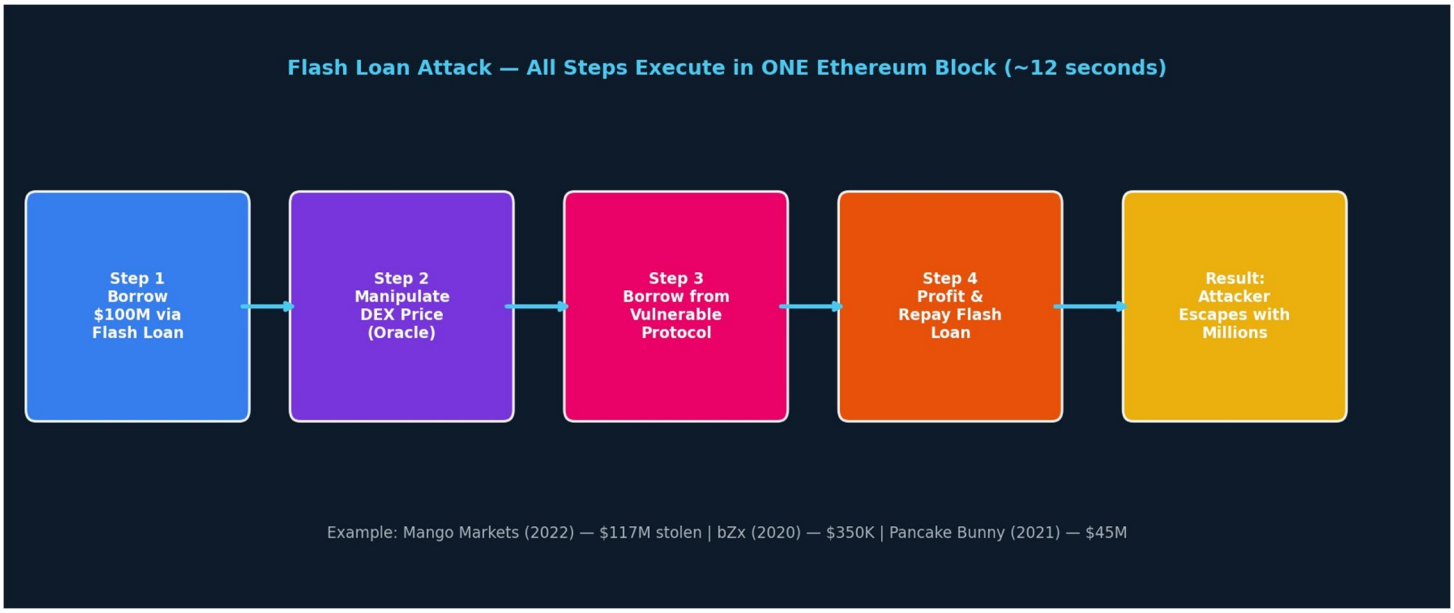


Figure H: Flash Loan Attack Borrow, Manipulate, Exploit, Repay all in One ~12-Second Block

5) Phishing & Social Engineering

Phishing in the cryptocurrency space has evolved far beyond the crude, easily detectable email scams of the early internet era into a highly sophisticated, precisely targeted discipline that exploits both technical vulnerabilities and fundamental human psychology. Attackers invest considerable effort in constructing pixel-perfect replicas of legitimate exchange websites, wallet interfaces, and DeFi protocol front-ends complete with authentic-looking domain names that differ from the genuine site by a single character, a transposed letter, or a substituted homoglyph that is virtually invisible to the naked eye. Victims who land on these counterfeit pages and enter their credentials, private keys, or seed phrases hand attackers complete and irreversible control over their wallets in an instant. Beyond fake websites, spear-phishing campaigns have become increasingly common, where attackers conduct detailed research on high-value targets studying their on- chain holdings, social media activity, and known project affiliations before crafting deeply personalized messages that impersonate trusted colleagues, project founders, or exchange support staff with alarming credibility. The Ronin Network hack of 2022, which resulted in the theft of approximately
$625 million, was partly traced back to a fake job offer PDF sent to a senior engineer at Sky Mavis a single malicious document that ultimately served as the initial foothold for one of the largest cryptocurrency heists ever recorded.

SIM swapping represents one of the most invasive and difficult-to-defend social engineering attacks in the cryptocurrency threat landscape, because it does not attack the victim's devices or software directly it attacks the telecommunications infrastructure that underpins their identity verification. In a SIM swap attack, the adversary contacts the victim's mobile carrier, impersonates them using a combination of personally identifiable information harvested from data breaches, social media profiles, or purchased from underground markets, and convinces the carrier's customer service representative to transfer the victim's phone number to a SIM card under the attacker's control. From that moment forward, every SMS-based two-factor authentication code, every account recovery message, and every login verification sent to that number is intercepted by the attacker rather than the legitimate owner. Armed with this capability, attackers can systematically reset passwords and bypass 2FA on exchange accounts, email inboxes, and cloud storage creating a cascading breach that can drain every linked account within minutes. Michael Terpin, a prominent cryptocurrency investor, suffered a SIM swap attack in 2018 that resulted in the theft of approximately
$24 million worth of cryptocurrency, subsequently filing a landmark $224 million lawsuit against AT&T for negligence in allowing the swap to proceed despite security protections supposedly being in place on his account. What makes both phishing and SIM swapping particularly devastating in the cryptocurrency context is the absolute absence of a recovery mechanism once funds have been moved. In traditional banking, a fraudulent transfer can be flagged, frozen, or reversed through established dispute resolution processes. In cryptocurrency, a transaction confirmed on the blockchain is final there is no customer service line to call, no fraud department to escalate to, and no governing authority with the power to intervene. Attackers exploit this irreversibility deliberately and systematically, immediately routing stolen funds through mixers, cross-chain bridges, and peer-to-peer exchanges the moment they gain access, ensuring that by the time the victim realizes what has happened, the trail is already cold. The crypto industry has responded with measures such as hardware security keys, authenticator app-based 2FA, withdrawal address whitelisting, and anti-phishing codes embedded in official communications but the fundamental reality remains that in an ecosystem built on self-sovereignty and trustless transactions, the human being sitting at the keyboard will always be the most exploitable element in the entire security chain.

C. Notable Hacking Incidents

Year	Incident	Loss (USD)	Method	Outcome
2014	Mt. Gox (Bitcoin)	~$450M	Hot wallet compromise / insider fraud	Exchange declared bankruptcy; ~850,000 BTC lost
2016	The DAO (Ethereum)	~$60M	Re-entrancy smart contract exploit	Ethereum hard- forked to recover funds
2018	Coincheck (NEM)	~$534M	Hot wallet, insufficient security	Partial repayment to users; exchange restructured
2020	KuCoin Exchange	~$281M	Private key compromise	~84% recovered through legal action & freezing
2021	Poly Network	~$611M	Cross-chain bridge smart contract bug	Hacker returned all funds; largest DeFi hack at time
2022	Ronin Network (Axie)	~$625M	Compromised validator private keys	Largest DeFi hack to date; US sanctions on Lazarus
2022	Wormhole Bridge	~$320M	Signature verification flaw in bridge contract	Jump Crypto injected $320M to cover losses
2022	Nomad Bridge	~$190M	Faulty message verification logic	Chaotic free-for- all; partial recovery
2023	Euler Finance	~$197M	Donation attack + flash loan exploit	Hacker returned ~$177M after negotiations
2024	Radiant Capital	~$50M	Malware on developer machines; multisig compromise	Ongoing investigation; Lazarus Group suspected

Cumulative Losses: According to Chainalysis, over $7 billion USD was stolen from crypto projects in 2022 alone primarily from cross-chain bridge exploits and DeFi protocol hacks.

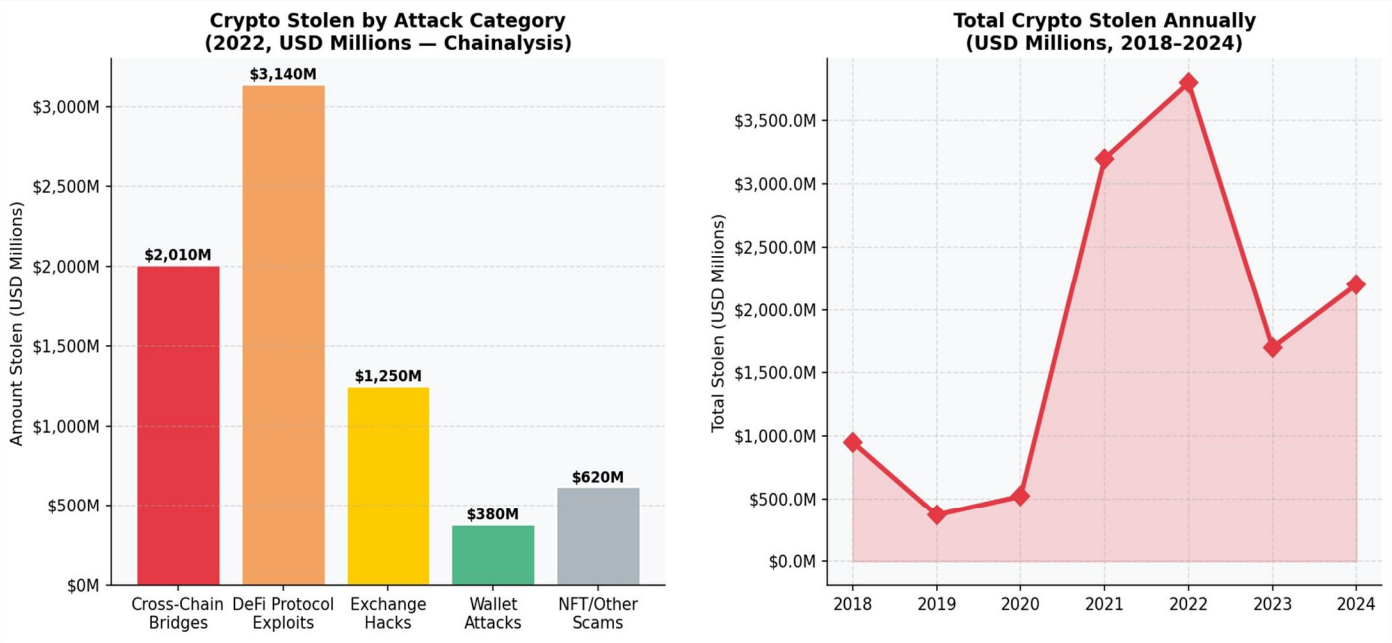


Figure I: Total Cryptocurrency Stolen Annually (2018-2024) & by Attack Category in 2022 (Chainalysis)

FIGURE 5: Timeline of Major Cryptocurrency Hacking Incidents

MAJOR CRYPTO HACK TIMELINE

2014 ● Mt. Gox: $450M (850K BTC stolen)
2016 ● The DAO: $60M (Ethereum hard fork follows)
2018 ● Coincheck: $534M (largest at the time)
2020 ● KuCoin: $281M (private key leak)
2021 ● Poly Network: $611M (fully returned!)
2022 ● Ronin / Axie: $625M (N. Korea Lazarus Group)
2022 ● Wormhole Bridge: $320M
2022 ● Nomad Bridge: $190M
2023 ● Euler Finance: $197M (mostly returned)
2024 ● Radiant Capital: $50M (Lazarus suspected)

Total estimated losses (2014-2024): > $15 Billion USD

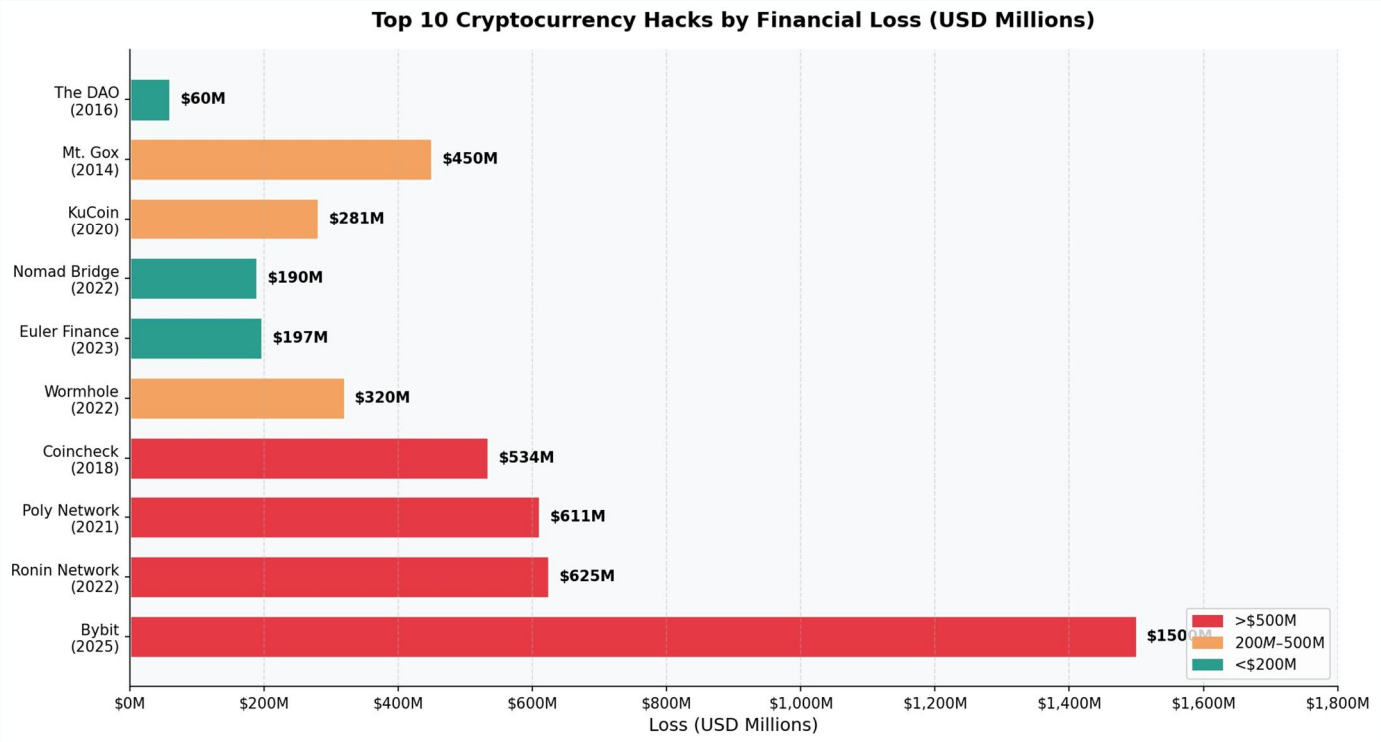


Figure F: Top 10 Cryptocurrency Hacks by Financial Loss (USD Millions), 2014-2025

VI. SECURITY BEST PRACTICES & MITIGATIONS

A. *For Exchanges & Protocols*

- Store the majority of funds in cold wallets (air-gapped, hardware-secured).
- Conduct comprehensive smart contract audits before deployment.
- Implement multi-signature (multisig) authorisation for large transactions.
- Deploy bug bounty programmes to incentivise responsible disclosure.
- Use timelocks and governance delays for major protocol changes.

B. *For Individual Users*

- Use hardware wallets (Ledger, Trezor) for long-term storage.
- Never share private keys or seed phrases store them offline.
- Enable hardware-based 2FA (YubiKey) rather than SMS-based 2FA.
- Verify smart contract addresses before interacting.
- Be sceptical of unsolicited messages, airdrops, and 'too good to be true' offers.

VII. FUTURE OUTLOOK

The blockchain and cryptocurrency industry continues to mature rapidly. Several key trends are shaping the future of the ecosystem:

Trend	Description
Layer 2 Scaling	Solutions like Ethereum's Optimism, Arbitrum, and zkSync reduce fees and increase throughput by processing transactions off-chain and settling proofs on-chain.
Zero- Knowledge Proofs	ZK-SNARKs and ZK-STARKs enable privacy-preserving transactions and efficient on- chain verification of complex computations.
Real-World Assets (RWA)	Tokenisation of physical assets (real estate, bonds, commodities) on blockchain, enabling fractional ownership and 24/7 global markets.
Institutiona l Adoption	Spot Bitcoin ETFs approved in the US (2024), increasing institutional participation and regulatory clarity.
Regulatory Framework s	MiCA (EU), DORA, and evolving global frameworks are creating clearer rules for crypto businesses and investors.
AI + Blockchain	Integration of AI with blockchain for autonomous smart contracts, on-chain AI agents, and decentralised AI compute markets.

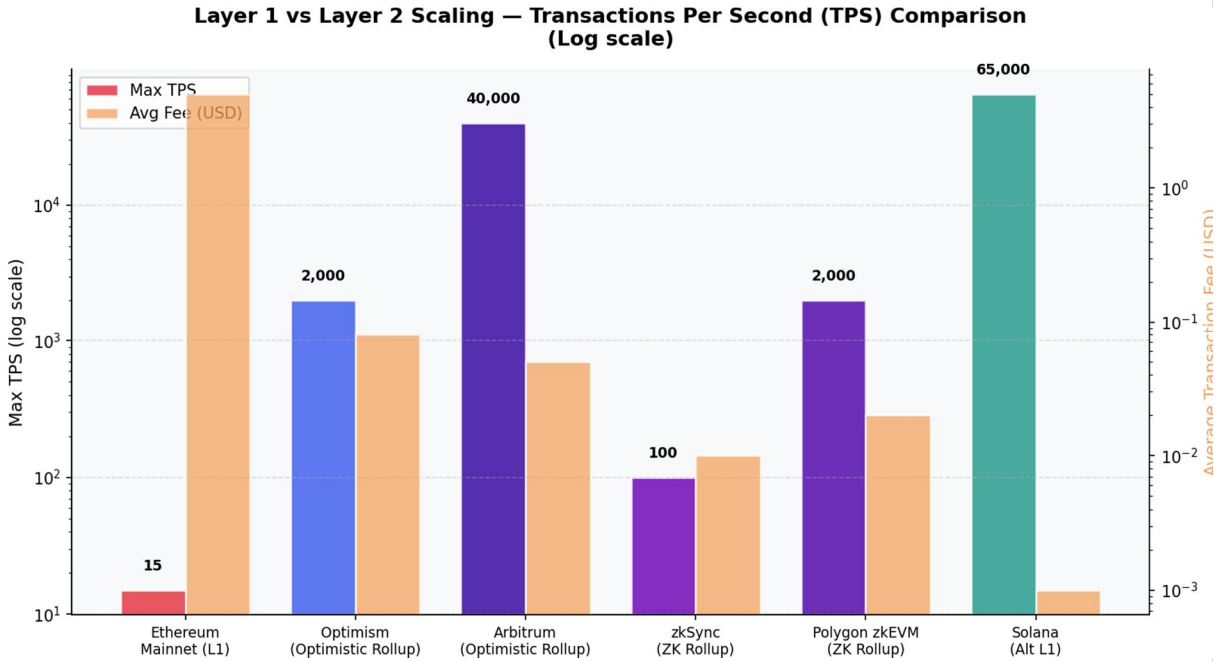


Figure J: Layer 1 vs Layer 2 Scaling TPS & Avg Transaction Fee Comparison (Log Scale)

VIII. CONCLUSION

Blockchain technology and cryptocurrency represent a fundamental shift in how value is stored, transferred, and programmed. From Bitcoin's pioneering peer-to-peer payments to Ethereum's smart contract revolution and the explosive growth of DeFi, the ecosystem has demonstrated both immense potential and significant risks.

The security challenges documented in this paper from exchange hacks and smart contract exploits to state-sponsored attacks underscore the critical importance of rigorous security engineering, comprehensive auditing, and informed user behaviour. The losses sustained, while staggering, have also driven significant improvements in protocol design, multi- layered security architectures, and cross-industry collaboration.

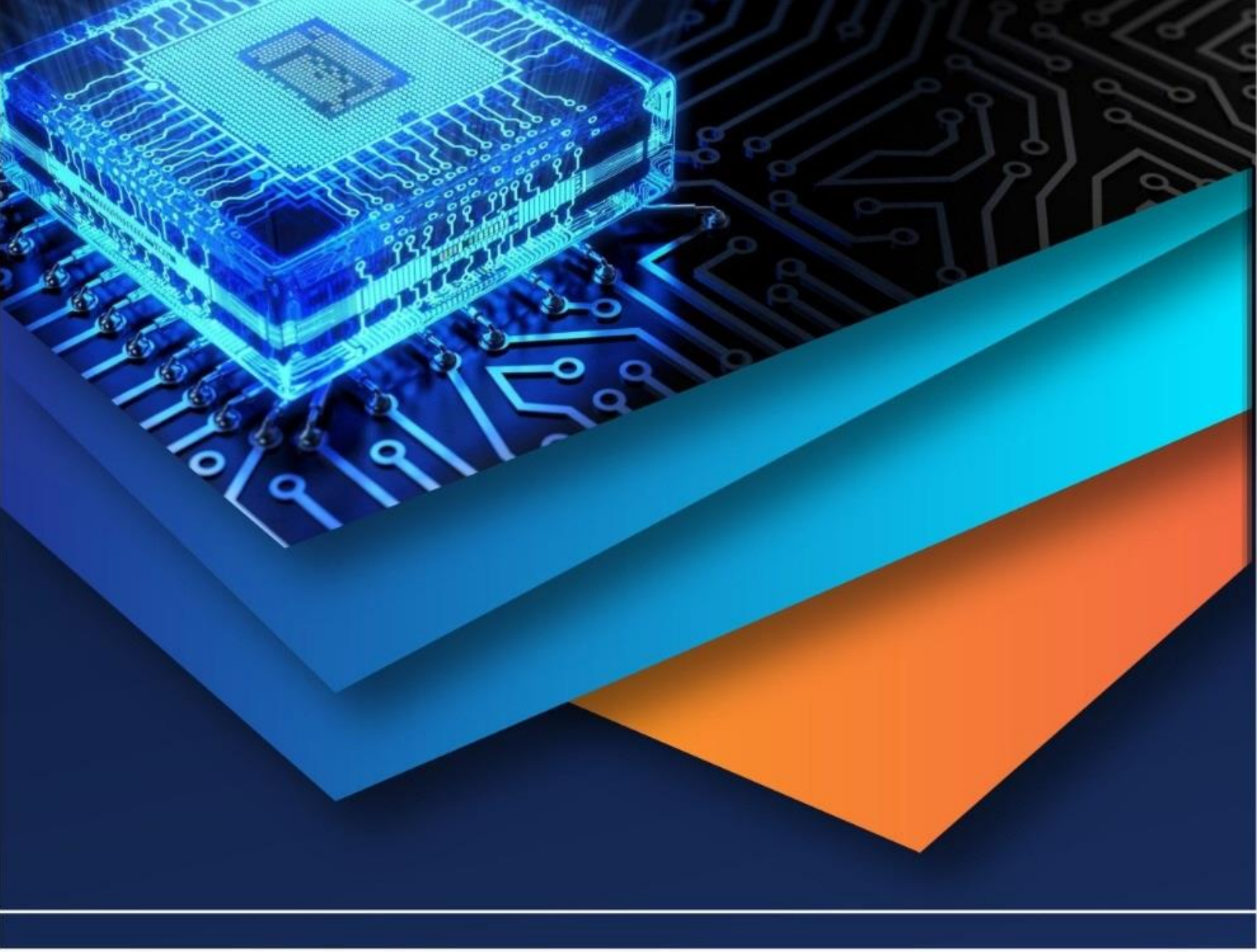
As the industry matures, convergence with regulatory frameworks, institutional finance, and emerging technologies such as zero-knowledge proofs and artificial intelligence is expected to drive the next wave of innovation. The fundamental promise of trustless, permissionless, and programmable finance remains as compelling as ever.

REFERENCES

[1] Nakamoto, S. (2008). Bitcoin: A Peer-to-Peer Electronic Cash System. bitcoin.org
[2] Buterin, V. (2014). Ethereum White Paper. ethereum.org
[3] Chainalysis. (2023). The Chainalysis Crypto Crime Report 2023.
[4] Wood, G. (2014). Ethereum: A Secure Decentralised Generalised Transaction Ledger. Ethereum Foundation.
[5] Bonneau, J. et al. (2015). SoK: Research Perspectives on Bitcoin and Cryptocurrencies. IEEE S&P.
[6] US CISA & FBI (2022). Alert on North Korea's Lazarus Group and Cryptocurrency Theft.
[7] Szabo, N. (1997). Formalizing and Securing Relationships on Public Networks. First Monday.
[8] MiCA Regulation (2023). Markets in Crypto-Assets Regulation. European Union.
[9] Poly Network Post-Mortem (2021). Official blog.medium.com/poly-network
[10] Ronin Network Post-Mortem (2022). Axie Infinity / Sky Mavis Blog.

End of Research Paper

©IJRASET: All Rights are Reserved | SJ Impact Factor 7.538 | ISRA Journal Impact Factor 7.894 |



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Call : 08813907089 (24*7 Support on Whatsapp)