



MONTHLY BULLETIN | 01 OCT 2023

Role of India's **G-20** Presidency In Global Crypto Regulations

- Why is the **G-20**
Declaration Crucial?

- Why is India
Pushing For
Crypto Regulation?








- Highlights
IMF & FSB's
Synthesis Paper



भारत 2023 INDIA



INDEX

	Editorial	02
	Global Market Watch	03
	First Cover Story	11
	Second Cover Story	17
	Rendezvous with Founder	22
	Learn with Gabbar	28
	Gabbar Archive	32

EDITORIAL

As the halving event approaches, the prices of Bitcoin has started to show a stable growth. This is a positive sign along with the fact that the overall valuation of the Crypto Markets has also stabilized.

The bid development in the recent past has been the acceptance of the advisory paper by IMF on Crypto Assets at the G20 forum. This opens the gates for discussion and acceptance. This is a welcome step as the attitude of the Regulators has shifted from Apathetic to Exploratory.

Although the period has been marred by a few crypto hacks but the growth of technology has seen a new dimension with the start of the biggest events of the year in different geographies. While the Korean Blockchain Week and Token 2049 started the crypto season for the South East Asia Region, the Crypto Expo set the stage for the barrage of events coming in the near future.

These events shall surely bring out the best of the development happening in the Web3 space for the world to see. One more benefit of these events has been the shift of inclination from basic Web3 Projects to some deep tech projects which are bent towards solving real life problems.

The coming times are good for the Crypto World as a whole and we can expect a lot of positive changes, both at the policy levels and the standard of projects building up.



Sudeep Saxena

Co-founder at CoinGabbar

GLOBAL MARKET WATCH

"Bitcoin Analysis Based on Daily Chart"



Bitcoin's strong September performance raises October expectations.

BTC exhibited robust momentum over the course of the week, with a notable highlight being its surge to \$27,000 during the last week of September. What stands out is that September witnessed a 4% increase in BTC's price, signifying the first September price uptick since 2016. This positive turn of events brought relief to the digital asset market capitalization, which had experienced two consecutive months of decline in July and August.

Bitcoin is currently at the forefront of this upward trend, as indicated by the Bitcoin dominance metric, which stands at 49.82%, up from 49.18% at the previous Month end. This underscores its relative strength when compared to the broader digital asset market.

However, Despite these promising price movements, trading volumes remain conspicuously subdued. Daily trading volumes on centralized exchanges, measured over a 7-day period, continue to exhibit limited activity, with the total trading volume over the past week hovering at a pproximately \$10.5 billion, closely mirroring the figures recorded seven days prior. On a monthly basis, trading

volumes on centralized exchanges amounted to roughly \$312 billion in September, marking a 26% decrease compared to the \$423 billion observed in August.

Although volatility and trading volume have remained subdued for several months, the next two quarters hold significant promise as potential drivers for the digital asset market, rekindling enthusiasm and trading participation. Importantly, these pivotal events are on the horizon, with the majority of Bitcoin Spot ETF approvals or rejections anticipated by mid-March, closely followed by the scheduled Bitcoin halving in mid-April 2024.

Since the beginning of 2023, BTC has experienced a decrease of approximately 15% from its peak. The largest cryptocurrency by market value is currently trading at around \$26,960. This comes after an impressive 86% surge during the first half of the year, which served as a rebound from the steep 64% decline witnessed in 2022. The digital asset sector had been rocked by scandals and bankruptcies in the preceding year.

Bitcoin has been trading within a narrow range since late in the second quarter, primarily due to uncertainty in the macroeconomic landscape. The Federal Reserve opted to keep interest rates unchanged but signaled a commitment to maintaining higher rates for an extended period. This move has, in turn, reduced the appeal of riskier assets, resulting in a decline in both traditional and digital asset markets. The Federal Reserve's hawkish stance has elevated investor concerns and contributed to these downturns.

From a technical perspective, 2023 has generally been a positive year for Bitcoin. However, the last two months have seen the world's largest cryptocurrency facing losses, leading to growing concerns about a deeper retracement. September, on the other hand, has witnessed a rebound from the significant psychological level of \$25,000, potentially signaling the beginning of an upward trend.

When examining the weekly timeframe, the price action has been turbulent, but the previous week displayed a bullish candlestick pattern. Currently, there is a descending trendline that has acted as resistance, notably around the \$27,800 mark, coinciding with the 20 and 200-day moving averages. A breakout above this descending channel would require clearing the hurdle of the 200-day MA before a potential rally toward the crucial psychological level of \$30,000. If the price manages to surpass \$30,000, it would present a fresh challenge for Bitcoin bulls, who have struggled to maintain momentum above this price level.

Conversely, in the event of a downward move from the current levels, the \$25,000 level would be a significant support level to contend with, with the 50-day MA just below it, roughly around the \$24,400 mark. Below that, there is a notable support area marked at \$22,500, and a breach of this level could potentially lead to a decline toward the lowest point observed in 2022 year-to-date.

Total Crypto Market Capitalization

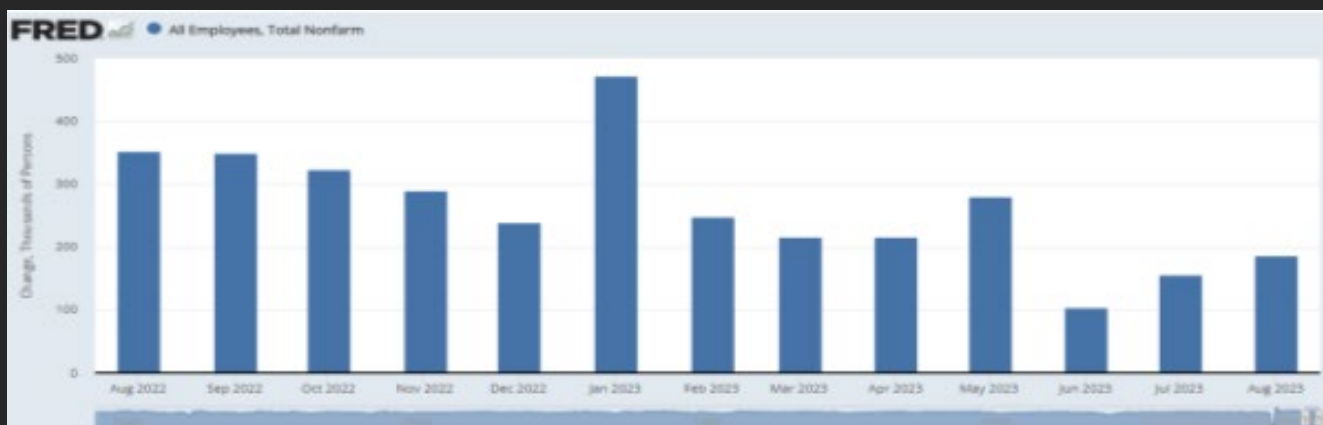


Key Observations

On September 30th, the global cryptocurrency market capitalization stands at \$1.056 trillion, marking a notable shift in market sentiment. Over the last 30 days, the market has witnessed a 2.83% increase. Bitcoin continues to lead the way with a market capitalization of \$527 billion. The overall cryptocurrency market cap has surged, indicating increased buying interest, spurred by Bitwise Asset Management's updated spot Bitcoin (BTC) exchange-traded fund (ETF) application and the imminent trading launch of two Ether (ETH) futures ETFs on October 2nd.

U.S. Non Farm Payroll Data

The Federal Reserve kept rates unchanged in September, but there's uncertainty about a rate hike in November. The Fed's decision had a hawkish bias, with the 2024 Fed funds target rate raised to 5.1%. The strong US economy has pushed rates to their highest levels since 2007. With the US dollar and rates rising, the economy faces risks with further rate hikes. The August payrolls report showed 187k new jobs and a rise in the unemployment rate to 3.8%. Wage growth was softer at 4.3%, which is welcomed by the Federal Reserve. Inflation is picking up, driven by higher fuel prices, which could lead to wage inflation. Expectations for the next report are 155k new jobs and a 3.7% unemployment rate. Watch for signs of wage stickiness, as another strong report could support another rate hike before year-end, especially if core prices and wages remain elevated.



US and China inflation, UK GDP, and Fed minutes

In the coming month, we'll see the release of Fed minutes from the September FOMC meeting, along with a review of US inflation through CPI data. China will also provide updates on factory gate and consumer prices. Meanwhile, the UK and Eurozone will release August GDP and industrial production numbers amid growth concerns. The S&P Global Investment Manager Index, reflecting over \$3.5 trillion in assets, will offer insights into the US equity market.

The US stock market has been affected by concerns about rising interest rates, and the Fed minutes might not offer much relief as investors look for clues about potential rate reductions. Additionally, we await September's CPI data, expected to confirm lingering inflation, reinforcing the Fed's rate-holding stance.

In the UK, August GDP data, sector updates, and a recruitment industry survey will shed light on economic trends. The Eurozone's industrial production data suggests ongoing weakness.

In the APAC region, Singapore's advance GDP figures will provide early insights into Q3 growth, while mainland China's inflation and trade data after the Golden Week holidays will be crucial.

Keep an eye on the S&P Global Investment Manager Index, which reveals money managers' sentiments about the US equity market. Recent surveys have shown a risk-averse attitude and concerns about equity valuations. Allocation preferences among sectors and markets will also be updated this month.

The European Central Bank might find it necessary to increase interest rates once more should factors such as rising wages, increased profits, or supply chain disruptions lead to a surge in inflation. While there has been a recent decrease in inflation, with it hitting its lowest point in two years at 4.3% in September, this development is seen as positive. However, there are still potential risks on the horizon, including the possibility of unexpectedly robust wage and profit increases or new disruptions to the supply chain.

The Bank of Japan's upcoming actions will largely hinge on when it revises its inflation projections for the fiscal years 2024 and 2025. These revisions could occur either in October or next January, during the BOJ's quarterly review of its economic growth and price forecasts.

Global Economic Challenges Persist"

The global economy faced continued challenges in September, as indicated by the latest PMI data. Global output experienced only modest growth for the second consecutive month, signaling a significant slowdown from the earlier robust pace observed earlier this year. It's worth noting that the situation might deteriorate further, as new work inflows to manufacturing and service sector firms declined for the first time since January.



To gain a deeper understanding of the shifts since the promising second quarter, we can delve into the detailed sector-specific PMI data. These data highlight two significant developments.

Firstly, the demand for consumer-oriented services such as travel, tourism, and recreation has stagnated after substantial growth earlier this year. This development is not surprising, as the earlier strong growth was linked to the global economy fully reopening as the last COVID-19 containment measures were lifted. However, the enthusiasm for travel and leisure has waned, overshadowed by increased spending pressures from higher interest rates and the rising cost of living.

Secondly, there has been a marked reversal in demand for financial services, also tied to higher interest rates. Earlier in the year, expectations of a shift in central bank monetary policy had boosted demand for financial services. However, concerns that interest rates may remain elevated for a longer period than initially anticipated have led to a decline in demand for financial services. In September, new orders for financial services decreased for the second consecutive month, primarily driven by sharp declines in banking and real estate. The weakness in the financial sector raises concerns as it often foreshadows broader economic challenges.

Global Economic Challenges Persist"

In recent notable events, cyber-attacks targeted major cryptocurrency platforms, resulting in substantial losses. CoinEx exchange and Stake.com were among the victims, losing \$53 million and \$41 million, respectively.

Attributed to the Lazarus Group, a North Korean hacking collective, these attacks have drawn attention. Presently, the group holds approximately \$45.6 million in cryptocurrency assets, as per the latest data from Dune Analytics.

When considering exploits throughout the year, these incidents have contributed to a staggering total of \$925.4 million in crypto losses. July marked another significant month for exploit losses, with a total of \$285.8 million stolen.

In addition to exploit-related losses, exit scams accounted for \$1.9 million in losses, while flash loan attacks resulted in approximately \$400,000 lost. Phishing attacks further added to the challenges, causing losses totalling \$25 million, according to CertiK.

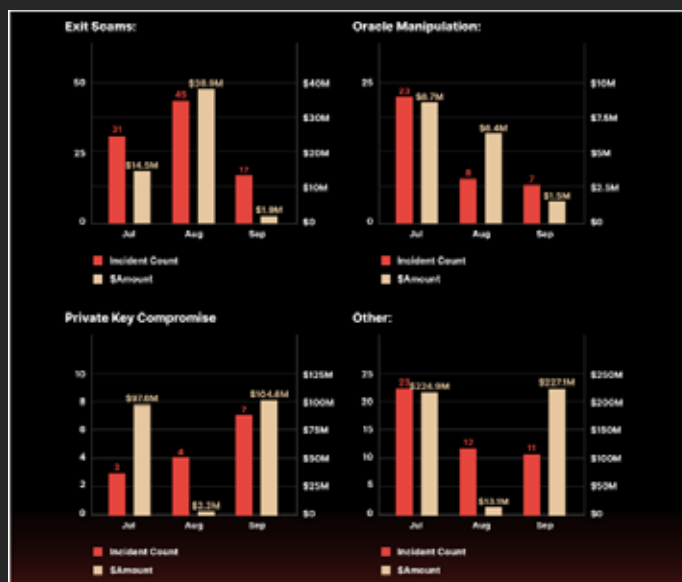
Certik reports \$332 million lost in crypto hacks

CertiK, a leading blockchain security company, has released a report underscoring significant losses totalling \$332 million within the crypto space in September. This underlines the ongoing security challenges prevalent in the crypto ecosystem, including breaches, hacks, and scams, highlighting the necessity for robust security measures.

According to the CertiK report, a majority of the losses, approximately \$329.8 million, were lost due to various crypto-related exploits. Following closely were exit scams, accounting for around \$1.9 million, and flash loans contributing about \$0.4 million. Noteworthy in the report is the severe impact on Mixin Network, a cross-chain transfer protocol based in Hong Kong, which suffered the biggest losses for September, totalling \$200 million.

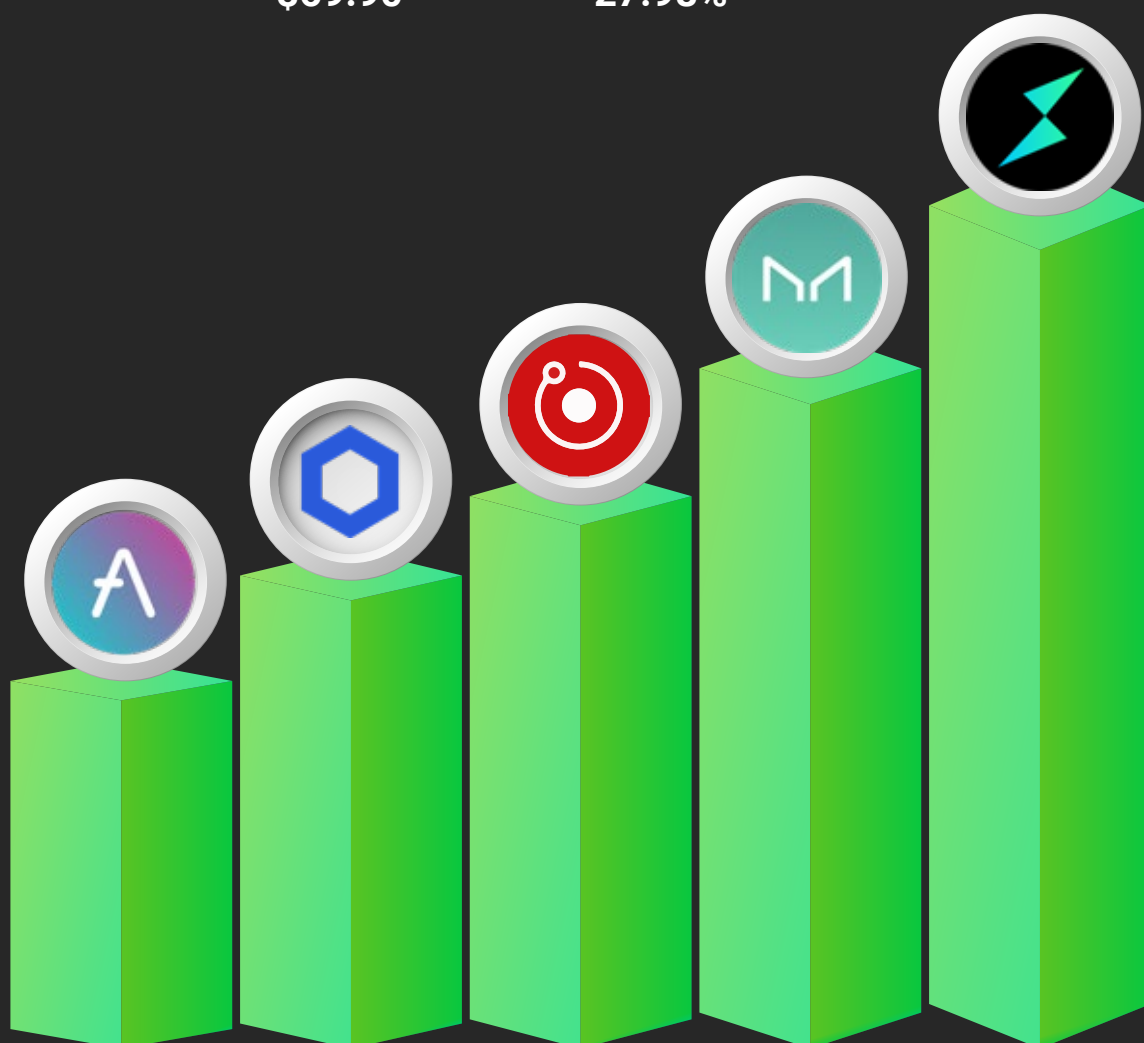
Image credit: Certik

As per the data given above, even though the total number of exit scams and oracle manipulation scams registered a comparative decline, the private key compromises and other scams in the market make September to become one of the most damaging month for crypto in 2023, as labelled by [quillaudits](#).



MONTHLY TOP5 GAINERS

COIN	PRICE	30 ^D %
ThorChain	\$2.05	33.46%
Maker	\$1464	29.70%
Render	\$1.74	29.36%
Chainlink	\$7.68	28.04%
Aave	\$69.90	27.98%



MONTHLY TOP5 LOSERS

COIN	PRICE	30 ^D %
Klaytn	\$0.1142	14.28%
Apecoin	\$1.18	14.18%
XDC Network	\$0.05044	13.95%
Quant	\$88.86	10.59%
Casper	\$0.03224	10.34%



ROLE OF INDIA'S G-20 PRESIDENCY IN GLOBAL CRYPTO REGULATIONS

The last month can be marked as a significant milestone for the crypto industry as the world's leading economies came together on the table to discuss a common framework to regulate virtual digital assets. Under the presidency of India, the Group of 20 Nations, popularly known as G20, discussed and delved deeper into bringing a common consensus on the state of crypto regulations while the industry is facing a dire need for government legitimisation.



This event has brought hope among crypto stakeholders from all around the world that regulating authorities are up for a conversation needed to modulate virtual digital assets. Along the lines of these scenarios, the Government of India is playing a proactive role in shaping this dialogue and bringing key stakeholders to a single table to discuss IMF and FSB's Synthesis Paper and follow the suite of balanced crypto regulations.

This cover story will dive into India's stance and role in driving global crypto regulatory proceedings and pushing the global economies to take the final steps towards building a global consensus on the matter.

Why is the G-20 declaration crucial?

The G-20, in the New Delhi Declaration 2023, underscores the urgency of monitoring the swiftly evolving crypto-asset ecosystem. According to the official documentation shared by the Government of India on behalf of a commonly accepted declaration, G-20 nations including the African Union support the Financial Stability Board's high-level suggestions for supervising crypto-assets and global stablecoin arrangements.

"We welcome the IMF-FSB Synthesis Paper, including a Roadmap, that will support a coordinated and comprehensive policy and regulatory framework taking into account the full range of risks and risks specific to the emerging market and developing economies (EMDEs) and ongoing global implementation of FATF standards to address money laundering and terrorism financing risks," the Delhi Declaration states.

The declaration cites that its focus is on consistent global implementation to thwart regulatory disparities. Acknowledging the IMF-FSB Synthesis Paper and the BIS Report on The Crypto Ecosystem, the G-20 underlines comprehensive regulatory frameworks. According to the report, Finance Ministers and Central Bank Governors plan to delve deeper into the IMF-FSB Roadmap during their upcoming October 2023 meeting in Marrakesh.



Why is India pushing for crypto regulation?

From the Finance Minister to G-20 Sherpa, the commitment to work towards a better-regulated crypto ecosystem is coming all the way from the Government's top brass. These repetitive iterations for global collaborations indicate the government's commitment to push other economies towards a common consensus.

Here are some of the reasons that can be cited as the government's motivation behind this regulatory push:

- To protect investors and consumers. Cryptocurrencies are a new and volatile asset class, and there are many risks associated with investing in them. India wants to ensure that investors and consumers are aware of these risks and have the necessary protections in place.
- To prevent money laundering and terrorist financing. Crypto can be used to anonymously transfer large sums of money, which makes them attractive to criminals.
- To promote financial stability. Cryptocurrencies are not legal tender in India, and they are not regulated by the central bank. India wants to ensure that the growth of cryptocurrencies does not pose a risk to the financial system.
- India is aware that cryptocurrencies are a global phenomenon, and that no single country can regulate them effectively. India wants to work with other G20 countries to develop a coordinated regulatory framework for cryptocurrencies.



Highlights IMF and FSB's synthesis paper

The Indian G20 Presidency requested collaboration between the IMF and FSB to produce a synthesis paper. This document highlights key areas of discussion and offers policy suggestions to help reach a global agreement on regulations and standards. Despite this, the IMF emphasizes that this paper does not introduce new policies or recommendations for its member authorities.

"Widespread adoption of crypto-assets could undermine the effectiveness of monetary policy, circumvent capital flow management measures, exacerbate fiscal risks, divert resources available for financing the real economy, and threaten global financial stability," it says.

The Financial Stability Board (FSB) along with Standard Setting Bodies (SSBs) have created a global framework of recommendations to regulate crypto assets worldwide. Here is a list of the suggestions that the synthesis paper put forward for global leaders to discuss:



- Implement FATF AML/CFT standards for virtual assets and service providers.
- Identify and assess money laundering and terrorist financing risks associated with virtual assets.
- Refer to FATF Guidance for a risk-based approach to virtual assets for effective implementation.
- Follow the FATF's roadmap for accelerated global implementation of AML/CFT controls in the crypto-asset sector.
- Consider additional targeted measures for emerging markets and developing economies based on specific risks.
- Adapt measures to country-specific circumstances and capacity constraints.
- Collaborate with international organizations for coordinated policy response and capacity building in the crypto-asset sector.

Challenges in Regulating Cryptocurrencies

Even though governments from around the world have put in their word that they are committed to working towards regulating cryptocurrencies, doing so is not as easy as it sounds. Blockchain and cryptocurrencies were inherently designed to bypass the central power center and define a new economic order which cannot be regulated by a central authority.

Thus, not only India but almost all countries around the world are struggling to build a mechanism that regulates crypto transactions while ensuring user

security and without curbing industry innovation. Here are some critical challenges in regulating cryptocurrencies;

Decentralized Nature

Cryptocurrencies are not subject to any central authority, such as a government or bank. This makes it difficult for regulators to enforce regulations and to track down criminals.

Global Scale

Cryptocurrencies can be traded and used anywhere in the world. This makes it difficult for regulators to coordinate and develop international regulations.

The rapid pace of Innovation

The cryptocurrency industry is constantly evolving, with new cryptocurrencies and applications being launched all the time. This makes it difficult for regulators to keep up and develop effective regulations.

Lack of Understanding

Many people, including regulators, do not fully understand how cryptocurrencies work. This makes it difficult to develop effective regulations and to educate consumers about the risks of investing in cryptocurrencies.

Commitment to bringing consensus

One can understand the gravity of the commitment the government is presenting on a global stage when the Prime Minister clearly comes forward to address the problems in crypto adoption and calls for its adoption and democratization instead of ignoring it. While talking to a reputed legacy news broadcaster, Prime Minister Narendra Modi explicitly expressed his intent to promote a global unified approach to regulating cryptocurrencies.

"The rapid pace of change of technology is a reality—there is no point in ignoring it or wishing it away. Instead, the focus should be on adoption, democratization and a unified approach," PM Modi told India Today.

On one hand, the government is willing to proceed with regulating crypto assets, it has no intention to self-regulate the growth of decentralized finance within the country while international crypto startups enjoy higher liberty to innovate. The government wants to bring every major stakeholder to one understanding of this intricate technology and formulate equal global regulations.

"There is a challenge associated with cryptocurrencies. In this matter maximum integrated approach is needed. I think there is a need for preparing a global framework which should take care of the interests of all stakeholders," the prime minister said while addressing the Business-20 (B20) meeting.

7 DEADLY SINS OF CRYPTO SECURITY

&

**CAPITAL VIRTUES
TO FIGHT THEM BACK**



Investing in crypto has become a mandate among those investors who want to diversify from their traditional investments while also reaping the benefits of a volatile market that has a record of major upswings. But many crypto investors even after investing substantial sums in crypto tokens do not take their security seriously, making them vulnerable to many potential crypto scams.

Most crypto users do not foray into barricading their crypto storages because they find it too technical or something their exchanges are obliged to do for them. However, trusting your crypto security with anyone else is as good as having zero control over it.

If that makes you anxious and you want to upgrade your crypto wallet security, follow this dummies' guide to understand what are the things you should avoid and some practices that you must embrace to secure your crypto.

Crypto hackers are smarter than you

Amid all the crypto chaos that we come across, one thing is crystal clear: crypto hackers are often a step ahead. Armed with sophisticated techniques, they continuously find ways to exploit vulnerabilities in wallets and exchanges. They prey on the overconfidence of individuals and organizations who believe their assets are secure.

Hackers exploit human errors, such as weak passwords and phishing susceptibility, and technical loopholes to gain unauthorized access to crypto assets. The anonymity and irreversible nature of blockchain transactions further embolden their malicious intents. Staying vigilant, continuously updating security measures, and educating oneself about the latest security threats are crucial to safeguarding one's assets in this digital age.



Take out time for your money before they do

Weekdays are filled up with important tasks that you have to undertake and weekends are piled up with your plans to live this one life that you have got. Who has time for the boring part where you will have to sit down and get your hands dirty in upgrading your password security, choosing better password managers, upgrading to 2-factor authentications and switching to a cold wallet?

This is all the boring stuff but remember - these are the only things that will save your funds on a rainy day.

7 Deadly Sins in Securing Your Crypto Assets

Even though there are hundreds of things that you should avoid while venturing through the decentralized financial space but following are some of the most basic and most deadly sins that you can commit while securing your crypto assets.

Sloth (Neglecting Crypto Security)

Updating your wallet software and security protocols will take so much time. You do not need to change passwords every month. Hot wallets are fine as shifting to a cold wallet is another unpleasant task. If these are your thoughts about your own crypto security, you might be under the influence of sloth and trust us, you have to get over it as soon as possible.

Pride (Overconfidence in Personal Security)

Overconfidence can lead to neglecting basic security measures. Even the most tech-savvy individuals can fall victim to sophisticated hacking techniques. So know that - you are never secure enough to stop taking care of the good practices while using any crypto products.

Envy (Using Shoddy Apps)

Crypto is not a get-rich-quick scheme and getting envious of others' gains can lead to rash decisions, like using unverified third-party services or platforms which might be insecure or fraudulent. Know your game, and trust in long-term investing. Do not let envy drive your decisions and do proper research before investing.

Wrath (Let Your Emotions Win)

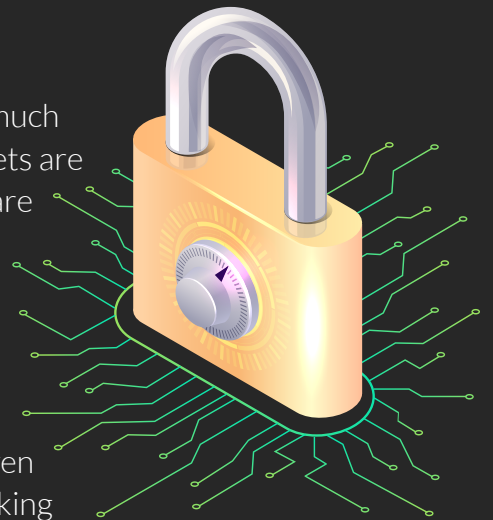
It is easy for you to let your emotions take the driving seat when things are not going right. Most of the time investors can be really frustrated with the volatility of the market and take impulsive decisions. If you are an informed investor, ensure that you are not making decisions based on your emotions but on your strategy.

Lust (Chasing Too Good To Be True Offers)

The desire for quick, easy gains can lead to falling for scams and phishing schemes. Always do thorough research and maintain skepticism towards offers that seem too good to be true.

Gluttony (Overloading Single Wallets)

Most crypto users never feel the need to diversify other than their main crypto wallet despite having substantial holdings. You should know that storing all your assets in one wallet is risky. Distribute your assets across different wallets to minimize the impact in case one gets compromised.



Greed (Following Mob Mentality)

Greed is a well-known driving force in any trading market, so much so that it is even the sole reason for a majority of crypto investments around the world. However, being greedy when everyone is greedy can hardly be stated as a good investment strategy. According to market experts, being greedy when the market is in the fear zone is fair enough but following the mob mentality is never a great idea.

7 Capital Virtues in Securing Your Crypto Assets

In contrast to the "7 Deadly Sins" for securing crypto assets, here are the "7 Capital Virtues" to secure your crypto assets, each one countering a corresponding sin:

Diligence (Maintaining Better Security)

Counteract Sloth by regularly updating your wallet software and security protocols. Stay informed about the latest security advancements and apply them to safeguard your assets and never let the sloth overshadow your intention to secure your assets.

Humility (Acknowledging Security Limits)

You have to sideline your pride for your own security by acknowledging that no one is immune to security breaches. Continuously educate yourself about the latest security threats and solutions while continuously upgrading your security measures.

Kindness (Choosing Vetted Services)

Take all the time you need and patiently research to find well-reviewed and reliable third-party services and platforms to transact cryptocurrencies. Take recommendations from trusted sources and ensure the security of the platforms you use. Be kind to yourself and do not lose your money just because of carelessness.

Patience (Regular Backups)

Agree or not, it is true that nobody really likes to keep waiting while your system gets properly backed up but if you are someone who can wait patiently to regularly back up your wallet's private keys and other crucial information, it will be hard for destiny to make you lose your crypto. So always store backups in multiple secure, offline locations and be patient with your investments.

Chastity (Avoiding Scams)

Counteract your lust for get-rich-quick schemes by avoiding the allure of too-good-to-be-true offers. Practice discernment and skepticism, and prioritize security over potential gains. Stay loyal to your investment strategy and never lose your integrity for short-term gains.

Temperance (Distributing Assets)

Act against gluttony by putting in some effort and not keeping all your eggs in one single basket. Distribute your assets across different wallets and use cold storage for significant amounts to minimize risks. Fat wallets are only comfortable for the thieves who will steal them.

Charity (Give before you take)

Always be ready to give and feed your crypto investments with adequate time, patience, knowledge, and research before you start expecting returns from them. You will have to put in effort and water your crypto investments slowly over time to make them grow piece by piece.

By embracing these virtues, you can significantly enhance the security of your crypto assets and protect them against various threats and vulnerabilities.

RENDEZVOUS WITH FOUNDER



PREETAM RAO

CEO of QuillAudit

Q. How does a smart contract audit contribute to the security of cryptocurrency transactions?

So, when we talk about the auditing process, it's all about taking a really close look at the code, the logic, and the overall structure of these smart contracts. It involves going through the code line by line manually, and we also use specialized tools for automated testing. What we're aiming for here is to make sure that these smart contracts meet the highest security standards and follow the best coding practices out there. This way, we ensure that cryptocurrency transactions happen in a safe and reliable environment.

Q. What is the primary purpose of a smart contract audit in cryptocurrency?

The purpose of conducting audits is to find and resolve any security issues that might be hiding in the smart contract code. By doing this, we make sure that crypto protocols are as secure and dependable as possible. This, in turn, improves the user's trust in the protocol and provides a safer space for them to carry out their crypto transactions

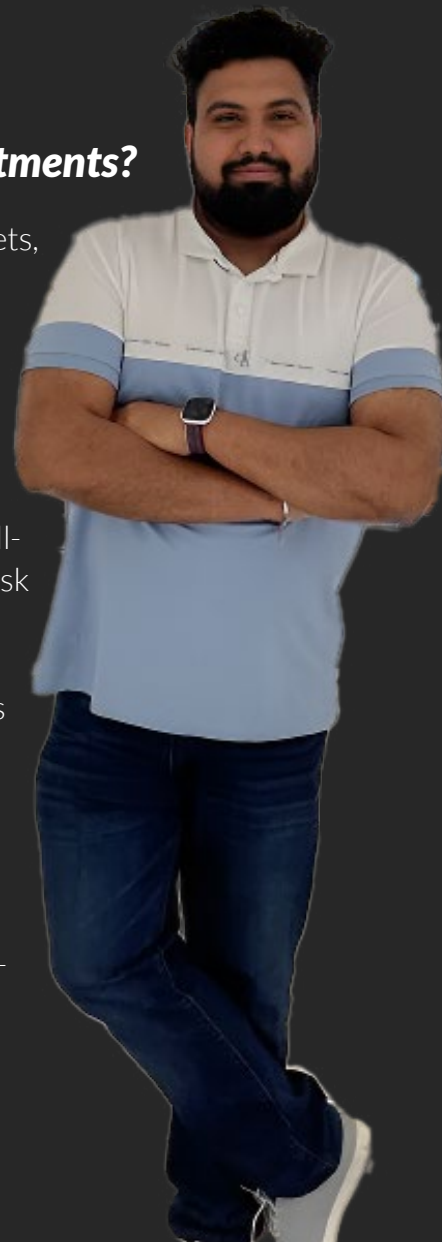
Q. What key security measures should individuals and organisations take to protect their cryptocurrency investments?

To point out some key security measures, I'd suggest using cold storage wallets, robust encryption methods, two-factor authentication (2FA), creating secure backups of wallet and account information, and, most importantly, safeguarding private keys.

But even before investing in crypto/DeFi tokens, it's crucial to look out for the project's code, token background, its market and social media score, etc. To make this process more manageable, you can leverage tools like Quill-Check, which puts the token through a series of security tests and gives a risk score right away based on the findings.

To stay committed to the security of your investments, you can set up alerts for your invested projects in QuillMonitor. So, if there's any hint of suspicious activity or unusual transactions, QuillMonitor promptly sends you an alert with which you can safeguard your assets at the earliest signs of trouble.

So, remember, while crypto investments offer exciting opportunities, proactive security measures and the right tools are always important to sail the dynamic sphere with confidence and peace of mind.



Q. What is a smart contract audit, and why is it important in the world of cryptocurrency?

A smart contract audit has one primary goal: to identify and fix possible security vulnerabilities and risks. This is crucial because it ensures that transactions carried out through smart contracts are secure and reliable. Through audits, we maintain the utmost standards of security, reducing the chances of bugs, vulnerabilities, and potential breaches.

Q. Why are audit services vital in blockchain?

Audit services are indispensable for several compelling reasons. Let me point them out. Firstly, they help in identifying and mitigating security vulnerabilities. Secondly, audit services enhance trust and reliability on the blockchain, assuring users that their transactions are secure. Additionally, they protect users' assets and investments from potential breaches. In essence, audit services provide an essential layer of security and assurance for both users and organizations.

Q. Can you explain the process of how a smart contract audit works?

Absolutely, I'd be glad to share the whole process of how we go about auditing a smart contract.

- The first step is the Specification Gathering, and this is where it all begins. We gather all the information to understand the smart contract and its intended behaviour clearly, which serves much like a blueprint for the audit.
- Followed by a manual review, where our auditors read through the contract's code line by line to ensure that every detail in the specifications is actually implemented in the smart contract.
- On completing the manual review, we put the contract to the test by deploying it on a test network. Here, every transaction is carefully recorded and closely observed for gas consumption and how the functions behave.
- Next up is functional testing, where we deploy the contracts in a controlled environment and test their functions under various conditions.



- Once the manual part is done, we utilize automated tools to catch things we humans might miss. Tools like Slither, Mythril, and others to perform additional checks and catch any bugs that might be hiding.
- After all the testing and reviewing, if we find any vulnerabilities, we give them in the initial audit report and also outline steps to address them.
- After addressing those identified issues in the initial audit, we repeat the process to ensure everything is ship-shape and then goes the final audit report.
- So, in a nutshell, a smart contract audit is like a thorough health check for the project's code, and we rectify any discrepancies present.

Q. What types of vulnerabilities or issues can a smart contract audit help identify?

A smart contract audit is instrumental in identifying a wide range of vulnerabilities that could compromise the security of cryptocurrency transactions. It may include reentrancy attacks, oracle manipulation issues, Gas griefing, transaction order dependence (frontrunning), force-feeding attacks, timestamp dependence, and denial of service (DoS) attacks, to name a few.

For complete coverage, here we maintain a repository of all the web3 attack vectors for anyone to explore, click on the link below.

★ **Solidity Smart Contract Attack Vectors**

★ **DeFi Attack Vectors**

★ **NFT Attack Vectors**

Q. Explain the role of KYC in financial due diligence.

"KYC, or 'Know Your Customer,' is a process used by financial institutions, including crypto exchanges, to confirm customer identities and understand their business. The goal is to assess risks and prevent misuse, like money laundering. KYC safeguards financial integrity and minimizes illicit activity risks.

Q. Why is due diligence important in cryptocurrency investments?

When it comes to cryptocurrency investments, conducting thorough due diligence is absolutely important. Why? Because the crypto market is extremely volatile, understanding the risks associated with different digital assets is essential. Plus, the speed and anonymity of crypto transactions can attract malicious actors for illicit purposes like money laundering. By doing your homework, you make informed choices. It's all about staying smart and secure in this fast-paced crypto landscape

Q. What is the goal of technical due diligence for technology investments?

Technical due diligence is all about assessing the tech side. It's like peeking under the hood to spot any red flags that could affect your investment. We're talking about vulnerabilities, scalability, and whether it plays by the rules of the crypto game. It's about making smart investment moves by knowing the tech inside out.

Q. Name three key security measures for protecting cryptocurrency investments.

Technical due diligence is all about assessing the tech side. It's like peeking under the hood to spot any red flags that could affect your investment. We're talking about vulnerabilities, scalability, and whether it plays by the rules of the crypto game. It's about making smart investment moves by knowing the tech inside out.

Q. What type of information should be stored securely in cryptocurrency hardware wallets?

Cryptocurrency hardware wallets provide secure storage for sensitive data like private keys and recovery seeds. Private keys authorize transactions, while the recovery seed helps regain access in case of loss or theft. Always safeguard these credentials using hardware wallets to protect your crypto assets.

Q. What is the importance of using a secure internet connection for crypto transactions?

Using a secure internet connection for cryptocurrency transactions is crucial to prevent potential security breaches. Public Wi-Fi networks and unsecured connections can expose your sensitive data to hackers and eavesdroppers. A secure internet connection, preferably through a trusted VPN, encrypts your data and shields it from potential threats.



Q. What are the key types of audits commonly conducted in the blockchain and cryptocurrency world?

We can categorize them into two based on who performs the audit. Generally, the first type is internal audits, where our in-house team members conduct audits, and the other is external audits, in which outside parties engage in auditing contracts

Q. Why is two-factor authentication (2FA) important for cryptocurrency accounts?

I'd say two-factor authentication (2FA) is necessary for cryptocurrency accounts because it adds an extra layer of security beyond just a password. This additional step helps protect accounts from unauthorized access, even if an attacker manages to obtain the password. It significantly enhances the security of cryptocurrency holdings, reducing the risk of unauthorized transactions or account breaches.

Q. How can individuals protect themselves from phishing scams in the crypto space?

To shield yourself from phishing scams, always double-check URLs and verify the authenticity of websites or emails. Don't click on suspicious links, and never share your private keys or personal information. Use hardware wallets for added security, and keep your software up-to-date to patch potential vulnerabilities. Trust your instincts – if something feels off, it probably is.

Q. What is your overall experience of the Industry as a whole?

My overall experience in the industry has been quite enlightening. We've seen remarkable growth and innovation, but security remains a critical concern. While strides have been made, there's still work to be done to ensure the industry heads in the right direction regarding project security. I feel constant vigilance and proactive measures are essential.

Q. In your opinion, is the Industry going in the right direction as far as security of the Projects is concerned?

There's a growing awareness of the importance of security audits and best practices. However, given the evolving nature of technology and threats, there's always room for improvement. Continued collaboration and innovation will be key to staying ahead in the security game.

Q. How do you see the Web3 Industry placing itself in the coming 5 years?

I envision the Web3 industry flourishing over the next five years. With the global Web3 market projected to soar to over USD 44.2 billion by 2031 at a CAGR of 44.13%, we can expect significant advancements. We anticipate blockchain, decentralized apps (Dapps), and NFTs will see more mainstream adoption. Web3 will reshape finance, gaming, art, and beyond. It's an exciting time for innovation and decentralization.

GABBAR ARCHIVE



Investor Mark Cuban loses \$870K in Hot Wallet Hack

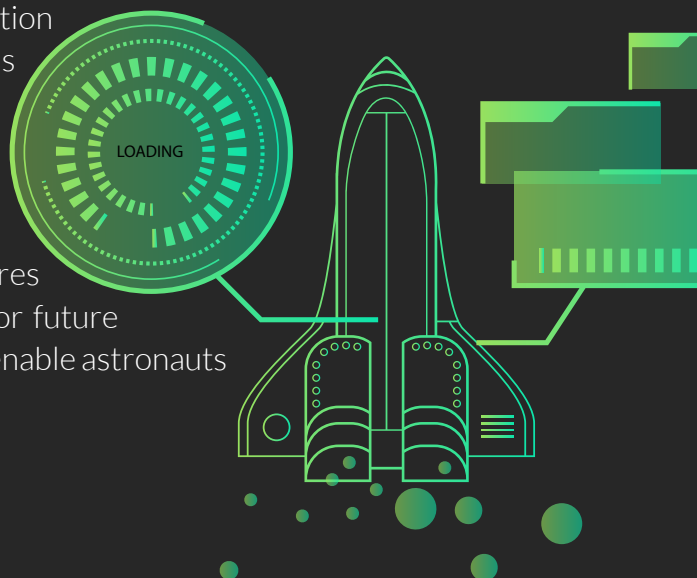
Billionaire investor and Dallas Mavericks owner Mark Cuban fell victim to a cryptocurrency hack, resulting in the theft of nearly \$900,000 worth of digital assets. The breach was first detected by blockchain investigator Wazz on September 15, who noticed unusual activity in one of Cuban's wallets. A significant amount of assets, including USD Coin Ether and Lido Staked Ether (stETH), was swiftly withdrawn within a short time-frame. Cuban later confirmed the hack, suggesting that the attackers had been monitoring his wallet for the right moment. As a precaution, he moved his remaining assets to Coinbase custody. This incident adds to Cuban's prior crypto-related setbacks, including losses in an algorithmic stablecoin project in June 2021.



NASA Plans to Verify Lunar Landings Using Blockchain

NASA is partnering with Lonestar, a Florida-based computing startup, and the Isle of Man to send data cubes to the Moon in February 2024, with plans to use blockchain technology for data verification upon their return to Earth. This venture is part of NASA's Artemis missions, with Artemis 2 launching in November 2024 as a precursor to Artemis 3, which aims to return humans to the lunar surface.

The blockchain-based data verification process ensures data integrity, making it tamper-proof and accessible for future Moon missions. This innovative use of blockchain could enable astronauts to verify lunar activities during future lunar landings.



Binance CEO CZ Denies Rumors Financial Troubles and Turnover



Binance CEO CZ Zhao has refuted rumors surrounding the company's financial health and internal turmoil, affirming the safety of customer funds and smooth operations. Amid regulatory and internal issues, including the resignation of 10 executives and regulatory obstacles in Australia and Germany, CZ remains optimistic. He highlights positive industry developments, such as new fiat options, product launches, hires, and legal wins for Ripple and Grayscale. Critics point to these challenges as signs of deeper troubles, but CZ attributes them to common employee turnover in the dynamic crypto sector, asserting Binance's financial strength and workforce resilience amid adversity.

Brazilian Crypto Streamer Loses \$60K Due to Reveal Private Keys

A prominent Brazilian cryptocurrency streamer, "CryptoKing," recently experienced a substantial loss of \$60,000 in digital assets after accidentally disclosing his private keys during a livestream tutorial on wallet security. Despite efforts to transfer the assets to a new wallet, viewers quickly exploited the error, draining the wallet. This incident underscores the critical importance of safeguarding private keys in the cryptocurrency realm. Unlike traditional banking systems, cryptocurrencies use irreversible blockchain technology, making transactions permanent. Cybersecurity experts emphasize the need for robust security measures when dealing with digital assets, comparing private keys to keys for one's home – not to be shared carelessly.

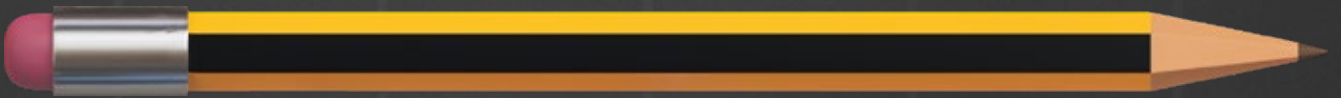


Alibaba Releases a More Advanced AI System Than ChatGPT

Starting from September 13, Alibaba's Tongyi Qianwen, a large language model similar to ChatGPT, has become available to the general public and businesses in China. While specific details about its parameters remain undisclosed, early reports suggest it may be trained with 10 trillion parameters, surpassing OpenAI's GPT-4 by tenfold. This release coincided with China's relaxation of artificial intelligence (AI) technology regulations, mandating special testing and certification for all publicly released AI models. This move follows similar efforts by other Chinese tech giants like Baidu, Tencent, TikTok, and ByteDance to launch AI models in compliance with the new rules, while global discussions on AI regulation continue.



LEARN WITH GABBAR



What are Smart Contracts in Blockchain?

With the advent of Blockchain, we have seen several innovations out of the old traditional manner of doing things due to its unique features. Smart Contracts emerged as the most appealing among these novel properties, as they enable the transfer of anything on a blockchain. They opened up previously untapped potential and developed assets like money programmable and DApps. Their applications have grown to the point that they now control billions of dollars.

Let's take a detailed look at how they work and their features.

What is a Smart Contract?

A smart contract is a secure code that executes on a blockchain network when certain predefined conditions are met. They are automated applications or lines of code that operate on a decentralized system such as a blockchain. This code controls the execution of irreversible and trackable transactions.

They enable trustworthy agreements and transactions to be carried out between different anonymous parties without the requirement of a legal system, or central authority. They let developers create apps that use blockchain security, dependability, and accessibility while providing complex peer-to-peer functionality ranging from banking to logistics and trade.

It is similar to a traditional contract in terms of laying out the conditions of an arrangement. However, the terms of a smart contract are performed as code running on a blockchain such as Ethereum. Technically, it can also be called an Ethereum account, which has a balance and can also send transactions over the network.

Smart contracts are replicated on each node of the blockchain network to avoid contract manipulation. Human error might be eliminated by allowing machines to execute tasks and using services supplied by blockchain platforms to prevent conflicts over such contracts.



Features of a Smart Contract

■ No Need for an Intermediary

They enabled users to codify their agreements and trust relationships by allowing automated transactions to take place without the oversight of a central authority. The elimination of a trusted third party will reduce the transaction costs and authority imposed by them.

The autonomous execution of tasks, depending on the situation, increases the efficiency of a system without any human actions or biased actions. As a result, smart contracts are a viable option for most applications that demand alternatives without the involvement of trusted third parties.

■ Transparency

It is one of the key differentiating characteristics acquired by smart contracts from the blockchain. The smart contract is transparent in two ways. Firstly, the code stated in smart contracts is transparent to both intervening parties and the general public. Secondly, the set of transactions included in the blocks is likewise visible to the general public

As a result, the blockchain network's intervening parties may trust the logic and transactions in the blockchain network. Centralized databases are likewise at risk. It is also hard to determine whether any changes were made to the data at rest. Transparency of smart contract code guarantees that participants in the blockchain ecosystem are publicly visible and ensures that they are executed correctly.

■ Security

Digital signatures are used to validate the integrity of distributed ledger transaction records. Individual transactions were also inspected and authorized before being added to the ledger. The ledger is made up of immutable authorized transactions. An individual cannot be committed to the modification. An immutable smart contract code is put on the blockchain.

However, smart contracts can only be changed if all of the nodes in the blockchain agree. This implies that all blockchain network participants can trust the smart contract and believe that the executed code contains the logic given and agreed upon by each blockchain network participant. It can be read by anyone but can only be changed by the developer or creator.

Features of a Smart Contract

■ No Need for an Intermediary

They enabled users to codify their agreements and trust relationships by allowing automated transactions to take place without the oversight of a central authority. The elimination of a trusted third party will reduce the transaction costs and authority imposed by them.

The autonomous execution of tasks, depending on the situation, increases the efficiency of a system without any human actions or biased actions. As a result, smart contracts are a viable option for most applications that demand alternatives without the involvement of trusted third parties.

■ Transparency

It is one of the key differentiating characteristics acquired by smart contracts from the blockchain. The smart contract is transparent in two ways. Firstly, the code stated in smart contracts is transparent to both intervening parties and the general public. Secondly, the set of transactions included in the blocks is likewise visible to the general public.

As a result, the blockchain network's intervening parties may trust the logic and transactions in the blockchain network. Centralized databases are likewise at risk. It is also hard to determine whether any changes were made to the data at rest. Transparency of smart contract code guarantees that participants in the blockchain ecosystem are publicly visible and ensures that they are executed correctly.

■ Flexibility

The flexibility to readily amend contract terms saves parties' expense on contract drafting and renegotiation. Anyway, smart contracts are distributed infrastructure programs that are designed to automate predefined processes based on transparent and trusted data sources. Implying that smart contracts are not flexible in the usual sense. Their flexibility is built into the coding and the way they are employed in the Smart Legal Contract's contract text.

Smart contracts can improve the drafting phase by removing ambiguities, inconsistencies, and redundancies that are the source of litigation. It is simple to get more clarity in knowing the full agreement, duties, and obligations. Furthermore, when the requirements indicated in the code are met, particular actions are automatically triggered: actions that no longer rely on the parties' subjective (and arbitrary) volition, but on objective and confirmed aspects.

However, their flexibility is conditional! It indicates that they conduct a procedure and then apply a new pattern/rule based on the information received (input data). Smart contracts cannot address such problems of flexibility, but they can assist in detecting them and eliminating gaps.

Smart contracts are definitely way ahead of traditional contracts due to their variety of benefits, including speed, efficiency, accuracy, trust, transparency, security, and cost savings. They automate operations by using computer protocols, saving hours in many business procedures.

How Does Smart Contracts Work?

Smart contracts are written in many programming languages (including Solidity, Vyper, and Michelson). Each smart contract's code is kept on the Ethereum network's blockchain, allowing any interested participant to view the contract's code and current state to verify its functionality. In addition to the blockchain and transaction data, each computer on the network (or "node") holds a copy of all existing smart contracts and their current state.

Smart-Contract

This figure depicts key stages in the setup and transaction processing of blockchain-based smart contracts. The first step is to initialise smart contracts. The smart contract must be placed on the network once the terms and conditions have been defined as a software program. To ensure fairness and to meet the primary criteria of blockchain-based smart contracts, the smart contract implemented in each node is identical in all respects.

Transactions are received by the blockchain network from the interfacing apps(APIs). After the transaction is received by the blockchain network, it is checked for numerous requirements. The digital signature is required to verify that the transaction is valid and was initiated by the real network member. Furthermore, certain blockchain networks include platform-specific inspections.

In this stage, the platform checks for double-spending. When a transaction is determined to be valid, it is flagged as verified and the smart contract is executed. A mining node adds the transaction to the block, and the finished block is formed. The verified block is subsequently distributed throughout the network and approved by every node based on the pre-defined consensus rule. The block is attached to the blockchain after the consensus requirement is fulfilled.

Based on their underlying mechanism, a smart contract is most typically a class consisting of state variables, functions, function modifiers, events, and structures that are designed to execute and control important events and activities per the contract rules. It can also call for other smart contracts to be executed (contracts can also deploy other contracts).

Every smart contract has states and functionalities. States are variables that contain data or the wallet address of the owner, i.e., the addresses in which the smart contract is deployed. While functionalities are chunks of code that have the ability to read or alter states. Once the smart contract has been deployed and the returned parameters (e.g., contract address) have been received, users can call any accessible smart contract function by sending a transaction, and a unique hash is generated after every transaction.

History of Smart Contracts

It's quite surprising that the concept of smart contracts emerged in the 1990s, long before Ethereum was created. At that time, Nick Szabo proposed the word "smart contracts," referring to "a set of promises, stated in digital form, including protocols within which the parties fulfil these promises."

The term was first used in 1998 to identify objects in the rights management service layer of the system The Stanford Infobus, which was part of the Stanford Digital Library Project. They are often compared to vending machines. Vending machines allow a seller to provide a product to a consumer without the requirement for an actual human to collect the money and hand over the item. Smart contracts provide the same function but are far more adaptable.

Smart contracts have come a long way in recent years. They began as basic if-then expressions that any programmer could construct and execute. One of the biggest leaps in smart contract history is the development of Ethereum. Users were able to join the public Ethereum blockchain and deploy smart contract apps on the public blockchain.

It's not that only Ethereum can use smart contracts, many other networks, including Bitcoin (BTC), also use them. Every BTC transaction is a simplified version of a smart contract, and layer-two solutions like the lightning network have been created to increase the network's capability. However, Ethereum's usage of smart contracts is an exception.

Unlike other blockchain networks, which are defined as distributed ledgers, Ethereum is a distributed state machine that includes the Ethereum Virtual Machine (EVM). This machine state, which all Ethereum nodes agree to retain a copy of, contains smart contract code as well as the regulations that these contracts must follow.

Advantages of Smart Contracts

Smart contracts offer several advantages, which is why they have gained popularity in blockchain and decentralized application (DApp) development. Some of the key advantages of smart contracts include:

- **Trust:** Smart contracts are self-executing and self-enforcing, meaning they automatically execute and enforce the terms of an agreement without the need for intermediaries. This reduces the need to trust a central authority or third party, enhancing trust in transactions.
- **Security:** Smart contracts are tamper-resistant and secure by design, as they are stored on a blockchain, which is known for its robust security features. Once deployed, it's extremely difficult to alter or manipulate a smart contract's code or its execution.
- **Transparency:** All actions and transactions within a smart contract are recorded on a public blockchain ledger, making them transparent and auditable by anyone. This transparency reduces the risk of fraud and ensures accountability.
- **Efficiency:** Smart contracts automate processes, eliminating the need for manual intervention and paperwork. This leads to increased operational efficiency and cost savings, as intermediaries and administrative tasks are reduced or eliminated.
- **Cost Savings:** By removing intermediaries and automating processes, smart contracts can significantly reduce transaction costs. This is particularly beneficial in financial, legal, and supply chain industries.
- **Speed:** Smart contracts execute automatically when predefined conditions are met, eliminating the time delays associated with traditional contract execution and settlement. This can lead to faster transaction times.
- **Accuracy:** Automation reduces the risk of human error in contract execution and calculations. Smart contracts precisely follow the coded logic, ensuring accurate outcomes.
- **Global Reach:** Smart contracts are not bound by geographical restrictions. They can be accessed and executed from anywhere with an internet connection, making them suitable for international transactions.

- **Immutable Record:** Once a smart contract is deployed on a blockchain, its code and transaction history are immutable, meaning they cannot be altered or deleted. This creates a permanent and verifiable record of all interactions.
- **Innovation:** Smart contracts enable developers to create decentralized applications (DApps) and innovative solutions in various fields, such as decentralized finance (DeFi), supply chain management, and more.
- **Reduced Fraud:** The transparency and security of blockchain-based smart contracts make it difficult for parties to engage in fraudulent activities, reducing the risk of scams and disputes.

Common Smart Contract Default Remedies

In a smart contract context, remedies in case of default are typically automated and self-executing, as they are coded into the smart contract itself. The specific remedies available in a smart contract depend on the design and programming of the contract. Here are some common remedies that can be implemented in smart contracts to address default:

- **Automated Penalties:** Smart contracts can include programmed penalties that are automatically enforced in the event of a default. For example, if one party fails to make a payment on time, the smart contract can deduct a predefined penalty amount from their account.
- **Liquidation or Collateral Seizure:** In decentralized finance (DeFi) applications, if a borrower defaults on a loan, the smart contract can automatically liquidate the borrower's collateral to repay the lender.
- **Escrow and Mediation:** Some smart contracts include dispute resolution mechanisms where funds are held in escrow until certain conditions are met. In the case of a dispute, a mediator can be appointed to make a decision, and the smart contract will execute based on that decision.
- **Termination of the Contract:** Smart contracts can include provisions that allow the innocent party to terminate the contract in case of default. This can trigger the release of any remaining funds or assets held in the contract.
- **Automatic Refunds:** If a product or service is not delivered as agreed upon in the contract, the smart contract can automatically trigger a refund to the party who did not receive what was promised.
- **Blockchain Governance:** In some blockchain networks with governance tokens, token holders may vote to decide on remedies for defaults or breaches in decentralized applications. This can include changes to the smart contract's code or other actions to address the issue.

In a smart contract context, remedies in case of default are typically automated and self-executing, as they are coded into the smart contract itself. The specific remedies available in a smart contract depend on the design and programming of the contract. Here are some common remedies that can be implemented in smart contracts to address default:



COIN GABBAR