Cryptocurrencies for Investors

Their Valuation and the Potential Scams

Jacques R. Island
Jovana DesGouttes

October 31, 2025

THIS PAGE IS INTENTIONALLY BLANK

Table of Contents

THIS PAGE IS INTENTIONALLY BLANK

Executive Summary

Cryptocurrencies are a double-edged sword: a genuine technological innovation built on distributed trust, but operating in a largely opaque environment that makes it unusually fertile ground for fraud. The value of crypto is driven less by sovereign backing and more by a mix of scarcity, utility, adoption, speculation, trust, and regulation—factors that can amplify gains but also fuel volatile boom-and-bust cycles. From there, we demystify how tokens are created and why "mining" is not a hobbyist gimmick but an industrial operation with significant hardware, energy, cybersecurity, and compliance burdens. Here we compare major consensus models—Proof of Work (energy-intensive but widely viewed as robust), Proof of Stake (lower energy, validator staking incentives), and Delegated Proof of Stake (faster throughput via elected delegates, but with governance still in private hands).

The core practical value of this paper is its scam taxonomy and its emphasis on the "insider threat" as the primary mode of attack. It illustrates how fraudsters recycle classic schemes using crypto jargon and staged technical "proof":

- **Fake mining companies** that show glossy dashboards and staged server footage while operating as Ponzi structures (case study 1);
- **Community/faith-based Ponzi schemes** that weaponize trust networks and social recruitment (case study 2);
- **Hosting/cloud-mining betrayals** where the victim believes they control rigs but the host silently redirects mining proceeds using "dashboard theater" and wallet misdirection (case study 3); and
- **Pump-and-dump/rug-pull tokens** driven by viral hype and code-based selling restrictions (case study 4).

Across these cases, the warning pattern is consistent: impressive interfaces, high promised yields, and social proof substitute for verifiable ownership, auditable output, and transparent operations.

The paper closes with a practical, due-diligence checklist aimed at investors: verify corporate legitimacy and physical presence, demand transparency and audits of mining output and costs, assess security controls (MFA, encryption, cold storage, audits/pen tests), evaluate customer support credibility, and stay current on evolving scam patterns. And it highlights an often-missed point: cybersecurity hygiene helps against outsiders, but the bigger risk in many mining arrangements is the **insider threat** posed by the host itself—so investors should avoid relinquishing control, maintain ownership documentation, build an audit trail, and conduct periodic (including unannounced) inspections where possible.

The overarching conclusion is blunt: crypto can be legitimate, but investors should treat mining and "too-easy" yield claims as high-risk propositions requiring industrial-grade verification and ongoing oversight.

Cryptocurrencies for Investors

Their Valuation and the Potential Scams

In 2011, inside a small Berlin café, two patrons made history by "buying" two cups of coffee for 0.01 Bitcoin—worth only a few U.S. cents at the time. The barista humored them and laughed at the idea of paying for coffee with invisible money mined from computers. Yet that moment would later symbolize a seismic shift: the beginning of the cryptocurrency era. Just two years later, on a sunlit beach in the Philippines, a self-styled entrepreneur pitched investors on "golden rigs" that would mine Bitcoin around the clock. Weeks after they wired their money the website vanished along with their savings. These twin stories—one of innovation, the other of deception—capture the dual nature of cryptocurrency: promise and peril.

"The issue with crypto currencies is that they are created not by governments with underlying economies but by thousands of private entrepreneurs" [worldwide].

What determines what particular "coins" can substitute today's "legal tender" is public acceptance and use. Just as some government-issued currencies have little value outside their borders, so are some currencies considered as good as "gold" everywhere because of the strength and trust behind the governments that issue them. Take, for instance, the value and utility of two current examples: the Iranian Rial, and the U.S. dollar. The Rial is all but useless outside of Iran, although it is what Iranians must use to carry on their daily lives. On the other hand, the U.S. dollar is the "international" standard—accepted and sought after everywhere in the world because of the stability and strength of the issuing country's economy. Cryptocurrencies are built on this trust, though in an unregulated and often opaque environment that leaves investors exposed to risks.

The issue with crypto currencies is that they are created not by governments with underlying economies but by thousands of private entrepreneurs. Crypto currencies are, instead, "mined" by these entrepreneurs by converting the output of specialized computer banks, and the energy needed to run them, into virtual "tokens." And their value is determined by many factors other than a government's assurances. So, if not government backing, what truly assures the value of these digital tokens—other than the collective belief that others will continue to accept them? What tangible economic mechanisms do private entities have at their disposal to establish and stabilize cryptocurrency value? And can a decentralized network of

independent enterprises genuinely self-regulate and enforce trustworthy standards across such a volatile marketplace?

People who want to join the cryptocurrency revolution need to know how crypto coins are created, their trustworthiness and utility, what potential value they hold into the future, and—very importantly—how to avoid the many fraudulent schemes that now exist at all levels of governments and economies.

What Makes Cryptocurrencies Valuable?

Cryptocurrency value depends on confidence and six intertwined factors: scarcity, utility, community adoption, speculation, trust, and regulation (Antonopoulos and Harding 44). Bitcoin, for example, has a limited supply of 21 million coins, giving it gold-like scarcity. Ethereum's value, in contrast, stems from its utility—fueling smart contracts[1] and decentralized apps.

Community adoption acts as a multiplier: the more users and developers join, the more valuable and secure the network becomes. But speculation—driven by hype and fear—often overshadows fundamentals. As journalist Nathaniel Popper observed, Bitcoin's boom-and-bust cycles mirror "the mania of gold rushes past" (Popper 218). Regulation, meanwhile, can stabilize or shake prices; the stronger the oversight, the more legitimacy a coin may gain.

The Ways to "Mint" Crypto Tokens

Crypto miners work to create valuable tokens through substantially different processes; but the different methods of production carry different costs in equipment and energy consumption. The process involves validating and adding new transactions to a blockchain, a decentralized ledger that records all transactions.

Different methods achieve different levels of integrity. Some cryptocurrencies, like Bitcoin, use proof-of-work mining, while others use alternative consensus mechanisms such as proof-of-stake or delegated proof-of-stake. These three methods are discussed below.

[1] A *smart contract* is a self-executing computer program stored on a blockchain that automatically enforces the terms of an agreement once specific conditions are met. In effect, it functions like a digital vending machine: when the right inputs are provided, it automatically delivers the agreed outcome without the need for intermediaries.

Proof-of-Work Mining

In proof-of-work (PoW), the more traditional form of mining, powerful computers compete to solve complex mathematical problems, and the first miner to solve the problem is rewarded with newly created coins. This process requires significant computational power and energy consumption but, it is, still, considered the most trustworthy method of crypto mining despite its production costs.

Proof-of-Stake Mining

Proof-of-stake (PoS) mining uses a "consensus" mechanism in blockchain networks to validate and add new blocks to the blockchain.

Unlike PoW mining that requires miners to solve complex mathematical puzzles, in the PoS mining process, block "validators" are chosen to create new blocks based on the number of cryptocurrency tokens they already hold and are willing to "stake" as collateral. The higher the stake, the higher the chances of being selected as a validator. This eliminates the need for the resource-intensive mining hardware and electricity consumption associated with PoW mining.

Figure 1: Source Freepik.com

The selection of validators is usually determined by an algorithm that considers various factors, including the number of tokens held and the length of time they have been held (known as "coin age"). Validators are then responsible for creating new blocks, validating transactions, and securing the network.

In some PoS systems, validators can be punished or have their stakes slashed if they act maliciously or attempt to validate invalid transactions.

Proof-of-Stake mining offers several advantages over Proof-of-Work. It typically consumes significantly less energy, making it more environmentally friendly. It also reduces the risk of a 51% attack, where a single entity or group of entities controls the majority of the network's mining power.

Additionally, PoS mining allows token holders to earn rewards for staking their tokens and participating in the network's consensus process. These rewards are typically distributed proportionally to the number of tokens staked by each validator.

Delegated Proof-of-Stake Mining

Delegated Proof-of-Stake (DPoS) is a consensus mechanism that builds upon the basic principles of PoS mining. DPoS introduces the concept of delegates, or witnesses, who are responsible for validating transactions and creating new blocks on behalf of token holders in a blockchain network.

In a DPoS system, token holders vote to select a limited number of delegates from a pool of candidates. These delegates are trusted individuals or entities who have the authority to produce blocks and maintain the network's consensus. The number of delegates can vary depending on the specific blockchain implementation.

Once the delegates are elected, they take turns in a round-robin fashion to create blocks. The order in which they create blocks is typically determined by the number of votes received during the election process. Delegates are incentivized to act in the best interest of the network since their reputation and future chances of being elected depend on their performance.

Delegated Proof-of-Stake offers several benefits. It allows for faster block confirmation times compared to other consensus mechanisms, as the number of delegates responsible for block creation is limited. This can result in higher transaction throughput and improved scalability. DPoS also enhances network security by eliminating the need for every token holder to participate in block validation, reducing the risk of centralization.

What DPoS does is add a layer of oversight to the creation of new crypto coins (tokens), but the oversight in still in private hands with stakes in the process. This mining process would carry more value and trust if the delegates were neutral regulators from a trusted government.

The Complexity and Cost of Producing Cryptocurrencies

Producing cryptocurrency isn't as simple as running code—it's a global industrial operation that blends engineering, economics, and risk. Modern mining farms fill warehouses in Iceland, Texas, and Kazakhstan, with computer racks that glow like small suns. Energy consumption is massive; Bitcoin mining alone uses more electricity each year than Argentina (Cambridge Centre for Alternative Finance).

Beyond hardware costs, miners face steep technical demands. Successful mining requires mastery of cryptography, programming, and network management. Security flaws can lead to multimillion-dollar losses—as in 2014 when the Mt. Gox exchange lost 850,000

Figure 2: Illustration of cryptocurrency mining rigs. Image generated by freepik.com using AI.

Bitcoins due to a vulnerability. And legal compliance adds more weight: governments increasingly require miners to follow anti-money-laundering (AML) and know-your-customer (KYC) laws.

Even for legitimate ventures, scalability and sustainability are ongoing struggles. Profit margins fluctuate with coin prices and electricity rates. Miners often form pools to share resources and smooth income volatility, transforming cryptocurrency mining into a high-risk, low-margin business.

The Machinery of Cryptocurrency Production

A cryptocurrency mining rig looks more like a server rack than a hole in the ground to extract gold or other precious metals; they are banks of motherboards, graphics cards (GPUs), application-specific integrated circuits (ASICs), power supply units (PSUs), and cooling systems, crunching equations continuously, day and night. Each machine validates transactions and adds them to an immutable digital ledger known as the blockchain.[2]

[2] A *blockchain* is a shared, tamper-resistant database run by many independent computers. It stores data in time-stamped "blocks," each block pointing to the previous one with a cryptographic fingerprint (a hash, see next footnote). New blocks are added only after the network reaches *consensus* (e.g., proof-of-work or proof-of-stake), making the record *append-only*,

When a new block is created, miners run a "hashing"[3] function—a mathematical operation that transforms transaction data into a fixed-length code, like a fingerprint. The block is accepted by the network, and added to the chain, only if this code meets precise conditions.

Mining can look to an outsider like and endless stream of code across screens. But for crypto miners, each successful hash means income. The process is competitive, automated, and relentless—machines run 24/7, monitored for temperature and efficiency. Overheating, software bugs, or cyberattacks can mean instant losses.

Another thing a mining machine needs is software—an operating system, typically Microsoft Windows or Linux—and specialized mining software compatible with the specific cryptocurrency being mined. The mining software connects the machine to the mining network and coordinates the mining process.

Because of the complexity of mining, some miners choose to pool into "collectives" to pool their resources where they combine their computing power to collectively, more efficiently, mine cryptocurrencies. Pooling increases their chances of earning individual rewards more frequently, and the rewards are shared among the members.

Sourcing Mining Machines

If cryptocurrency mining were the modern-day gold rush, then the mining rig is the digital prospector's pickaxe. But as in the 19th-century gold fields, not every pickaxe is forged equal—and not every seller is trustworthy. The market for crypto-mining hardware has exploded into a global trade stretching from Shenzhen to Seattle, drawing in professional miners, hobbyists, and opportunists alike.

The Main Sources

Sources for mining rigs vary widely in reliability and risk. The typical ways to acquire—or seek to acquire—them, are these:

transparent, and extremely hard to rewrite. Many blockchains can also run small programs called smart contracts (see previous footnote) that automatically execute rules when conditions are met.

[3] A *hash* (or *hashing*) is a cryptographic one-way function that maps data of any size to a fixed-length digest: the same input always yields the same digest, tiny input changes produce an unpredictably different digest (avalanche effect), and recovering the original data or finding two different inputs with the same digest is *computationally infeasible*. Systems may retain the data alongside a hash, or store only the hash and later verify by recomputing and comparing digests. In blockchains, coin value is recorded as explicit numeric amounts in transactions; hashes do not encode value. Hashes secure value by serving as tamper-evident identifiers for transactions and blocks and by cryptographically chaining blocks, so any alteration changes the hashes and fails validation under the network's consensus rules—protecting balances and preventing double-spends.

Manufacturer direct sellers are major players like Bitmain, Canaan, and MicroBT who sell rigs directly through their official websites, offering everything from industrial-grade ASIC units designed for Bitcoin to lower-powered models for alternative coins. Buying direct gives miners some assurance that their machine is genuine, though even these manufacturers have faced counterfeiting and supply-chain scams too.

Online marketplaces include websites like Amazon, eBay, and Alibaba, and are littered with listings for "high-yield" miners, often at suspiciously attractive prices. The convenience of one-click ordering hides a darker reality: counterfeit hardware, dead-on-arrival units, or sellers that vanish once payment clears. The credibility of a seller should be verified by checking independent reviews, warranty coverage, and return policies. These can make the difference between running a profitable rig and owning an expensive paperweight.

> *"Even if [investors] avoid [costly mining rig]…scams… investors…face…the next frontier of risk: the* human element *… [f]raudsters [who] exploit the technical ignorance of investors…."*

Specialized retailers are companies that focus exclusively on mining hardware. They maintain online stores or even physical shops, sourcing rigs from multiple manufacturers. These retailers often provide setup support or bulk pricing, but investors should confirm that the shop is an authorized distributor, not a middleman reselling refurbished or obsolete models at new-equipment prices.

Secondhand markets are secondary sellers in an industry that moves fast and in which a cutting-edge rig can become obsolete quickly. Used mining machines flood secondary markets whenever prices fall or mining rewards shrink. On forums and Telegram groups, used ASICs can sell for a fraction of their original cost, but the savings come with risk. Burned-out chips, tampered firmware, or power supplies on the brink of failure are common hazards. Buyers will be smart to request serial numbers, performance logs, and clear photos *before* transferring funds.

The True Cost of a Mining Rig

Even if you avoid the scams, buying a mining machine is a gamble. Prices swing with the cryptocurrency market, power costs, and technological leaps in chip efficiency. A single high-end Bitcoin rig can cost anywhere from $2,000 to over $10,000, and that's before accounting for electricity, cooling, and hosting space. Three major factors drive the economics:

Type of cryptocurrency, that is, the type of tokens being mined will affect cost; for example, Bitcoin mining demands specialized ASIC

hardware and vast energy consumption, while other coins may be mined with less power-hungry GPUs.

Performance specifications, like the "hash rate"—the rig's computational output—determines how fast it can solve cryptographic puzzles and earn rewards. Higher hash rates bring higher costs, both in dollars and electricity.

Market demand influences equipment prices. When Bitcoin's price surges, demand for rigs skyrockets and manufacturers can't keep up. Prices soar, scalpers appear, and even outdated models get snatched up by speculators hoping for one last profitable run.

For all the hype, successful mining requires an industrial mindset: calculating *return on investment (ROI)* beyond the initial sticker price. Factors from the ongoing burn rate of electricity, cooling, maintenance, and market volatility need to be factored in. As one industry veteran put it, *"Mining isn't a get-rich-quick scheme—it's an arms race with physics and finance."*

From Hardware to Hustle

Once investors grasp the realities of mining, they face the next frontier of risk: the *human element*. Fraudsters exploit the technical ignorance of investors by selling "cloud mining" contracts that promise steady payouts without owning a rig at all. Many of these programs—like HashFlare and other so-called mining hosts—turn out to be elaborate Ponzi schemes.

Understanding how mining machines are sourced and valued is the first safeguard. The next, as we explore in the following section, is recognizing the mining opportunities that are too good to be true—and the scams that hide behind them.

Potential Scams Targeting Crypto Mining Investors

As cryptocurrencies gained popularity, fraudsters adapted old schemes to new technology. The scams targeting crypto mining investors blend technical deception with social manipulation. The most common types include fake mining companies, Ponzi schemes, hidden-mining betrayals, and pump-and-dump tokens.

Case studies offer the best ways to illustrate the kinds of schemes cryptocurrency investors need to be wary of. Knowing that fraudsters are constantly evolving and adapting and may well present new

variations of the examples we show here, an informed investor should be able to spot new fraudulent schemes.

Case study 1: The BitClub Network — A "Fake Mining Company" Masquerade

Between 2014 and 2019, the founders of the BitClub Network pitched a compelling dream to investors worldwide: buy "shares" in their massive Bitcoin-mining pools and receive steady profits as the computers generated new coins. Their website displayed gleaming rows of servers and professional charts tracking supposed production. Early investors received payouts, encouraging them to recruit others. What few realized was that the entire operation was smoke and mirrors.

Figure 3: Promotional frame from a BitClub Network video showing server banks purportedly used for cryptocurrency mining, later identified as a cryptocurrency Ponzi scheme. Screenshot from YouTube (accessed October 30, 2025).

Federal prosecutors later revealed that BitClub's operators were fabricating numbers and had no meaningful mining activity behind the scenes. Over five years they siphoned more than $722 million from investors who believed they owned real mining hardware. One of the programmers admitted that BitClub's promoters even joked internally that they were "building this whole model on the backs of idiots."

When the scheme finally collapsed in 2019, the FBI described it as a high-tech Ponzi that "used Bitcoin's mystique to disguise one of the oldest scams in the book." Forensic analysis showed that investors' deposits were simply redistributed to earlier participants, while the supposed "rigs" shown in online videos were staged props or third-party footage.

BitClub exemplifies the fake mining company: professional websites, virtual "data centers," and glossy marketing meant to appear technical — yet no true mining ever occurs, only illusion and circular money flows. (ABC News.)

Case Study 2: NovaTech Ltd. and AWS Mining — A Faith-Based Ponzi Scheme

Beginning in 2019, two intertwined companies, NovaTech Ltd. and AWS Mining Pty Ltd., cultivated trust inside immigrant and religious communities, especially among Haitian-Americans. Their founders, Cynthia and Eddy Petion, marketed themselves as devout Christians bringing "God-given opportunities" in cryptocurrency. Investors were told their funds would be used to purchase mining rigs and engage in foreign-exchange trading that yielded weekly profits.

Figure 4: Promotional frame from a NovaTech Ltd Trading video advertising a market-trading strategy claimed to achieve win rates of 85–90 percent. Screenshot from YouTube (accessed October 30, 2025).

Social-media videos showed racks of computers and dashboards with green profit bars climbing each week. Participants were urged to recruit friends and family — "bring others to the blessing," one promoter said in Creole. By 2022 NovaTech claimed over 200,000 members and boasted of risk-free earnings of 15 to 20 percent per month. But behind the scenes, there were no functioning mines and little trading at all. The SEC later charged the companies with misappropriating more than $650 million.

When withdrawals suddenly froze in mid-2023, panicked investors flooded online forums demanding answers. NovaTech's leaders blamed "system upgrades" and even circulated a story about a "data-center fire." Investigators would later call it staged theater

designed to buy time. As one victim told Reuters, "They used our faith against us — they prayed with us while stealing from us." (Reuters.)

The NovaTech case demonstrates how Ponzi mining schemes prey on community trust, religious networks, and the promise of effortless prosperity — using crypto jargon and fabricated mining operations as modern camouflage.

Case Study 3: The Hidden Mining and Hosting Betrayal — When Control Is an Illusion

A subtler and more technical deception comes from "hosting" and "cloud-mining" arrangements — in which the victim believes they own a mining rig or a portion of a mining facility operated remotely by a professional host. A recent investigation by cybersecurity firms uncovered multiple cases where the host appeared legitimate but quietly redirected mining output to wallets under its own control.

The way this works, as happened to a tech-savvy investor who was new to crypto-mining, is that the victim pays thousands of dollars for a mining rig or "virtual machine" and is then given access to an online dashboard that displays the machine's temperature, hash rate, uptime, and the daily amount of coins it is supposedly mining. Everything looks normal. But what the investor doesn't see is that the rig — whether physical or virtual — is configured to deposit its earnings not into the investor's digital wallet, but into a wallet secretly owned by the host. The host might show a partial "credit" to the investor's dashboard to maintain credibility, but the real coins are being deposited elsewhere. (*Cryptocurrency Mining Fraud* 2023.)

Figure 5: Illustration of a cryptocurrency mining host presenting to a remote customer his alleged profitable mining performance metrics. Image generated by freepik.com using artificial intelligence (AI).

In another real-world example, hackers exploited misconfigured cloud servers at Tesla and several smaller firms, installing mining software that silently generated Monero cryptocurrency for the attackers. Tesla's engineers only discovered the breach when their internal power bills spiked abnormally. Another case involved

criminals hijacking clients' Amazon Web Services (AWS) accounts and running unauthorized mining programs, charging the unsuspecting users for enormous computing bills while diverting the coins. (Centre for Cybersecurity.)

The genius — and cruelty — of these hidden-mining betrayals lies in their invisibility. Victims often see a convincing online interface proving their rigs are "running," yet all real control resides with the fraudster in an undisclosed location. By the time the deception is uncovered, the mined currency has already been transferred through multiple anonymous wallets and is virtually unrecoverable.

Case Study 4: The Squid Game Token — A Modern Pump-and-Dump Frenzy

In October 2021, an anonymous team of developers launched the Squid Game Token (SQUID), claiming it was tied to a forthcoming play-to-earn video game inspired by the hit Netflix series. The website showcased slick graphics, celebrity tweets, and a presale countdown that fueled a speculative stampede. The token's value exploded from less than one cent to over $2,800 within days.

Thousands of small investors, fearing they'd "miss the next Bitcoin," rushed to buy in. But when they tried to sell, they discovered the contract code itself prevented selling — only the creators could withdraw. Minutes later, the developers drained the liquidity pool and vanished, making off with roughly $3.3 million. The token's price collapsed to nearly zero in under ten minutes.

Image generated by freepik.com using AI.

The Squid Game debacle became one of the most infamous pump-and-dump token scams in crypto history, illustrating how viral marketing and pop-culture references can be weaponized to drive investment mania. As blockchain analysts later noted, more than 90 percent of new tokens created that month showed similar "rug-pull" characteristics.

For many observers, the SQUID scam is a parable of the crypto age: in markets driven by memes and emotion, hype can mint millions — but often only for the people who planned the exit in advance. (Bloomberg Crypto.)

Protecting Against Scams

While scams in the world of cryptocurrency mining can be disheartening, there are steps investors can take to protect themselves:

1. **Do Your Due Diligence**: Always research and verify the legitimacy of a mining operation, its ownership, and its history prior to making any investments. Look for proper licensing, transparency, and reviews from reputable sources.
    - Research the Company: Start by researching the mining company thoroughly. Look for information about their background, team members, and track record in the industry. Check if they have a physical address, company registration, and any certifications or credentials that validate their credibility.
    - Online Presence and Reputation: Evaluate the company's online presence. Check their website, social media profiles, and forums to gather insights about their reputation within the cryptocurrency community. Look for customer reviews, complaints, or any red flags that might indicate fraudulent activities or poor business practices.

Figure 7: Source freepik.com.

    - Transparency and Account Audits: Legitimate mining companies often provide regular audits and transparency regarding their mining operations. Look for evidence of regular reporting of mining outputs, hardware setups, and electricity costs. This information should be publicly available, and any reluctance to provide these details could be a warning sign.
    - Mining Facility and Equipment: Verify whether the company owns or operates a mining facility. Request proof, such as photos or videos, of their hardware setups, mining farms, or data centers. Reliable companies are transparent about their infrastructure and readily provide evidence to substantiate their claims.
    - Legal Compliance: Ensure the mining company complies with relevant regulations and licensing requirements. Look for evidence of licensing, permits, or compliance with industry standards. Lack of proper legal compliance is a clear warning sign of a potential scam.
    - Reputation and Trustworthiness: Consult reputable cryptocurrency publications, forums, and communities to gauge the general sentiment and reputation of the mining

company. Engage in discussions with experienced users who have dealt with the company before, and seek their opinions and firsthand experiences.

- Check Security Measures: Investigate the company's security measures and protocols. Look for two-factor authentication, encryption, and secure storage of the cryptocurrencies mined. Companies that prioritize security demonstrate their commitment to protecting their clients' investments.
- Customer Support and Communication: Reach out to the company's customer support to evaluate their responsiveness and professionalism. Prompt and helpful responses indicate a company's commitment to its customers, while evasive or inconsistent answers should raise concerns.

Above all, remember that due diligence is an ongoing process, and it is essential to adapt these steps based on the specific circumstances and changing market dynamics. By conducting thorough research and being careful with your investments, you can significantly reduce the risk of falling prey to cryptocurrency mining scams.

2. **Use secure platforms**: Use only trusted, reputable platforms for your mining activities that have robust security measures and adhere to industry regulations. This is no simple task but essential for an individual contemplating a significant investment of money.

Figure 8: Source freepik.com.

- Compliance and regulation: Ensure the platform complies with relevant legal and regulatory frameworks. Look for information about licenses, permits, or registrations that authenticate their operations. Platforms that adhere to regulatory requirements typically prioritize security measures to protect investors.
- Encryption and data protection: Verify that the platform implements robust encryption protocols to safeguard user data and communications. Secure Socket Layer (SSL) encryption is a minimum requirement. Additionally, inquire about their data storage practices and whether they follow industry-standard security measures, such as firewalls and intrusion detection systems.
- Multi-Factor Authentication (MFA): A reputable platform will offer MFA as an additional layer of security. This feature requires users to provide multiple forms of identification during the login process, reducing the risk of unauthorized access to accounts.

- Cold storage and wallet security: Inquire about the platform's storage practices for cryptocurrencies. Look for information about cold storage solutions, which keep a majority of funds offline in secure hardware wallets. This approach minimizes the risk of hacking and protects against online vulnerabilities.
- Penetration testing and security audits: Ask if the platform has undergone independent security audits and penetration testing by reputable third-party firms. Such assessments evaluate the platform's vulnerabilities and measure the effectiveness of their security protocols. Reports from these audits are a strong indicator of a platform's commitment to security.
- Bug bounty programs: Consider whether the platform has a bug bounty program, where they incentivize ethical hackers to identify and report security vulnerabilities. This practice demonstrates the platform's proactive approach to security and their willingness to address any potential weaknesses.
- Insurance coverage: Inquire if the platform provides insurance coverage for any losses due to security breaches or hacking incidents. While not all platforms offer this, having insurance coverage can provide an additional layer of protection and instill confidence in the platform's commitment to security.
- Transparent security disclosure: Trustworthy platforms are open about their security measures and procedures. They should have a clear and detailed security policy available to users. Review this policy to understand how the platform protects against various security threats and how they respond to security incidents.
- Reputation and user feedback: Research the platform's reputation within the cryptocurrency community. Look for user reviews and feedback regarding their experience with security features and practices. Engage in discussions on reputable forums to gain insights from other investors regarding the platform's security track record.

Figure 9: Source freepik.com.

By carefully assessing these key factors, investors can gain confidence in a crypto mining host's security measures and make informed investment decisions while minimizing the risks associated with potential security breaches.

3. **Keep current**: Stay updated on the latest scams and frauds prevalent in the industry. Knowledge is the best defense against scams. This really needs no further explanation other than to say that scammers are like viruses: always adapting to

countermeasures and morphing into new threats that victims may not recognize.

4. **Practice cybersecurity**: Prioritize the use of strong, unique passwords, enable two-factor authentication, and invest in quality antivirus software to protect against potential hacking attacks.

    - Cybersecurity protective measures aim to thwart external attacks against an investor's operation, but it does little to protect against the **insider threat** that may be posed by the crypto mining host itself.

    - To protect against an insider threat, do not relinquish control of the crypto mining process. Investors that do, should take these steps:
    - Physically inspect and register equipment serial numbers
    - Take possession of sale receipts that attest to ownership
    - Execute a clear agreement about the host's responsibilities
    - Ensure the agreement shows the investor owns the output
    - Check and verify the identity of the seller or host principal
    - Create an audit trail system that tracks machine activity
    - Establish periodic (and unscheduled) audits of the operation
    - "Trust but verify, Verify, VERIFY"!

      In short, assure you can periodically physically inspect the mining machines and audit their output to prevent skimming (or outright theft) by the host. Investors who rely on video calls and "show and tells" for auditing can be easily scammed. Even physical audits can be corrupted by devious hosts, but investors are much less likely to be victimized when they actively monitor their operation.

Figure 10: Source ChatGPT AI.

If Investing in Cryptocurrencies

Cryptocurrency remains both a technological marvel and a magnet for fraud. Understanding mining's mechanics helps investors distinguish legitimate innovation from illusion. By studying past scams and verifying every promise, investors can protect themselves in an industry where transparency is both the greatest strength and weakest link.

Bibliography

ABC News. “Arrested in Alleged $722 Million Cryptocurrency Ponzi Scheme Targeting Investors.” ABC News, 2019.

Antonopoulos, Andreas M., and David Harding. *Mastering Bitcoin: Unlocking Digital Cryptocurrencies*. 3rd ed., O'Reilly Media, 2023.

BBC News. “Inside a Bitcoin Mine: How Cryptocurrency Is Made.” BBC News, 10 July 2021.

Bloomberg Crypto. “Squid Game Token Collapses After $3.3 Million Exit Scam.” Bloomberg, 2 Nov. 2021.

Cambridge Centre for Alternative Finance. “Global Cryptocurrency Benchmarking Study.” University of Cambridge, 2020.

Centre for Cybersecurity. “Cryptojacking Case Study on Tesla’s Experience.” 2022.

Cryptocurrency Mining Fraud (Confidential internal record; Case ID: AW-20230730-1 [redacted]). Internal document (Inquesta Corporation), 2023.

Lewis, Antony. *The Basics of Bitcoins and Blockchains: An Introduction to Cryptocurrencies and the Technology That Powers Them*. Kindle, Mango, 2018.

Popper, Nathaniel. *Digital Gold: Bitcoin and the Inside Story of the Misfits and Millionaires Trying to Reinvent Money*. HarperCollins, 2015.

Reuters. “New York Sues over $1 Billion Crypto Frauds Targeting Immigrants.” Reuters, 6 June 2024.

U.S. Department of Justice. “BitClub Network Founders Charged in $722 Million Cryptocurrency Fraud.” Justice.gov, 10 Dec. 2019.

YouTube video, “BitClub Network” promotional video depicting server banks purportedly used for cryptocurrency mining, https://www.youtube.com/watch?v=fR0B2m6jtCM (accessed Oct. 30, 2025).

YouTube video, “NovaTech Ltd Trading…,” https://www.youtube.com/watch?v=M032eDs2va8 (accessed Oct. 30, 2025).

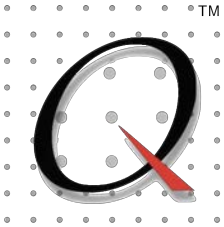
Accronyms

AI	Artificial Intelligence
AML	Anti-money-laundering
ASIC	Application-specific integrated circuit
AWS	Amazon Web Services
DPoS	Delegated Proof of Stake
FBI	Federal Bureau of Investigation
GPU	Graphics Processing Unit
KYC	Know Your Customer
MFA	Multifactor Authentication
PoS	Proof of Stake
PoW	Proof of Work
PSU	Power Supply Unit
ROI	Return on Investment
SEC	Securities Exchange Commission
SSL	Secure Socket Layer, an encryption protocol

About the Authors

Jacques R. Island, president of the Inquesta Corporation, has been a crisis manager since 1977 when he began service with the U.S. State Department protecting U.S. missions, diplomatic personnel and U.S. citizens abroad from terrorism, civil wars, and natural disasters. He wrote numerous emergency contingency plans and executed several in response to the forceful take-over of a U.S. embassy by a mob, and the evacuation of another embassy in the midst of a civil war. He transferred to the Federal Bureau of Investigation in 1982 where he performed collateral duties as a crisis negotiator and manager, dealing with prison uprisings, hostage takers, and terrorist incidents. He retired from the F.B.I. in 2002 to provide private investigation and risk management services to corporations in the U.S. and abroad. He is the author of *Your Plan is Your Parachute: A Simplified Guide to Business Continuity and Crisis Management*.

Jovana Desgouttes, Vice President for the Inquesta Corporation, has been involved in the administration of the company and assists with the management of investigations and consulting projects. She is currently a CyberAB Registered Practitioner for the company's Cybersecurity Maturity Model Certification (CMMC) projects for Department of Defense contractors and, as an active member of ISACA, and is working to become a Certified Information Systems Manager (CISM). She is also an active member of the Jacksonville (Florida) chapter of InfraGard, the F.B.I.-Private Sector partnership for protecting the critical infrastructures of the United States.



INQUESTA CORPORATION
2655 S. Le Jeune Road, Suite 581
Miami, FL 33134
305-779-3069
www.inquesta.com