



ESG and Cryptocurrency

Malk Insights — May 2023

Key Takeaways

- The rapid growth of the cryptocurrency market has presented investors with significant risks related to underdeveloped corporate governance controls and industry regulations, necessitating in-depth due diligence to ensure investments are positioned for longevity and scale.
- Key ESG considerations include governance structures, sales tactics, crypto crime, regulatory compliance, data privacy and security, and climate and environmental effects.
- Cryptocurrencies can have meaningful impacts due to their global reach and fast transaction speeds, which should be weighed against the potential risks and recent scandals faced by the industry.

ESG and Cryptocurrency

There are approximately [23,000 cryptocurrencies in existence today](#) that are used for various purposes, including as a means of payment, as investment vehicles, or as digital collectibles. The rapid growth in the crypto market, coupled with lagging regulation and limited precedent, expose the industry to ethics and compliance, data privacy and security, and climate change risks, which investors should consider.

Why ESG Diligence Should Matter to Crypto Investors

A February [class action lawsuit](#) accused several investors of promoting FTX, giving it an “air of legitimacy.” Investors at these firms have maintained they were misled, and that appropriate due diligence was performed. This lawsuit and another recent class action filed against more than a dozen defendants will have large scale implications, holding private equity and venture capital firms accountable for the promotion of their investments.

As public scrutiny and regulatory oversight of the cryptocurrency industry grows, investors should recognize their role in the development of the space. Investments in poorly governed companies that publicly crash and burn can hurt both professional and retail investors, affect regulation, and decrease crypto adoption and support. To manage related risks, investors should look for companies with operational best practices, including strong processes and policies that will support them as they scale. Not only can this lead to stronger investments, but it can aid in the advancement of the positive outcomes crypto can potentially achieve for society.

Key ESG Considerations

Ethics & Compliance Risks

Importance of Governance Structures

Governance failures in the industry are the most evident ethics risks given the crypto industry's nascency, lack of regulation, and limited precedent for governance controls. Examples of crypto companies that have suffered due to poor governance controls include Celsius, which was found to maintain insufficient funding for its compliance team, and [FTX](#), whose management was notorious in the investment community for being "so averse to outside input that investors who dared suggest that a more experienced executive run the company were likely to be shut out of future rounds of funding." Investors can identify and work to mitigate exposure to crypto investments with poor governance structures through robust due diligence processes. Diligence should include a review of company management structures, oversight, and programming to ensure investments maintain developed internal controls. For further detail on governance risks see Malk's FTX article [here](#).

Risks of Unethical Sales and Gamification

Unethical sales tactics increase the risk of customers being misled and manipulated. In the crypto industry, these tactics include too-good-to-be-true promotions, influencer promotion of risky products, and advertisements that don't align with contractual statements. These tactics are aimed towards impressionable traders and make crypto sound exciting, popular, and lucrative without clearly explaining the risks that come with the volatile market.

Two examples of this behavior can be seen in the fallen crypto companies Terraform (Terra) and Celsius:

1. Anchor, Terra's savings and lending platform, [promised 20% annual percentage yields](#) to borrowers in exchange for Terra deposits and interest payments. This promotion created artificial demand for Terra and raised concerns about the company downplaying risk and highlighting rewards to entice retail investors. When the company ultimately collapsed, almost \$40 billion dollars were lost. In February of this year, the [SEC charged Terra and its founder](#) with orchestrating a multi-billion-dollar securities scheme and defrauding investors.
2. The Celsius CEO [reportedly misled retail investors](#) when he tweeted that the company did not trade with or have access to customer funds. Hidden in Celsius' [terms of use](#) was a clause stating that customer funds deposited into Celsius accounts would belong to the company for use at its own discretion. [Former employees shared](#) that the company would use customer funds to manipulate the crypto market without their consent, and recent reports indicate Celsius used customer funds up until it declared bankruptcy.

Further, gamification can attract unseasoned traders and encourage risky trades. [Robinhood came under scrutiny by the State of Massachusetts](#) for gamification features such as confetti exploding on screen and scratch cards for free stocks earned by referring friends. The easy to use, game-like UI replaces the plain and somewhat confusing layout of a traditional trading platform, [making trades faster, easier, and more enjoyable](#), presenting users with instant gratification that can lead to trading addiction and a loss of their savings. FTX tapped into the gamification aspect of crypto trading by creating [FTX Battle Royale](#), which launched in 2019 as a way to bring more traders to the platform. This video game-like competition featured almost \$150,000 in prizes, badges, and a leaderboard.

Crypto Crime

[Law enforcement has greatly improved](#) at tracking blockchain transactions and catching criminals that use crypto to circumvent centralized banking. That said, such activity is still prominent in the industry; in 2022, [the US Treasury sanctioned crypto mixing service Tornado Cash](#) for allegedly laundering \$7 billion since 2019. Companies without strong Know Your Customer (KYC) or Anti-Money-Laundering (AML) controls in place increase their risk of facilitating crime, heightening the chance of public scrutiny, government attention, and

sanctions against them. Other kinds of crypto crime include hacking and ransom requests. Most crypto exchanges will keep customer funds offline in cold wallets, with a certain amount held in hot wallets for quick withdrawals. While both are secure, [hot wallets](#) are susceptible to attack due to their internet connection. Companies without robust data privacy and security programs and regularly cadenced audits increase the risk of a breach or leak occurring. Besides losing trust in the company, customers may never recover their losses as crypto is not insured under the FDIC.

Regulatory Compliance

The largest compliance risk crypto companies face is the rapidly evolving regulatory landscape. US-based crypto companies must currently abide by CFTC anti-money laundering (AML), know your customer (KYC), and market manipulation requirements, with pending US regulation including Executive Order 1406, the DCCPA, and the Infrastructure Investment and Jobs Act. Crypto companies operating in the US should also stay abreast of changes stemming from the ongoing FTX case and increasing congressional scrutiny. Many crypto companies do not operate in the US to avoid these protections but must nonetheless remain knowledgeable of [international crypto regulation](#) to ensure compliance given that the EU, UK, and UAE are in the drafting process.

Data Privacy & Security Risks

Data Privacy and Security risks primarily stem from the collection of significant amounts of PII from customers who create usernames and passwords when creating accounts or opening wallets. For companies with KYC requirements, sensitive data such as DOB, passport, ID, other government identification, and sometimes facial identification is collected, increasing the quantity and sensitivity of data collected and increasing the potential severity of an attack. Notably, some of the [most common cybersecurity risks](#) associated with crypto companies include exposure to phishing attacks, malware, and insufficient account security. Crypto companies and their third-party providers have become attractive targets for hackers, with [3.8 billion dollars lost to attacks in 2022](#); as such, crypto companies should have proper data security controls in place and perform appropriate technology due diligence on vendors. Companies should also maintain strong information security policies and processes and hold vendors to the same standards to reduce the chance of a breach occurring.

An additional risk relates to privacy on the blockchain. Privacy from a regulatory perspective can be difficult to achieve given that transactions and information shared on the blockchain are accessible to everyone and may be identified and used by bad actors for unknown purposes. Companies using blockchain technologies for transactions and/or information storage must protect data subject rights appropriately. [No official recommendations for processing personal data](#) on public or private blockchains exist but [some best practices companies can maintain](#) to align with data privacy regulation include irreversible data transformations such as hashing, combining on chain and off chain data, and using privacy-centric technology and cryptographic methods.

Climate & Environmental Risks

Cryptocurrency mining is an energy intensive operation, and as such, companies within the crypto industry can maintain significant greenhouse gas (GHG) emissions footprints. Notably, global electricity use for the largest market cap crypto assets resulted in a range of [emissions similar to emissions from diesel fuel used in railroads in the United States](#). Additionally, as climate regulations evolve, crypto companies may be required to track and report their GHG emissions, necessitating proper tracking processes and capabilities. Cryptocurrency mining can also cause environmental damage such as the production of electronic waste, noise, water, and air pollution. As the equipment used for mining is [highly specialized](#) and cannot be reused, companies must ensure proper chip disposal processes to prevent the leaching of toxic materials into the ground or air.

Potential Positive Use Cases

Despite the risks presented in the current crypto market, when managed appropriately, there are significant opportunities within the industry for enabling positive impact.

1. Developing countries are some of the largest users of cryptocurrency due to its popularity in the remittance market where migrants send money back to friends and family at home. Instead of conventional remittance services which can charge extremely high fees, [users can send crypto directly](#) or cash via crypto services to family instantly and with much lower costs.
2. In countries with financial instability or difficulty accessing traditional financing tools such as banks, crypto can help expand economic freedom. These benefits are especially significant in countries suffering from extreme inflation such as Argentina, Lebanon, Turkey, and Venezuela.
3. Due to its accessibility, crypto can also increase financial inclusion globally by [enabling financial access to underserved and unbanked populations](#). Approximately 6% of Americans have no bank account, for example, and rely on alternative financial services like payday loans, check cashing services, money orders, and pawn shop loans to pay bills. These alternative financing options expose unbanked individuals to obstacles like high service fees and unethical lenders and keep them from growing wealth.
4. Cryptocurrency can serve as a possible path to freedom for domestic violence victims, [99% of whom are also financially abused](#). Financial abuse can prevent a victim from leaving an abusive partner because victims may not have access to cash or bank accounts; additionally, fear of retaliation from abusers can prevent victims from earning money through work. Traditional crowd sourcing platforms require an ID or bank account information, which can expose victims attempting to source money, but [new crypto crowdsourcing platforms](#) allow users to remain anonymous, avoiding the risk of identification.
5. [Funding disaster relief and providing aid](#) with crypto is faster than using traditional financial channels, and capital is transferred directly to the people that need it most. Since the war in Ukraine began, for example, [an estimated \\$212 million in cryptocurrency](#) has been used to facilitate aid and military contributions with \$65 million donated in the first month of the war.

Investors and crypto companies both play a role in creating impactful crypto products. Investors can provide valuable guidance and expertise to companies not only around margin and process improvement, but on governance, ethics, and scaling; companies, in turn, must be open to the suggestions offered. Both parties should understand that these outcomes can only be achieved through proper controls and technological and ethical responsibility.

How Malk Can Support:

Public and investor interest in cryptocurrency has soared in recent years, as has the amount of scrutiny levied against the industry. Investors should continue to make time for in-depth due diligence and remember that just because something has high market value does not mean it is a strong investment. Investors should integrate ESG throughout the whole investment period by continuing to work with scaling companies on managing ongoing and upcoming risks, and Malk is well positioned to assist investors in this process. By providing in-depth due diligence that goes beyond an ESG score, and by creating targeted recommendations, Malk enables investors to proactively manage their ESG risks and identify value creation opportunities within their portfolio.



Kelsey Jarrett
Vice President
e: kjarrett@malk.com



Storm McLaughlin
Engagement Manager
e: smclaughlin@malk.com



Christina Tedeschi
Project Manager
e: ctedeschi@malk.com



Alana Miro
Associate
e: amiro@malk.com

Malk Partners does not make any express or implied representation or warranty on any future realization, outcome or risk associated with the content contained in this material. All recommendations contained herein are made as of the date of circulation and based on current ESG standards. Malk is an ESG advisory firm, and nothing in this material should be construed as, nor a substitute for, legal, technical, scientific, risk management, accounting, financial, or any other type of business advice, as the case may be.

About Malk Partners

Malk Partners is the preeminent advisor to private market investors for creating and protecting value through environmental, social, and governance (“ESG”) management and impact investing. Founded in 2009, Malk Partners advises many of the world’s leading alternatives managers investing across private equity, growth equity, venture capital, and private credit by helping them define ESG goals, achieve ESG results, and guide their portfolio companies in driving value creation and mitigating risks. The firm is headquartered in La Jolla, California with a second office located in New York. For more information about Malk Partners, please visit www.malk.com.