APPENDIX 1

ADDITIONAL DISCLOSURE OF RISK FACTORS OF GREENCOIN.AI

Item 1. Risk Factors

A description of the risks and uncertainties associated with our business is set forth below. You should carefully consider the risks and uncertainties described below. The risks and uncertainties described below are not the only ones we face. Additional risks and uncertainties that we are unaware of or that we deem immaterial may also become important factors that adversely affect our business. If any of the following risks occur, our business, operating results, financial condition and future prospects could be materially and adversely affected.

Risk Factors Summary

Consistent with the foregoing, our business is subject to a number of risks and uncertainties, including those risks discussed at length below. These risks include, among others, the following, which we consider our most material risks:

• our operating results have and will significantly fluctuate due to the highly volatile nature of crypto;

• our total revenue is substantially dependent on the prices of crypto assets and volume of transactions conducted on our platform. If such price or volume declines, our business, operating results, and financial condition would be adversely affected;

• the future development and growth of crypto is subject to a variety of factors that are difficult to predict and evaluate. If crypto does not grow as we expect, our business, operating results, and financial condition could be adversely affected;

• cyberattacks and security breaches of our platform, or those impacting our customers or third parties, could adversely impact our brand and reputation and our business, operating results, and financial condition;

• we are subject to an extensive and highly-evolving regulatory landscape and any adverse changes to, or our failure to comply with, any laws and regulations could adversely affect our brand, reputation, business, operating results, and financial condition;
• as we continue to expand and localize our international activities, our obligations to comply with the laws, rules, regulations, and policies of a variety of jurisdictions will increase and we may be subject to inquiries, investigations and enforcement actions by U.S. and non-U.S. regulators and governmental authorities;

• we may be subject to material litigation, including individual and class action lawsuits, as well as inquiries, investigations and enforcement actions by regulators and governmental authorities;

• we currently rely on third-party service providers for certain aspects of our operations, and any interruptions in services provided by these third parties may impair our ability to support our customers;

• loss of a critical banking or insurance relationship could adversely impact our business, operating results, and financial condition;

• any significant disruption in our products and services, in our information technology systems, or in any of the blockchain networks we support, could result in a loss of customers or funds and adversely impact our brand and reputation and our business, operating results, and financial condition;

• the loss or destruction of private keys required to access any crypto assets held in custody for our own account or for our customers may be irreversible. If we are unable to access our private keys or if we experience a hack or other data loss relating to our ability to access any crypto assets, it could cause regulatory scrutiny, reputational harm, and other losses.

**Risk Factors**

**The Most Material Risks Related to Our Business and Financial Position**

*Our operating results have and will significantly fluctuate due to the highly volatile nature of crypto.*

Our operating results are dependent on crypto assets and the broader cryptoeconomy. Due to the highly volatile nature of the cryptoeconomy and the prices of crypto assets, our operating results have, and will continue to, fluctuate significantly from quarter to quarter in accordance with market sentiments and movements in the broader cryptoeconomy. Our operating results will continue to fluctuate significantly as a result of a variety of factors, many of which are unpredictable and in certain instances are outside of our control, including:

• our dependence on offerings that are dependent on crypto asset trading activity, including trading volume and the prevailing trading prices for crypto assets, whose trading prices and volume can be highly volatile;
• our ability to attract, maintain, and grow our customer base and engage our customers;

• changes in the legislative or regulatory environment, or actions by U.S. or foreign governments or regulators, including fines, orders, or consent decrees;

• regulatory changes that impact our ability to offer certain products or services;

• our ability to diversify and grow our subscription and services revenue;

• pricing for our products and services;

• investments we make in the development of products and services as well as technology offered to our ecosystem partners, international expansion, and sales and marketing;

• adding and removing of crypto assets on our platform;

• market conditions of, and overall sentiment towards, the cryptoeconomy;

• macroeconomic conditions;

• adverse legal proceedings or regulatory enforcement actions, judgments, settlements, or other legal proceeding and enforcement-related costs;

• the development and introduction of existing and new products and services by us or our competitors;

• increases in operating expenses that we expect to incur to grow and expand our operations and to remain competitive;

• system failure or outages, including with respect to our crypto platform and third-party crypto networks;

• breaches of security or privacy;

• inaccessibility of our platform due to our or third-party actions;

• our ability to attract and retain talent; and

• our ability to compete with our competitors.

As a result of these factors, it is difficult for us to forecast growth trends accurately.
and our business and future prospects are difficult to evaluate, particularly in the short term. In view of the rapidly evolving nature of our business and the cryptoeconomy, period-to-period comparisons of our operating results may not be meaningful, and you should not rely upon them as an indication of future performance. Quarterly and annual expenses reflected in our financial statements may be significantly different from historical or projected rates. Our operating results in one or more future quarters may fall below the expectations of securities analysts and investors.

**Our total revenue is substantially dependent on the prices of crypto assets and volume of transactions conducted on our platform. If such price or volume declines, our business, operating results, and financial condition would be adversely affected.**

We generate substantially all of our total revenue from transaction fees on our platform in connection with the purchase, sale, and trading of crypto assets by our customers. Transaction revenue is based on transaction fees that are either a flat fee or a percentage of the value of each transaction. For our retail brokerage product, we also charge a spread to ensure that we are able to settle purchases and sales at the price we quote to customers. We also generate total revenue from our subscription products and services and, while revenue from these products and services have not been significant to date, most of this revenue will also fluctuate based on the price of crypto assets. As such, any declines in the volume of crypto asset transactions, the price of crypto assets, or market liquidity for crypto assets generally may result in lower total revenue to us.

The price of crypto assets and associated demand for buying, selling, and trading crypto assets have historically been subject to significant volatility. Such circumstances may adversely affect our net revenue and operating results. The price and trading volume of any crypto asset is subject to significant uncertainty and volatility, depending on a number of factors, including:

- market conditions of, and overall sentiment towards, the cryptoeconomy;
- changes in liquidity, market-making volume, and trading activities;
- trading activities on other crypto platforms worldwide, many of which may be unregulated, and may include manipulative activities;
- investment and trading activities of highly active retail and institutional users, speculators, miners, and investors;
- the speed and rate at which crypto is able to gain adoption as a medium of exchange, utility, store of value, consumptive asset, security instrument, or other financial assets worldwide, if at all;
- decreased user and investor confidence in crypto assets and crypto platforms;
• negative publicity and events relating to the cryptoeconomy;

• unpredictable social media coverage or “trending” of, or other rumors and market speculation regarding crypto assets;

• the ability for crypto assets to meet user and investor demands;

• the functionality and utility of crypto assets and their associated ecosystems and networks, including crypto assets designed for use in various applications;

• retail user preferences and perceived value of crypto assets and crypto asset markets;

• increased competition from other payment services or other crypto assets that exhibit better speed, security, scalability, or other characteristics;

• regulatory or legislative changes and updates affecting the cryptoeconomy;

• the characterization of crypto assets under the laws of various jurisdictions around the world;

• the maintenance, troubleshooting, and development of the blockchain networks underlying crypto assets, including by miners, validators, and developers worldwide;

• the ability for crypto networks to attract and retain miners or validators to secure and confirm transactions accurately and efficiently;

• ongoing technological viability and security of crypto assets and their associated smart contracts, applications and networks, including vulnerabilities against hacks and scalability;

• fees and speed associated with processing crypto asset transactions, including on the underlying blockchain networks and on crypto platforms;

• financial strength of market participants;

• the availability and cost of funding and capital;

• the liquidity of crypto platforms;

• interruptions in service from or failures of major crypto platforms;
• availability of an active derivatives market for various crypto assets;

• availability of banking and payment services to support crypto-related projects;

• level of interest rates and inflation;

• monetary policies of governments, trade restrictions, and fiat currency devaluations; and

• national and international economic and political conditions.

There is no assurance that any supported crypto asset will maintain its value or that there will be meaningful levels of trading activities. In the event that the price of crypto assets or the demand for trading crypto assets decline, our business, operating results, and financial condition would be adversely affected.

The future development and growth of crypto is subject to a variety of factors that are difficult to predict and evaluate. If crypto does not grow as we expect, our business, operating results, and financial condition could be adversely affected.

Crypto assets built on blockchain technology were only introduced in 2008 and remain in the early stages of development. In addition, different crypto assets are designed for different purposes. Bitcoin, for instance, was designed to serve as a peer-to-peer electronic cash system, while Ethereum was designed to be a smart contract and decentralized application platform. Many other crypto networks—ranging from cloud computing to tokenized securities networks—have only recently been established. The further growth and development of any crypto assets and their underlying networks and other cryptographic and algorithmic protocols governing the creation, transfer, and usage of crypto assets represent a new and evolving paradigm that is subject to a variety of factors that are difficult to evaluate, including:

• many crypto networks have limited operating histories, have not been validated in production, and are still in the process of developing and making significant decisions that will affect the design, supply, issuance, functionality, and governance of their respective crypto assets and underlying blockchain networks, any of which could adversely affect their respective crypto assets;

• many crypto networks are in the process of implementing software upgrades and other changes to their protocols, which could introduce bugs, security risks, or adversely affect the respective crypto networks;

• Several large networks, including Bitcoin and Ethereum, are developing new features to address fundamental speed, scalability, and energy usage issues. If these issues are not successfully addressed, or are unable to receive
widespread adoption, it could adversely affect the underlying crypto assets;

- security issues, bugs, and software errors have been identified with many crypto assets and their underlying blockchain networks, some of which have been exploited by malicious actors. There are also inherent security weaknesses in some crypto assets, such as when creators of certain crypto networks use procedures that could allow hackers to counterfeit tokens. Any weaknesses identified with a crypto assets could adversely affect its price, security, liquidity, and adoption. If a malicious actor or botnet (a volunteer or hacked collection of computers controlled by networked software coordinating the actions of the computers) obtains a majority of the compute or staking power on a crypto network, as has happened in the past, it may be able to manipulate transactions, which could cause financial losses to holders, damage the network’s reputation and security, and adversely affect its value;

- the development of new technologies for mining, such as improved application-specific integrated circuits (commonly referred to as ASICs), or changes in industry patterns, such as the consolidation of mining power in a small number of large mining farms, could reduce the security of blockchain networks, lead to increased liquid supply of crypto assets, and reduce a crypto’s price and attractiveness;

- if rewards and transaction fees for miners or validators on any particular crypto network are not sufficiently high to attract and retain miners, a crypto network’s security and speed may be adversely affected, increasing the likelihood of a malicious attack;

- many crypto assets have concentrated ownership or an “admin key”, allowing a small group of holders to have significant unilateral control and influence over key decisions relating to their crypto networks, such as governance decisions and protocol changes, as well as the market price of such crypto assets;

- the governance of many decentralized blockchain networks is by voluntary consensus and open competition, and many developers are not directly compensated for their contributions. As a result, there may be a lack of consensus or clarity on the governance of any particular crypto network, a lack of incentives for developers to maintain or develop the network, and other unforeseen issues, any of which could result in unexpected or undesirable errors, bugs, or changes, or stymie such network’s utility and ability to respond to challenges and grow; and

- many crypto networks are in the early stages of developing partnerships and collaborations, all of which may not succeed and adversely affect the usability and adoption of the respective crypto assets.

Various other technical issues have also been uncovered from time to time that
resulted in disabled functionalities, exposure of certain users’ personal information, theft of users’ assets, and other negative consequences, and which required resolution with the attention and efforts of their global miner, user, and development communities. If any such risks or other risks materialize, and in particular if they are not resolved, the development and growth of crypto may be significantly affected and, as a result, our business, operating results, and financial condition could be adversely affected.

Cyberattacks and security breaches of our platform, or those impacting our customers or third parties, could adversely impact our brand and reputation and our business, operating results, and financial condition.

Our business involves the collection, storage, processing, and transmission of confidential information, customer, employee, service provider, and other personal data, as well as information required to access customer assets. We have built our reputation on the premise that our platform offers customers a secure way to purchase, store, and transact in crypto assets. As a result, any actual or perceived security breach of us or our third-party partners may:

• harm our reputation and brand;
• result in our systems or services being unavailable and interrupt our operations;
• result in improper disclosure of data and violations of applicable privacy and other laws;
• result in significant regulatory scrutiny, investigations, fines, penalties, and other legal, regulatory, and financial exposure;
• cause us to incur significant remediation costs;
• lead to theft or irretrievable loss of our or our customers’ fiat currencies or crypto assets;
• reduce customer confidence in, or decreased use of, our products and services;
• divert the attention of management from the operation of our business;
• result in significant compensation or contractual penalties from us to our customers or third parties as a result of losses to them or claims by them; and
• adversely affect our business and operating results.

Further, any actual or perceived breach or cybersecurity attack directed at other financial institutions or crypto companies, whether or not we are directly impacted, could lead to a general loss of customer confidence in the cryptoeconomy or in
the use of technology to conduct financial transactions, which could negatively impact us, including the market perception of the effectiveness of our security measures and technology infrastructure.

An increasing number of organizations, including large merchants, businesses, technology companies, and financial institutions, as well as government institutions, have disclosed breaches of their information security systems, some of which have involved sophisticated and highly targeted attacks, including on their websites, mobile applications, and infrastructure.

Attacks upon systems across a variety of industries, including the crypto industry, are increasing in their frequency, persistence, and sophistication, and, in many cases, are being conducted by sophisticated, well-funded, and organized groups and individuals, including state actors. The techniques used to obtain unauthorized, improper, or illegal access to systems and information (including customers’ personal data and crypto assets), disable or degrade services, or sabotage systems are constantly evolving, may be difficult to detect quickly, and often are not recognized or detected until after they have been launched against a target. These attacks may occur on our systems or those of our third-party service providers or partners. Certain types of cyberattacks could harm us even if our systems are left undisturbed. For example, attacks may be designed to deceive employees and service providers into releasing control of our systems to a hacker, while others may aim to introduce computer viruses or malware into our systems with a view to stealing confidential or proprietary data. Additionally, certain threats are designed to remain dormant or undetectable until launched against a target and we may not be able to implement adequate preventative measures.

Although we have developed systems and processes designed to protect the data we manage, prevent data loss and other security breaches, effectively respond to known and potential risks, and expect to continue to expend significant resources to bolster these protections, there can be no assurance that these security measures will provide absolute security or prevent breaches or attacks. We have experienced from time to time, and may experience in the future, breaches of our security measures due to human error, malfeasance, insider threats, system errors or vulnerabilities, or other irregularities. Unauthorized parties have attempted, and we expect that they will continue to attempt, to gain access to our systems and facilities, as well as those of our customers, partners, and third-party service providers, through various means, including hacking, social engineering, phishing, and attempting to fraudulently induce individuals (including employees, service providers, and our customers) into disclosing usernames, passwords, payment card information, or other sensitive information, which may in turn be used to access our information technology systems and customers’ crypto assets. Threats can come from a variety of sources, including criminal hackers, hacktivists, state-sponsored intrusions, industrial espionage, and insiders. Certain threat actors may be supported by significant financial and technological resources, making them even more sophisticated and difficult to detect. Further, there has been an increase in such activities as a result of the novel
coronavirus ("COVID-19") pandemic. As a result, our costs and the resources we devote to protecting against these advanced threats and their consequences may continue to increase over time.

Although we maintain insurance coverage that we believe is adequate for our business, it may be insufficient to protect us against all losses and costs stemming from security breaches, cyberattacks, and other types of unlawful activity, or any resulting disruptions from such events. Outages and disruptions of our platform, including any caused by cyberattacks, may harm our reputation and our business, operating results, and financial condition.

*We are subject to an extensive and highly-evolving regulatory landscape and any adverse changes to, or our failure to comply with, any laws and regulations could adversely affect our brand, reputation, business, operating results, and financial condition.*

Our business is subject to extensive laws, rules, regulations, policies, orders, determinations, directives, treaties, and legal and regulatory interpretations and guidance in the markets in which we operate, including those governing financial services and banking, trust companies, securities, broker-dealers and alternative trading systems ("ATS"), commodities, credit, crypto asset custody, exchange, and transfer, cross-border and domestic money and crypto asset transmission, retail and commercial lending, usury, foreign currency exchange, privacy, data governance, data protection, cybersecurity, fraud detection, payment services (including payment processing and settlement services), retail protection, escheatment, antitrust and competition, bankruptcy, tax, anti-bribery, economic and trade sanctions, anti-money laundering, and counter-terrorist financing. Many of these legal and regulatory regimes were adopted prior to the advent of the internet, mobile technologies, crypto assets, and related technologies. As a result, they do not contemplate or address unique issues associated with the cryptoeconomy, are subject to significant uncertainty, and vary widely across U.S. federal, state, and local and international jurisdictions. These legal and regulatory regimes, including the laws, rules, and regulations thereunder, evolve frequently and may be modified, interpreted, and applied in an inconsistent manner from one jurisdiction to another, and may conflict with one another. Moreover, the complexity and evolving nature of our business and the significant uncertainty surrounding the regulation of the cryptoeconomy requires us to exercise our judgement as to whether certain laws, rules, and regulations apply to us, and it is possible that governmental bodies and regulators may disagree with our conclusions. To the extent we have not complied with such laws, rules, and regulations, we could be subject to significant fines, revocation of licenses, limitations on our products and services, reputational harm, and other regulatory consequences, each of which may be significant and could adversely affect our business, operating results, and financial condition.

In addition to existing laws and regulations, various governmental and regulatory bodies, including legislative and executive bodies, in the United States and in other
countries may adopt new laws and regulations, or new interpretations of existing laws and regulations may be issued by such bodies or the judiciary, which may adversely impact the development of the cryptoeconomy as a whole and our legal and regulatory status in particular by changing how we operate our business, how our products and services are regulated, and what products or services we and our competitors can offer, requiring changes to our compliance and risk mitigation measures, imposing new licensing requirements, or imposing a total ban on certain crypto asset transactions, as has occurred in certain jurisdictions in the past. For example, under recommendations from the Financial Crimes Enforcement Network (“FinCEN”), and the Financial Action Task Force (“FATF”), the United States and several foreign jurisdictions are likely to impose the Funds Travel Rule and the Funds Transfer Rule (commonly referred to collectively as the Travel Rule) on financial service providers in the cryptoeconomy. We may face substantial compliance costs to operationalize and comply with the Travel Rule and may be further subject to administrative sanctions for technical violations or customer attrition if the user experience suffers as a result. More recently, in December 2020, FinCEN released a proposed rule that may require us to collect personal information from the owners of self-custodied wallets that transfer cryptocurrencies to or receive cryptocurrencies from us, and report certain transactions to the federal government. There are substantial uncertainties on how these requirements would apply in practice, and we may face substantial compliance costs to operationalize and comply with these rules. We may be further subject to administrative sanctions for technical violations or customer attrition if the user experience suffers as a result. As another example, the recent extension of anti-money laundering requirements to certain crypto-related activities by the European Union’s (“E.U.”) Fifth Money Laundering Directive has increased the regulatory compliance burden for business in Europe and, as a result of the fragmented approach to the implementation of its provisions, resulted in distinct and divergent national licensing and registration regimes for us in different E.U. member states. Further E.U.-level legislation imposing additional regulatory requirements in relation to crypto-related activities is also expected in the intermediate term which, among other things, may impose new or additional regulatory requirements on both crypto service providers and issuers of certain crypto assets, which may impact our operations in the E.U.

Because we have offered and will continue to offer a variety of innovative products and services to our customers, many of our offerings are subject to significant regulatory uncertainty and we from time to time face regulatory inquiries regarding our current and planned products. The regulatory treatment of fiat-backed stablecoins is highly uncertain and has drawn significant attention from legislative and regulatory bodies around the world. The issuance and resale of such stablecoins may implicate a variety of banking, deposit, money transmission, prepaid access and stored value, anti-money laundering, commodities, securities, sanctions, and other laws and regulations in the U.S. and in other jurisdictions. Certain products and services offered by us that we believe are not subject to regulatory oversight, or are only subject to certain regulatory regimes, may cause us to be deemed to be engaged in a form of regulated activity for which licensure is required or cause us to become subject to new and additional forms of regulatory oversight. We also offer various staking,
rewards, and other products, all of which are subject to significant regulatory uncertainty, and could implicate a variety of laws and regulations worldwide. While we have implemented policies and procedures designed to help monitor for and ensure compliance with existing and new laws and regulations, there can be no assurance that we and our employees, contractors, and agents will not violate or otherwise fail to comply with such laws and regulations. To the extent that we or our employees, contractors, or agents are deemed or alleged to have violated or failed to comply with any laws or regulations, including related interpretations, orders, determinations, directives, or guidance, we or they could be subject to a litany of civil, criminal, and administrative fines, penalties, orders and actions, including being required to suspend or terminate the offering of certain products and services.

Due to our business activities, we are subject to ongoing examinations, oversight, and reviews by U.S. federal and state regulators, and foreign financial service regulators, which each have broad discretion to audit and examine our business. We are periodically subject to audits and examinations by these regulatory authorities. As a result of findings from these audits and examinations, regulators may in the future require us to take certain actions, including amending, updating, or revising our compliance measures from time to time, limiting the kinds of customers which we provide services to, changing, terminating, or delaying our licenses and/or the introduction of our existing or new product and services, and undertaking further external audit or being subject to further regulatory scrutiny, including investigations and inquiries. We may in the future receive examination reports citing violations of rules and regulations, inadequacies in existing compliance programs, and requiring us to enhance certain practices with respect to our compliance program, including due diligence, monitoring, training, reporting, and recordkeeping. Implementing appropriate measures to properly remediate these examination findings may require us to incur significant costs, and if we fail to properly remediate any of these examination findings, we could face civil litigation, significant fines, damage awards, forced removal of certain employees including members of our executive team, barring of certain employees from participating in our business in whole or in part, revocation of existing licenses, limitations on existing and new products and services, reputational harm, negative impact to our existing relationships with regulators, exposure to criminal liability, or other regulatory consequences. Further, we believe increasingly strict legal and regulatory requirements and additional regulatory investigations and enforcement, any of which could occur or intensify, may continue to result in changes to our business, as well as increased costs, and supervision and examination for both ourselves and our agents and service providers. Moreover, new laws, regulations, or interpretations may result in additional litigation, regulatory investigations, and enforcement or other actions, including preventing or delaying us from offering certain products or services offered by our competitors or could impact how we offer such products and services. Adverse changes to, or our failure to comply with, any laws and regulations have had, and may continue to have, an adverse effect on our reputation and brand and our business, operating results, and financial condition.

As we continue to expand and localize our international activities, our
obligations to comply with the laws, rules, regulations, and policies of a variety of jurisdictions will increase and we may be subject to investigations and enforcement actions by U.S. and non-U.S. regulators and governmental authorities.

As we expand and localize our international activities, we have become increasingly obligated to comply with the laws, rules, regulations, policies, and legal interpretations both of the jurisdictions in which we operate and those into which we offer services on a cross-border basis. For instance, financial regulators outside the United States have in recent months significantly increased their scrutiny of crypto asset exchanges, such as by requiring crypto asset exchanges operating in their local jurisdictions to be regulated and licensed under local laws. Moreover, laws regulating financial services, the internet, mobile technologies, crypto, and related technologies outside of the United States are highly evolving, extensive and often impose different, more specific, or even conflicting obligations on us, as well as broader liability. For example, we are required to comply with laws and regulations related to sanctions and export controls enforced by U.S. Department of Treasury's Office of Foreign Assets Control (“OFAC”), and U.S. anti-money laundering and counter-terrorist financing laws and regulations, enforced by FinCEN and certain state financial services regulators. U.S. sanctions laws and regulations generally restrict dealings by persons subject to U.S. jurisdiction with certain governments, countries, or territories that are the target of comprehensive sanctions, currently the Crimea Region of Ukraine, Cuba, Iran, North Korea, Syria, and Venezuela as well as with persons identified on certain prohibited lists. We may share key particulars of our compliance program with OFAC and we believe we have a reasonable risk-based program in place. Nonetheless, there can be no guarantee that these measures will be viewed as compliant. In particular, the nature of the blockchain and of our services makes it technically infeasible in all circumstances to prevent transactions with particular persons or addresses. From time to time, we have submitted voluntary disclosures to OFAC or responded to administrative subpoenas from OFAC that have identified such transactions. Certain of these voluntary self-disclosures are currently under review by OFAC. To date, none of those proceedings has resulted in a monetary penalty or other adverse action. However, if we were to be found to have violated sanctions, or become involved in government investigations, that could result in negative consequences for us, including costs related to government investigations, financial penalties, and harm to our reputation. The impact on us related to these matters could be substantial. Although we have implemented controls, and are working to implement additional controls and screening tools designed to prevent similar activity from occurring in the future, there is no guarantee that we will not inadvertently provide our products and services to additional individuals, entities, or governments prohibited by U.S. sanctions in the future.

Regulators worldwide frequently study each other’s approaches to the regulation of the cryptoeconomy. Consequently, developments in any jurisdiction may influence other jurisdictions. New developments in one jurisdiction may be extended to additional services and other jurisdictions. As a result, the risks created by any new law or
regulation in one jurisdiction are magnified by the potential that they may be replicated, affecting our business in another place or involving another service. Conversely, if regulations diverge worldwide, we may face difficulty adjusting our products, services, and other aspects of our business with the same effect. These risks are heightened as we face increased competitive pressure from other similarly situated businesses that engage in regulatory arbitrage to avoid the compliance costs associated with regulatory changes.

The complexity of U.S. federal and state and international regulatory and enforcement regimes, coupled with the global scope of our operations and the evolving global regulatory environment, could result in a single event prompting a large number of overlapping investigations and legal and regulatory proceedings by multiple government authorities in different jurisdictions. Any of the foregoing could, individually or in the aggregate, harm our reputation, damage our brands and business, and adversely affect our operating results and financial condition. Due to the uncertain application of existing laws and regulations, it may be that, despite our regulatory and legal analysis concluding that certain products and services are currently unregulated, such products or services may indeed be subject to financial regulation, licensing, or authorization obligations that we have not obtained or with which we have not complied. As a result, we are at a heightened risk of enforcement action, litigation, regulatory, and legal scrutiny which could lead to sanctions, cease, and desist orders, or other penalties and censures which could significantly and adversely affect our continued operations and financial condition.

We may be subject to material litigation, including individual and class action lawsuits, as well as investigations and enforcement actions by regulators and governmental authorities.

We may from time to time become subject to claims, arbitrations, individual and class action lawsuits, government and regulatory investigations, inquiries, actions or requests, including with respect to both retail user and employment matters, securities matters, and other proceedings alleging violations of laws, rules, and regulations, both foreign and domestic. The scope, determination, and impact of claims, lawsuits, government and regulatory investigations, enforcement actions, disputes, and proceedings to which we are subject cannot be predicted with certainty, and may result in:

- substantial payments to satisfy judgments, fines, or penalties;
- substantial outside counsel legal fees and costs;
- additional compliance and licensure requirements;
- loss or non-renewal of existing licenses or authorizations, or prohibition from or delays in obtaining additional licenses or authorizations, required for our business;
• loss of productivity and high demands on employee time;
• criminal sanctions or consent decrees;
• termination of certain employees, including members of our executive team;
• barring of certain employees from participating in our business in whole or in part;
• orders that restrict our business or prevent us from offering certain products or services;
• changes to our business model and practices;
• delays to planned transactions, product launches or improvements; and
• damage to our brand and reputation.

Because of our large customer base, actions against us may claim large monetary damages, even if the alleged per-customer harm is small or non-existent. Regardless of the outcome, any such matters can have an adverse impact, which may be material, on our business, operating results, or financial condition because of legal costs, diversion of management resources, reputational damage, and other factors.

**We currently rely on third-party service providers for certain aspects of our operations, and any interruptions in services provided by these third parties may impair our ability to support our customers.**

We rely on third parties in connection with many aspects of our business, including payment processors, banks, and payment gateways to process transactions; cloud computing services and data centers that provide facilities, infrastructure, website functionality and access, components, and services, including databases and data center facilities and cloud computing; as well as third parties that provide outsourced customer service, compliance support and product development functions, which are critical to our operations. Because we rely on third parties to provide these services and to facilitate certain of our business activities, we face increased operational risks. We do not control the operation of any of these third parties, including the data center facilities we use. These third parties may be subject to financial, legal, regulatory, and labor issues, cybersecurity incidents, break-ins, computer viruses, denial-of-service attacks, sabotage, acts of vandalism, privacy breaches, service terminations, disruptions, interruptions, and other misconduct. They are also vulnerable to damage or interruption from human error, power loss, telecommunications failures, fires, floods, earthquakes, hurricanes, tornadoes, pandemics (including the COVID-19 pandemic) and similar events. For example, on
February 24, 2021, the U.S. Federal Reserve’s payments network experienced an outage, which had the potential to result in reduced functionality for certain of our products. In addition, these third parties may breach their agreements with us, disagree with our interpretation of contract terms or applicable laws and regulations, refuse to continue or renew these agreements on commercially reasonable terms or at all, fail or refuse to process transactions or provide other services adequately, take actions that degrade the functionality of our services, impose additional costs or requirements on us or our customers, or give preferential treatment to competitors. There can be no assurance that third parties that provide services to us or to our customers on our behalf will continue to do so on acceptable terms, or at all. If any third parties do not adequately or appropriately provide their services or perform their responsibilities to us or our customers on our behalf, such as if third-party service providers to close their data center facilities without adequate notice, are unable to restore operations and data, fail to perform as expected, or experience other unanticipated problems, we may be unable to procure alternatives in a timely and efficient manner and on acceptable terms, or at all, and we may be subject to business disruptions, losses or costs to remediate any of the deficiencies, customer dissatisfaction, reputational damage, legal or regulatory proceedings, or other adverse consequences which could harm our business.

**Loss of a critical banking or insurance relationship could adversely impact our business, operating results, and financial condition.**

We rely on bank accounts to provide our platform and custodial services. In particular, customer cash holdings on our platform are held with one or more of our banking partners. In some circumstances our banking partners may view us as a higher risk customer for purposes of their anti-money laundering programs. We may face difficulty establishing or maintaining banking relationships due to our banking partners’ policies and some prior bank partners have terminated their relationship with us or have limited access to bank services. The loss of these banking partners or the imposition of operational restrictions by these banking partners and the inability for us to utilize other redundant financial institutions may result in a disruption of business activity as well as regulatory risks. In addition, financial institutions in the U.S. and globally may, as a result of the myriad of regulations or the risks of crypto assets generally, decide to not provide account, custody, or other financial services to us or the cryptoeconomy generally. We also rely on insurance carriers to insure customer losses resulting from a breach of our physical security, cyber security, or by employee or service provider theft. Our ability to maintain crime and specie insurance is subject to the insurance carriers’ ongoing underwriting criteria and our inability to obtain and maintain appropriate insurance coverage could cause a substantial business disruption, adverse reputational impact, inability to compete with our competitors, and regulatory scrutiny.

**Any significant disruption in our products and services, in our information technology systems, or in any of the blockchain networks we support, could**
result in a loss of customers or funds and adversely impact our brand and reputation and our business, operating results, and financial condition.

Our reputation and ability to attract and retain customers and grow our business depends on our ability to operate our service at high levels of reliability, scalability, and performance, including the ability to process and monitor, on a daily basis, a large number of transactions that occur at high volume and frequencies across multiple systems. Our platform, the ability of our customers to trade, and our ability to operate at a high level, are dependent on our ability to access the blockchain networks underlying the supported crypto assets, for which access is dependent on our systems’ ability to access the internet. Further, the successful and continued operations of such blockchain networks will depend on a network of computers, miners, or validators, and their continued operations, all of which may be impacted by service interruptions.

Our systems, the systems of our third-party service providers and partners, and certain crypto asset and blockchain networks have experienced from time to time, and may experience in the future service interruptions or degradation because of hardware and software defects or malfunctions, distributed denial-of-service and other cyberattacks, insider threats, break-ins, sabotage, human error, vandalism, earthquakes, hurricanes, floods, fires, and other natural disasters, power losses, disruptions in telecommunications services, fraud, military or political conflicts, terrorist attacks, computer viruses or other malware, or other events. In addition, extraordinary Trading Volumes or site usage could cause our computer systems to operate at an unacceptably slow speed or even fail. Some of our systems, including systems of companies we have acquired, or the systems of our third-party service providers and partners are not fully redundant, and our or their disaster recovery planning may not be sufficient for all possible outcomes or events.

If any of our systems, or those of our third-party service providers, are disrupted for any reason, our products and services may fail, resulting in unanticipated disruptions, slower response times and delays in our customers’ trade execution and processing, failed settlement of trades, incomplete or inaccurate accounting, recording or processing of trades, unauthorized trades, loss of customer information, increased demand on limited customer support resources, customer claims, complaints with regulatory organizations, lawsuits, or enforcement actions. A prolonged interruption in the availability or reduction in the availability, speed, or functionality of our products and services could harm our business. Frequent or persistent interruptions in our services could cause current or potential customers or partners to believe that our systems are unreliable, leading them to switch to our competitors or to avoid or reduce the use of our products and services, and could permanently harm our reputation and brands. Moreover, to the extent that any system failure or similar event results in damages to our customers or their business partners, these customers or partners could seek significant compensation or contractual penalties from us for their losses, and those claims, even if unsuccessful, would likely be time-consuming and costly for us to address. Problems with the reliability or security of our systems would harm our
reputation, and damage to our reputation and the cost of remedying these problems could negatively affect our business, operating results, and financial condition.

In addition, we are continually improving and upgrading our information systems and technologies. Implementation of new systems and technologies is complex, expensive, time-consuming, and may not be successful. If we fail to timely and successfully implement new information systems and technologies, or improvements or upgrades to existing information systems and technologies, or if such systems and technologies do not operate as intended, it could have an adverse impact on our business, internal controls (including internal controls over financial reporting), operating results, and financial condition.

The loss or destruction of private keys required to access any crypto assets held in custody for our own account or for our customers may be irreversible. If we are unable to access our private keys or if we experience a hack or other data loss relating to our ability to access any crypto assets, it could cause regulatory scrutiny, reputational harm, and other losses.

Crypto assets are generally controllable only by the possessor of the unique private key relating to the digital wallet in which the crypto assets are held. While blockchain protocols typically require public addresses to be published when used in a transaction, private keys must be safeguarded and kept private in order to prevent a third party from accessing the crypto assets held in such a wallet. To the extent that any of the private keys relating to our hot or cold wallets containing crypto assets held for our own account or for our customers is lost, destroyed, or otherwise compromised or unavailable, and no backup of the private key is accessible, we will be unable to access the crypto assets held in the related wallet. Further, we cannot provide assurance that our wallet will not be hacked or compromised. Crypto assets and blockchain technologies have been, and may in the future be, subject to security breaches, hacking, or other malicious activities. Any loss of private keys relating to, or hack or other compromise of, digital wallets used to store our customers’ crypto assets could adversely affect our customers’ ability to access or sell their crypto assets, require us to reimburse our customers for their losses, and subject us to significant financial losses in addition to losing customer trust in us and our products. As such, any loss of private keys due to a hack, employee or service provider misconduct or error, or other compromise by third parties could hurt our brand and reputation, result in significant losses, and adversely impact our business. The total value of crypto assets in our possession and control may be significantly greater than the total value of insurance coverage that would compensate us in the event of theft or other loss of funds, which could cause our business, operating results, and financial condition to be adversely impacted in the event of such uninsured loss.