

**PART E****RISK AND LEGAL DISCLAIMERS****E1 DISCLAIMERS**

- E1.1 The information provided on this whitepaper does not constitute investment advice, financial advice, trading advice, or any other sort of advice and you should not treat any of the website's content as such.
- E1.2 The NuGenesis team ( expressly defined as including any 'issuer', 'founder', 'miner', 'core developer' or any team member or seller of NuCoin to you) does not recommend that any cryptocurrency should be bought, sold, or held by you. Do conduct your own due diligence and consult your financial advisor before making any investment decisions. By purchasing NuCoin, you agree that:
- (a) you are not purchasing a security or investment and you agree to hold the team harmless and not liable for any losses or taxes you may incur.
  - (b) the team is presenting the native Coin "as is" and is not required to provide any support or services. You should have no expectation of any form from NuGenesis and its team. Although NuCoin is an EXPERIMENTAL Coin for social experiment and not a digital currency, the team strongly recommends that United States persons do not purchase it because the team cannot ensure compliance with United states regulations. Always make sure that you are in compliance with your local laws and regulations before you make any purchase.
- E1.3 Please note that there are risks associated with smart contracts. Please use at your own risk any NuGenesis technology. The NuGenesis team and any company groups are not registered financial advisers. Everything provided therein is for informational and educational purposes and we rely upon you using this material to seek and obtain such professional advice as you require. We expect that all information herein contained will be independently verified and confirmed. The NuGenesis teams and persons associated are not responsible for any losses or damages that may be suffered whatsoever or howsoever arising from any reliance on information herein contained. Any trading that you may do involves risks in any financial markets – the crypto markets are particularly immature, lack liquidity that you may be used to in traditional markets and involve a layer of additional technical risk. Do not invest or speculate and certainly not with money that you cannot afford to lose.
- E1.4 For the purposes of the forgoing discussion summarising and expanding on particular aspects of risks, "we" and "our" is used in the collective sense. That is, "our" platform means:
- (a) all participants in the platform including major component entities within it; and,
  - (b) the platform which you, as a prospective user of NuCoin, are a part and one which we are assuming and relying, to be an active participant therein.  
Likewise, "We" means all the community members and includes major component entities within it.



E1.5 We note again that no reader should be looking to any NuGenesis company as some sort of manager, promoter or controller for the success or otherwise of the platform. That will always be a function of the entirety of the collective community that adopts it, contributes to it and uses it.

## **E2 FURTHER DISCLAIMERS AND REITERATIONS REGARDING WHAT IS NuCOIN**

- E2.1 It cannot be over-emphasised that the nature of the NuGenesis blockchain ecosystem is protocol based social experiment. Within this ecosystem, NuCoin may be considered the equivalent of the Oil that runs system of organisation of business, social and personal relationships that given the infrastructure upon which to develop activity with open participation. The activity is not limited economic activity but is rather a digital, virtual society with all its facets.
- E2.2 The value of any NuCoin is a function of how it is adopted and utilised in the ecosphere of this virtual society including such collaborations and applications built upon and/or parachained or networked with NuGenesis, and with increased emphasis on virtual relationships and means of expression and exchange that will occur in virtual reality may be increasingly token-less.
- E2.3 NuCoin is not a security in that, on any acquisition of NuCoin or derivative thereof, you do not:
- (a) acquire or can expect to ever acquire a shareholding, legal, beneficial or membership stake in any equity of any investment vehicle expressly including any 'issuer', 'founder', 'miner', 'core developer' or any team member or seller of NuCoin to you whether separately or collectively ("the NuGenesis Team") howsoever and in any way;
  - (b) acquire or can expect to ever acquire any right to fees, income, dividends, bonus issues in a NuGenesis team person;
  - (c) acquire or can expect to ever acquire any to vote, direct, control or influence a NuGenesis team person;
  - (d) become an object or purpose of any foundation, trust or investment vehicle related to a NuGenesis team person; and,
  - (e) have any rights to payment in money or kind or compel the performance of work or provision of services by any NuGenesis team person.
- E2.4 If you acquire or utilise any NuCoin, you declare and any issuer', 'founder', 'miner', 'core developer' or any persons referred to as a NuGenesis team member or seller of NuCoin to you whether separately or collectively rely(ies) upon you acknowledging, declaring and understanding that by the act of acquisition or utilisation, that you:
- (a) do so for your own business and social use;
  - (b) do so fully cognisant that you do not rely upon the management or efforts of any counterparty howsoever but entirely your own active participation and efforts;



- (c) do not consider nor rely upon any representations express or through omission the financial or other history of any NuGenesis team member or associated entities to be relevant howsoever to your decision-making;
- (d) that the evolution of the NuGenesis ecosphere is a function of the participation of yourself and persons yet unknown to you that cannot be predicted or foreseen; and,
- (e) that a NuGenesis team member changes their position in reliance upon your acknowledgement, declaration and understanding.

E2.5 NuCoin will not be the exclusive cryptoasset used throughout the NuGenesis ecosystem. Separate tokens or Coins or digital assets may be created for 'Just Social', the NuGenesis Ledger X exchange, the V2R Launchpad or for any protocol that may be necessary or convenient in the development of the ecosphere including for example any 'rebase protocol' to adjust the liquidity and supply of NuCoin.

### **E3 SUMMARY OF RISK FACTORS**

E3.1 Any blockchain technology is subject to numerous risks and uncertainties. Some of these risks include:

- (a) price for NuCoin can significantly fluctuate due to the highly volatile nature of crypto.
- (b) the NuCoin price is substantially dependent on the prices of crypto assets generally and volume of transactions conducted on the platform.
- (c) A major indicator of market sentiment is derived from transactions in Bitcoin and Ethereum. If demand for these crypto assets declines and is not replaced by new crypto asset demand, the overall financial condition could be adversely affected.
- (d) 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, the financial condition could be adversely affected.
- (e) Cyberattacks and security breaches of the platform, or those impacting our customers or third parties, could adversely impact the brand and reputation and consequently financial condition.
- (f) 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 the platforms' brand, reputation and financial condition.
- (g) We operate in a highly competitive industry and we compete against unregulated companies and companies with greater financial and other resources, and the platform may be adversely affected if we, as a community, are unable to respond to our competitors effectively.



- (h) 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 regulators and governmental authorities.
- (i) We may continue be subject to material litigation, including individual and class action lawsuits, as well as investigations and enforcement actions by regulators and governmental authorities, which may adversely affect our financial condition.
- (j) If we cannot keep pace with rapid industry changes to provide new and innovative products and services, the use of our products and services and, consequently, our financial condition could be adversely impacted.
- (k) A particular crypto asset's status as a "security" in any relevant jurisdiction is subject to a high degree of uncertainty and if we are unable to properly characterize a crypto asset, we may be subject to regulatory scrutiny, investigations, fines, and other penalties, and our financial condition may be adversely affected.
- (l) 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 community's ability to support our community members.
- (m) Loss of a critical banking or insurance relationships could adversely impact our financial condition.
- (n) Any significant disruption in our products and services, in our information technology systems, or in any of the blockchain networks we support, could adversely impact our brand and reputation and financial condition.
- (o) Our failure to safeguard and manage our customers' fiat currencies and crypto assets could adversely impact our financial condition.
- (p) The loss or destruction of private keys required to access any crypto asset held in custody for our own account or for our community users 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.
- (q) None of our founders are party to any contractual lock-up agreement or other contractual restrictions on transfer. Following our listing, the sales or distribution of substantial amounts of NuCoin, or the perception that such sales or distributions might occur, could cause the market price of NuCoin to decline.

E3.2 Other risks that many of which are unpredictable and in certain instances are outside of our collective community control, include:



- (a) our dependence on projects 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;
- (b) our ability to attract, maintain, and grow our community base and engage our community members;
- (c) changes in the legislative or regulatory environment, or actions by governments or regulators, including fines, orders, or consent decrees;
- (d) regulatory changes that impact our ability to offer certain products or services;
- (e) our ability to diversify and grow our subscription and services;
- (f) pricing for our collectively offered products and services;
- (g) 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;
- (h) adding and removing of crypto assets on our platform;
- (i) macroeconomic conditions;
- (j) adverse legal proceedings or regulatory enforcement actions, judgments, settlements, or other legal proceeding and enforcement-related costs;
- (k) the development and introduction of existing and new products and services by our collective community or our competitors;
- (l) increases in operating expenses that we expect to incur to grow and expand our operations and to remain competitive;
- (m) system failure or outages, including with respect to our crypto platform and third-party crypto networks;
- (n) breaches of security or privacy;
- (o) inaccessibility of our platform due to our or third-party actions;
- (p) our ability to attract and retain talent;
- (q) our ability to compete with our competitors;
- (r) unpredictable social media coverage or “trending” of crypto assets;
- (s) the ability for crypto assets to meet user and investor demands;



- (t) the functionality and utility of crypto assets and their associated ecosystems and networks, including crypto assets designed for use in various applications;
- (u) consumer preferences and perceived value of crypto assets and crypto asset markets;
- (v) increased competition from other payment services or other crypto assets that exhibit better speed, security, scalability, or other characteristics;
- (w) regulatory or legislative changes and updates affecting the cryptoeconomy;
- (x) the characterisation of crypto assets under the laws of various jurisdictions around the world;
- (y) the maintenance, troubleshooting, and development of the blockchain networks underlying crypto assets, including by miners-stakers-validators, and developers worldwide;
- (z) the ability for crypto networks in our ecosystem to attract and retain miners or validators to secure and confirm transactions accurately and efficiently;
- (aa) ongoing technological viability and security of crypto assets and their associated smart contracts, applications and networks, including vulnerabilities against hacks and scalability;
- (bb) fees and speed associated with processing crypto asset transactions, including on the underlying blockchain networks and on crypto platforms;
- (cc) financial strength of market participants;
- (dd) the availability and cost of funding and capital;
- (ee) the liquidity of crypto platforms;
- (ff) interruptions in service from or failures of major crypto platforms;
- (gg) availability of an active derivatives market for various crypto assets, particularly in the traditional capital markets;
- (hh) availability of banking and payment services to support crypto-related projects;
- (ii) level of interest rates and inflation;
- (jj) monetary policies of governments, trade restrictions, and fiat currency devaluations; and,
- (kk) national and international economic and political conditions.

- E3.3 in addition to the factors impacting the broader cryptoeconomy, NuCoin may be adversely affected if the markets for Bitcoin and Ethereum deteriorate or if their prices decline, including as a result of the following factors:
- (a) the reduction in mining rewards of Bitcoin, including block reward halving events, which are events that occur after a specific period of time which reduces the block reward earned by miners;
  - (b) the development and launch timeline of Ethereum 2.0, including the potential migration of Ethereum to a proof-of-stake model;
  - (c) disruptions, hacks, splits in the underlying network in our ecosystem also known as “forks”, attacks by malicious actors who control a significant portion of the networks’ hash rate such as double spend or 51% attacks, or other similar incidents affecting the Bitcoin or Ethereum blockchain networks;
  - (d) hard “forks” resulting in the creation of and divergence into multiple separate networks, such as Bitcoin Cash and Ethereum Classic in our ecosystem;
  - (e) informal governance led by Bitcoin and Ethereum’s core developers that lead to revisions to the underlying source code or inactions that prevent network scaling, and which evolve over time largely based on self-determined participation, which may result in new changes or updates that affect their speed, security, usability, or value;
  - (f) the ability for Bitcoin and Ethereum blockchain networks to resolve significant scaling challenges and increase the volume and speed of transactions;
  - (g) the ability to attract and retain developers and customers to use Bitcoin and Ethereum for payment, store of value, unit of accounting, and other intended uses;
  - (h) transaction congestion and fees associated with processing transactions on the Bitcoin and Ethereum networks;
  - (i) the identification of Satoshi Nakamoto, the pseudonymous person or persons who developed Bitcoin, or the transfer of Satoshi’s Bitcoins;
  - (j) negative perception of Bitcoin or Ethereum;
  - (k) development in mathematics, technology, including in digital computing, algebraic geometry, and quantum computing that could result in the cryptography being used by Bitcoin and Ethereum becoming insecure or ineffective; and
  - (l) laws and regulations affecting the Bitcoin and Ethereum networks or access to these networks, including a determination that either Bitcoin or Ethereum constitutes a security or other regulated financial instrument under the laws of any jurisdiction.



- E3.4 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 financial condition could be adversely affected.
- E3.5 Crypto assets built on blockchain technology were only introduced in 2009 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 decentralised 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:
- (a) 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.
  - (b) 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.
  - (c) 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.
  - (d) 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.
  - (e) 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.





- (f) 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.
  - (g) 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.
  - (h) 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.
  - (i) 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.
- E3.6 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 materialise, 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.
- E3.7 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.
- E3.8 Our collective Platform 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. Indeed it is a legal requirement for KYC/AML purposes. The platform's reputation will be built 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:
- (a) harm our reputation and brand;
  - (b) result in our systems or services being unavailable and interrupt our operations;
  - (c) result in improper disclosure of data and violations of applicable privacy and other laws;
  - (d) result in significant regulatory scrutiny, investigations, fines, penalties, and other legal, regulatory, and financial exposure;

- (e) cause us to incur significant remediation costs;
- (f) lead to theft or irretrievable loss of our or our customers' fiat currencies or crypto assets;
- (g) reduce customer confidence in, or decreased use of, our products and services;
- (h) divert the attention of management from the operation of our business;
- (i) 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
- (j) adversely affect our business and operating results.

- E3.9 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.
- E3.10 An increasing number of organisations, 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.
- E3.11 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 organised 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.
- E3.12 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. Unauthorised parties may 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 community members' crypto assets. Threats can come from a variety of sources, including criminal hackers, hackers, 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, or 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.

- E3.13 If we cannot keep pace with rapid industry changes to provide new and innovative products and services, the use of our products and services, and consequently could adversely impact our financial condition.
- E3.14 Our industry has been characterised by many rapid, significant, and disruptive products and services in recent years. These include decentralised applications, DeFi, yield farming, staking, token wrapping, governance tokens, innovative programs to attract customers such as transaction fee mining programs, initiatives to attract traders such as trading competitions, airdrops and giveaways, staking reward programs, and novel cryptocurrency fundraising and distribution schemes, such as "initial exchange offerings." We expect new services and technologies to continue to emerge and evolve, which may be superior to, or render obsolete, the products and services that we, collectively, can provide. We cannot predict the effects of new services and technologies on our community platform. However, our ability to grow our member base and net revenue will depend heavily on our ability to innovate and create successful new products and services, both independently and in conjunction with third-party developers. In particular, developing and incorporating new products and services into our business may require substantial expenditures, take considerable time, and ultimately may not be successful. Any new products or services could fail to attract customers, generate revenue, or perform or integrate well with third-party applications and platforms. In addition, our ability to adapt and compete with new products and services may be inhibited by regulatory requirements and general uncertainty in the law, constraints by our banking partners and payment processors, third-party intellectual property rights, or other factors. Moreover, we must continue to enhance our technical infrastructure and other technology offerings to remain competitive and maintain a platform that has the required functionality, performance, capacity, security, and speed to attract and retain customers, including large, institutional, high-frequency and high-volume traders. As a result, we expect to expend significant costs and expenses to develop and upgrade our technical infrastructure to meet the evolving needs of the industry. Our success will depend on our ability to develop and incorporate new offerings and adapt to technological changes and evolving industry practices. If we are unable to do so in a timely or cost-effective manner, our platform and our ability to successfully compete, to retain members, and to attract new members may be adversely affected.



**E4: Unfavourable media coverage could negatively affect our business.**

We can expect to receive a high degree of media coverage in the cryptoeconomy and around the world. Unfavourable publicity regarding, for example, our product changes, product quality, litigation or regulatory activity, privacy practices, terms of service, employment matters, the use of our products, services, or supported crypto assets for illicit or objectionable ends, the actions of our customers, or the actions of other companies that provide similar services to ours, has in the past, and could in the future, adversely affect our reputation. We have stress-tested our blockchain, its on-ramps and off-ramps with a number of ‘black hats’ and those expert in identifying hacks, loopholes and defects generally. Any of these people may find themselves in the media and an association may be drawn with our platform. Further, we may in the future, be the target of social media campaigns criticizing actual or perceived actions or inactions that are disfavoured by our customers, employees, or society at-large, which campaigns could materially impact our customers’ decisions to trade on our platform. Any such negative publicity could have an adverse effect on the size, activity, and loyalty of our customers and result in a decrease in net revenue, which could adversely affect our business, operating results, and financial condition.



## **E5: SPECIFIC RISK FACTORS EXPANDED UPON**

- E5.1 ***Our intellectual property rights are valuable, and any inability to protect them could adversely impact our business, operating results, and financial condition.***
- E5.2 Our platform's business activity depends in large part on our collective proprietary technology and our brand. We expect to rely on, a combination of trademark, domain name, copyright, and trade secret and laws, as well as confidentiality and licence agreements with our employees, contractors, consultants, and third parties with whom we have relationships, to establish and protect our brand and other intellectual property rights. However, our efforts to protect our intellectual property rights may not be sufficient or effective. Our proprietary technology and trade secrets could be lost through misappropriation or breach of our confidentiality and licence agreements, and any of our intellectual property rights may be challenged, which could result in them being narrowed in scope or declared invalid or unenforceable. There can be no assurance that our intellectual property rights will be sufficient to protect against others offering products, services, or technologies that are substantially similar to ours and that compete with our platform.
- E5.3 Subject to consensus change, the current view is that the platform does not intend to monetise our intellectual property rights or attempt to block third parties from competing with the platform by asserting our patents offensively against third parties, but our ability to successfully defend intellectual property challenges from competitors and other parties may depend, in part, on our ability to counter-assert our patents defensively. Effective protection of patents, trademarks, and domain names is expensive and difficult to maintain, both in terms of application and registration costs as well as the costs of defending and enforcing those rights. Further, intellectual property protection may not be available to us in every country in which our products and services are available. For example, some foreign countries have compulsory licensing laws under which a patent owner must grant licences to third parties. In addition, many countries limit the enforceability of patents against certain third parties, including government agencies or government contractors. In these countries, patents may provide limited or no benefit. We may also agree to license our patents to third parties as part of various patent pools and open patent projects. Those licenses may diminish our ability, though, to counter-assert our patents against certain parties that may bring claims against us.
- E5.4 We may be, sued by third parties for alleged infringement of their proprietary rights however unfounded.
- E5.5 In recent years, there has been considerable patent, copyright, trademark, domain name, trade secret and other intellectual property development activity in the cryptoeconomy, as well as litigation, based on allegations of infringement or other violations of intellectual property, including by large financial institutions. Furthermore, individuals and groups can purchase patents and other intellectual property assets for the purpose of making claims of infringement to extract settlements and some important parts of our network may be attacked. Our use of third-party intellectual property rights also may be subject to claims of infringement or misappropriation. Whilst we predominantly use our own developed software, we cannot guarantee that our internally developed or acquired technologies and content do not or will not infringe the intellectual property rights of others. From time to time, our competitors or other third parties may claim that we are infringing upon or

misappropriating their intellectual property rights, and some parts of our network may be found to be infringing upon such rights. Any claims or litigation could cause us to incur significant expenses and, if successfully asserted against major parts of our network, could require that we pay substantial damages or ongoing royalty payments, prevent us from offering our products or services or using certain technologies, force us to implement expensive work-arounds, or impose other unfavourable terms. We expect that the occurrence of infringement claims is likely to grow as the crypto assets market grows and matures. Accordingly, our exposure to damages resulting from infringement claims could increase and this could further exhaust our financial and management resources.

- E5.6 We may be adversely affected by natural disasters, pandemics, and other catastrophic events, and by man-made problems such as terrorism, that could disrupt our platforms' business operations, and our business continuity and disaster recovery plans may not adequately protect us from a serious disaster.
- E5.7 Natural disasters or other catastrophic events may also cause damage or disruption to our operations, international commerce, and the global economy, and could have an adverse effect on our business, operating results, and financial condition. Our platform's operations are subject to interruption by natural disasters, fire, power shortages, and other events beyond our control. In addition, our global operations expose us to risks associated with public health crises, such as pandemics and epidemics, which could harm our business and cause our operating results to suffer. For example, the ongoing effects of the COVID-19 pandemic and/or the precautionary measures that we have adopted have resulted, and could continue to result, in difficulties or changes to our customer support, or create operational or other challenges, any of which could adversely impact our platforms' business activity. Further, acts of terrorism, labour activism or unrest, and other geo-political unrest could cause disruptions in our platform's business or the businesses of our partners or the economy as a whole. In the event of a natural disaster, including a major earthquake, blizzard, or hurricane, or a catastrophic event such as a fire, power loss, or telecommunications failure, we may be unable to continue our operations and may endure system interruptions, reputational harm, delays in development of our platform, lengthy interruptions in service, breaches of data security, and loss of critical data, all of which could have an adverse effect on the business activity done on our platform.