CONTENT

1. INTRODUCTION

The purpose of the document is to provide information about the Cybercoinium cryptocurrency, its use in Blockchain, main conceptual idea, functional model, competitive advantages, project team, ICO details and roadmap for updating our project map. Soon, a more detailed description of the kernel architecture will be introduced. After sealing the original concept in a gift presentation, we tirelessly turned to the interested partners and organically built our team. Along this path we have found excellent partners and mentors who are interested and pleased to work with the precise tuning of our vision and refinement of our offer in the market. Approaching the ITO stage now, we thank all those who supported us and hope to exceed the expectations of the community in the future.
This technical paper will be published on an indefinite day, in its current version, and we recommend you periodically update information on our website and other multimedia channels for new information and updates.

1.1 The concept and social significance of the project

The Cybercoinium project implements open source software that allows you to connect and fully control personal or corporate workflow. The program provides full tracking of all the changes occurring in the files and can be used as a super secure storage of your data based on the Blockchain technology. You can independently write in the smart-policy the repository functionality, with a detailed indication of what actions with respect to your files should be identified as undesirable or prohibited, as the system will immediately signal the owner.
The second important project component is the creation of a blacklist for stolen purses, or for the addresses assisted the funds theft operations. All wallets associated with the stolen funds will be automatically added to the blacklist, until the funds return to the victim's purse. This function is introduced on a non-commercial basis and has the objective to improve the working conditions of the blocking community and the development of payments in the crypto industry. For more details check section 3.

1.2 Modern market issues

- Risks of hacking and loss of personal data

Data irregularities and loss is one of the most common and costly issues that organizations of any level face daily. The modern business system is structured for daily data transfer between business networks. Questions according

whether these data communications are secured were raised. Recent studies conducted by IBM and the Ponemon Institute have shown many companies and organizations have suffered from data breaches more than 17,000 times a year. Most of these violations led to a significant data leakage, which led to a decrease in productivity, a decrease in consumer confidence, trust and increased costs associated with the organization's response. Due to the growing number of security threats, data loss and data leakage in the workplace have become a serious problem for many companies and small businesses.

Organizations must exchange data for activities related to business both inside and outside. Ability to steal data and abuse increases. Therefore, organizations can use the capabilities of a distributed book, known as a chain of blocks, to prevent and protect the data of a confidential organization. Companies must share confidential data with both business units within the organization and with third-party service providers outside. Data can be sent via Email through a cloud storage or file-sharing service or even using a flash drive. It can contain confidential information that is downloaded from the service to meet the needs of the business or organization. However, just think a minute. As soon as the information leaves the organization, desktop or main data processing system, it is not protected and can be easily sent to an unauthorized recipient accidentally or stolen during a security breach or can be sent deliberately for misuse.

- Unscrambled turnover of crypto assets assigned by fraud.

A new trend in the field of cybercrime was the massive theft of cryptocurrencies from users' wallets. To date, this is a global problem for the entire cryptocommunity. In addition to professional hackers, taking away hundreds of millions of coins from exchange purses, there are many different options to assign your assets. To defraud cryptocurrency, the following methods are used: fake purses creation, phishing, fraudulent ICO, creation of a false cryptocurrency, financial pyramids and extortion programs.
Statistics of crimes involving cryptocurrency is increasing daily. In general, it is possible to note the largest thefts, such as theft of Mt.Gox in the amount of 740,000 BTC, the crack of Bitfinex Exchange with a loss of 120,000 Bitcoins in 2016, the robbery of Bitstamp and BitFloor for a total of 43,000 BTC. This is data without considering hundreds of less high-profile cases. For example, according to the statistics of the Chainalysis analytical agency, 10% of all funds invested in the air flowed into the hands of hackers.

In general, initially the theft of cryptocurrency increased due to the principles of cryptocurrency anonymity,. In contrast to the traditionally abducted funds, «money laundering» is not required, it is enough simply to bring them to the philanthropy through specialized exchange offices, or continue to wrap up in crypto-economics. The Cybercoinium project offers a solution to this problem by providing the cryptocommunity with a decentralized tool for creating a single database of stolen or involved in the circulation of stolen wallet funds. Due to the implementation of fraudulent addresses to a single register, the so-called blacklist, cybercriminals will face a significant obstacle and the inability to manage stolen assets.

2. SECURE DECENTRALIZED FILE STORAGE

«Cybercoinium File Storage» is a decentralized file storage that allows you to safely store and track all changes and activities of users in your documents, through the fact that all such events are recorded in the locker.
An important system advantage will be the smart policies tool, which will allow creating custom scenarios of automatic events that will be executed in case of important or unwanted changes in stored documents.
Smart Policies are scripts that send you notifications every time a file uploaded is viewed, or modified. They run actions, such as e-mailing to someone, rollback of changes or the completion of system processes (for servers).

To store large files (video / audio / photo content), not only text documents, a system to store files on decentralized servers encrypted and divided into different parts for storage will be developed (the hardware owners cannot be accessed to files) and files describing the network of servers on which the content will be stored will also be encoded and the hashes of these files will be stored in the blockchain and connected to alerts from Smart Policies.

Data storage is built on the basis of the Merkle trees. It can significantly increase the work speed and the amount of stored information about files, and (important in the long term) to reduce the requirements for the performance of processing systems.

Merkle trees aka «hash-trees» are known for a long time, their concept was patented by Ralph Merkle in 1979. This is a special data structure containing summary information about some large data amount which can be used for their verification. In this case, the set of information can be diverse: you can store any necessary data about the file, whether it’s size, creation date or something else.

Thus, it is clear the data structure has a tree-like form, at the nodes of which there are hashes created on the basis of data from other, lower-level nodes. At the end, root hashes added to the blockchain are formed,.
We use a binary structure in which each parent hash consists of two child hashes. If we imagine this in the scheme form, we get the following:

One of the main properties of the Merkle tree is knowing data 1, hash 2, hash 02 and hash 001, you can confirm the data authenticity data 1, even if the rest of the data is not known. This means if you put a file in Acronis Notary or sign a document using Acronis ASign, then give someone from your friends / colleagues only a hash of the source file (hash 1), a «branch» with hashes from hash 1 to the root hash (hash 001) and root hash (this structure is called «Merkle's proof»), then the friend / colleague can easily check whether the file is now in the repository or not.

For Smart Policies, a set of smart contracts to manage files will be created. The possibility of obtaining paid access to copyright content will be developed.
With its help, you can check the authenticity of the data stored in the backup. For example, musicians or artists can confirm the date and time of creating their works, providing as evidence the certificate Cybercoinium with this information, along with metadata about the work itself.

In addition, a smart contract for the storage of «personal data» as an international certificate to avoid problems associated with the theft of certain documents with personal data in order to counterfeit and steal your identity will be developed.
A separate set of smart contract templates will be developed to enable users to create copies of official documents confirming sales transactions, so that in the future they can not be challenged.

The «Signature Certificate» contains the following information:
- The document name that you signed and placed in the repository, for example, «Purchase Agreement No. 1»;
- Signing date;
- Document size;
- Hash or «checksum» of the document;
- Current status;
- Information about signers;
- Signature.

The detachment will contain a detailed history of events that occurred with the document (creation, sending to signers, signing), including timestamps and IP-addresses of signatories. It is necessary the delivered electronic signature comply with the requirements of the international «Electronic Signature Law» and be recognized in court.
The way to confirm the special file given to you is authentic and, accordingly, confirms the authenticity of the contract is its download to the verification page of Cybeconium File Storage.

The next step of the project will be the status of «legal recognition» in various countries with the possibility of electronic signing of backup copies of documents with automatic notarization. The user simply uploads the signed documents to the decentralized Cybercoinium cloud storage file and sends out electronic invitations to other signers. Each signer enters the cloud and, using a special interface, and stamps the document. Thus, a kind of agreement between the parties, automatically fixed in the detachment is signed, so that further transactions for the purchase and sale of the asset established on the platform could be carried out exclusively within the framework of the Cybercoinium platform and did not require further verification in the paperwork.

2.1 Basic types of stored documents

- Secret files, such as: sets of passwords, mnemonic phrases, storing secret documents / files that cannot be deleted any way, or changed after uploading to a blockchain system and other purposes;
- Logs of the system generated and written by the server equipment with the exclusive right to read and without the possibility of their further removal;
- System files for setting and executing tasks, control and accounting of goods, trade balances.

Files for working with the distribution system and copyrights' control, taking into account all the changes introduced by roles;

- Files of correspondence from messengers, chat rooms, sms messages, emails, for connection of which a specialized API will be developed.

2.2 Control Capabilities and User Policies

- Ability to reset changes in files back to the initial state. Allows to avoid undesirable changes and accidental content loss in stored and processed documents;
- Live backup allows you to store an incremental backup of all important data without fear of losing it in case of unforeseen circumstances, or interference from third parties;
- The ability to store information in several different blockchains for the most important impossible to lose documents;
- Alerts and control of the entire incoming and outgoing messages' history in your applications and the creation of security events (automatic password change) in applications such as: Slack, Trello, Dropbox, Twitter, Wechat, Gmail, CRM systems etc;
- The push notifications system in the form of sms / e-mail / messenger messages, which allows you to receive instant notifications, each time your monitored files are changed or viewed;
- Automatic shutdown allows you to automatically complete the entire system closing, or parts thereof;
- Custom scripts. Through the provided API and documentation, users will also be able to create, share and promote their own security policies. Within the platform framework, a market place will be created, allowing to distribute such scripts in a paid or free format.

3. DECENTRALIZED MANAGED BLACKLIST ON BLOCKCHAIN

The purpose of the system is reducing the activity of hackers and scammers and the subsequent possibility elimination of selling and using stolen cryptocurrencies through the collective participation and joint support of this users' movement - cryptocurrency holders whose transaction history is open.

The system principle is that after the application for stolen funds from the past KYC procedure user appears in the system, the wallet falls into the blacklist. From this moment, any transactions to other wallets automatically make the following purse-recipients compromised and automatically fall into the blacklist. The only option to remove the purse from the blacklist is to organize the return of the received transaction amount to the wallet through which you received such a transaction.

To the extent the transaction has come to you for the service rendered, or the goods sold, you can create a return request, as well as having previously passed the KYC procedure and the materials on your dispute with the sender will be sent to the appropriate authorized body to find out all the circumstances. For this period, your wallet will be added to the «gray list», which means that if after the following transaction-sending the amount on your balance sheet becomes less than the amount specified in the dispute - your account will be automatically moved to the blacklist.

Our project and followers teams will be engaged in the project development, the agreements with all exchanges, official purses, services for converting cryptocurrency into a fiat will be sent out that they will not accept transactions from purses in the «black list» and will return all such incoming transactions automatically, in the case of receiving those to their address, so that their address was not entered in the blacklist and their data were not transferred to the fraud investigation authorities in the crypto currency market who received real personal data of the final recipient will be able to easily track the chain of persons who carried out these transactions up to the swindler, or a person knowingly aware of the origin of the funds and still bought in a darknet a cryptocurrency from such a fraudster. In this case, the person who received such an asset on his account is equated with an accomplice in the crime.

In order to avoid «spam» mailings and apply for entry in the blacklist at the time of the system start, such applications are accepted for transactions that exceed the amount equivalent to 1000 US dollars at the time of such a transaction. In the future, if possible, this figure will be reduced to a minimum.

How to become a participant of the «goodwill» project:

a) You are an individual:

1. All users who want to secure their wallets created in Blockchain with an open transaction history (wallets and transfer amounts public data) on the «Cybercoinium File Storage» decentralized secure data storage service will be offered passing KYC (Know Your Client) procedure.

2. Optionally, install our API or start using the Cybercoinium wallet to automatically reject all transactions from the purse in the blacklist;

b) You are a service representative, or the seller of the goods:

1. Undergo the KYC procedure.
2. Setup our API / purse to automatically reject all transactions from purses in the blacklist;
3. Get the opportunity to put on your site / application the logo of the project «goodwill Blockchain» with the phrase «I support the goodwill Blockchain.»

Opportunities for the service users:

1. Possibility of checking the purse of the cryptocurrency potential sender for being in the blacklist.
2. Ability to remove your purse from the blacklist by sending back the received amount of cryptocurrency from the purse in the blacklist
3. In the event that a transaction was sent from your wallet unauthorized to the purse of another user, after passing the KYC procedure (if the first one was not performed), you can leave an official statement by putting such a statement in Cybercoinium File Storage.
4. In the event of malicious deception in order to return the funds paid for the goods / service by the sender, give an answer and transfer these materials to the judicial authorities independently.
5. Provide the authorized body decision details on the dispute resolution.

4. BLOCKCHAIN TECHNOLOGY APPLICATION

Blockchain technology can protect files in all distributed book algorithms. Distributed book is essentially an asset database that can be transferred across a network from several sites, geographic regions or institutions. All network members can have their own identicalbook copy. Any changes in the register are reflected in all copies immediately. This technology is based on the blockchain, which was invented to create the peer-to-peer digital money system in 2008. Blockchain algorithms allow you to aggregate Bitcoin transactions in a Blockchain, and they are added to the «chain» of existing blocks using a cryptographic signature. Cryptographic digital signatures use public-key algorithms to ensure data integrity. When you sign the data with a

digital signature, someone else can verify the signature and can prove the data has arisen from you and was not changed after it was signed. The «Bitcoin» book is built on the principle of «distributed» and «less», so anyone can add a block of transactions if they can solve a new cryptographic puzzle to add each new block. The incentive for this is that at present the bitcoins form awarded to the puzzle solver for each «block» is rewarded. Anyone who has access to the Internet and the processing power to solve cryptographic puzzles can add to the register and they are known as «Bitcoin miners».
A mountain analogy is appropriate, because the Bitcoin mining process is energy intensive, as it requires very large processing power. It was estimated that the energy requirements for running bitcoins exceed 1 gigabyte.
The document owner can automatically force who can view the file, what he can do with the file (edit, print, shoot the screen, etc.), From which device and for how long. Access to information and files can be canceled in real time even after distribution. In fact, you can set automatic expiration of access to information about data to third parties after the set date.

5. CBR TOKEN

The CBR token is an internal destination currency. The token will be released on the Stellar blockchain and will have all the advantages associated with this network, which has already proved itself to be fast, reliable and low-cost. Also, the main advantages of Stellar are:

- Simplicity of money transfers - users of the Stellar network can link their wallet address to the account ID. This service is implemented in the Ethereum network and is called ENS, but unlike the Ether, Stellar is completely free.

- Transaction security - Stellar's blocking system provides security by restricting the access of unreliable users.

- Liquidity of network tokens - the Stellar platform has its own decentralized exchange, integrated into the platform. This suggests the tokens created on the Stellar blockchain can be traded on this exchange already on the first day.

- The Stellar platform goal is to provide users with the latest innovative solutions from the world of blockchain and fintech. While other blockchain startups take years to solve today's problems, the Stellar platform already offers a ready-made high-performance solution.

- The high level of creators' competence - the Stellar team enlisted the support of the best specialists in the field of cryptoeconomics, fiintech and security. Co-founder Jed McCaleb was building p2p file exchanges, created the first Bitcoin-Exchange, and is also a co-founder of Ripple. The list of the rest of the

team includes such pioneers of blockchain technology as Greg Brockman, Sam Altman, Dan Kaminski, Patrick Collison, Keith Rabua and many others.

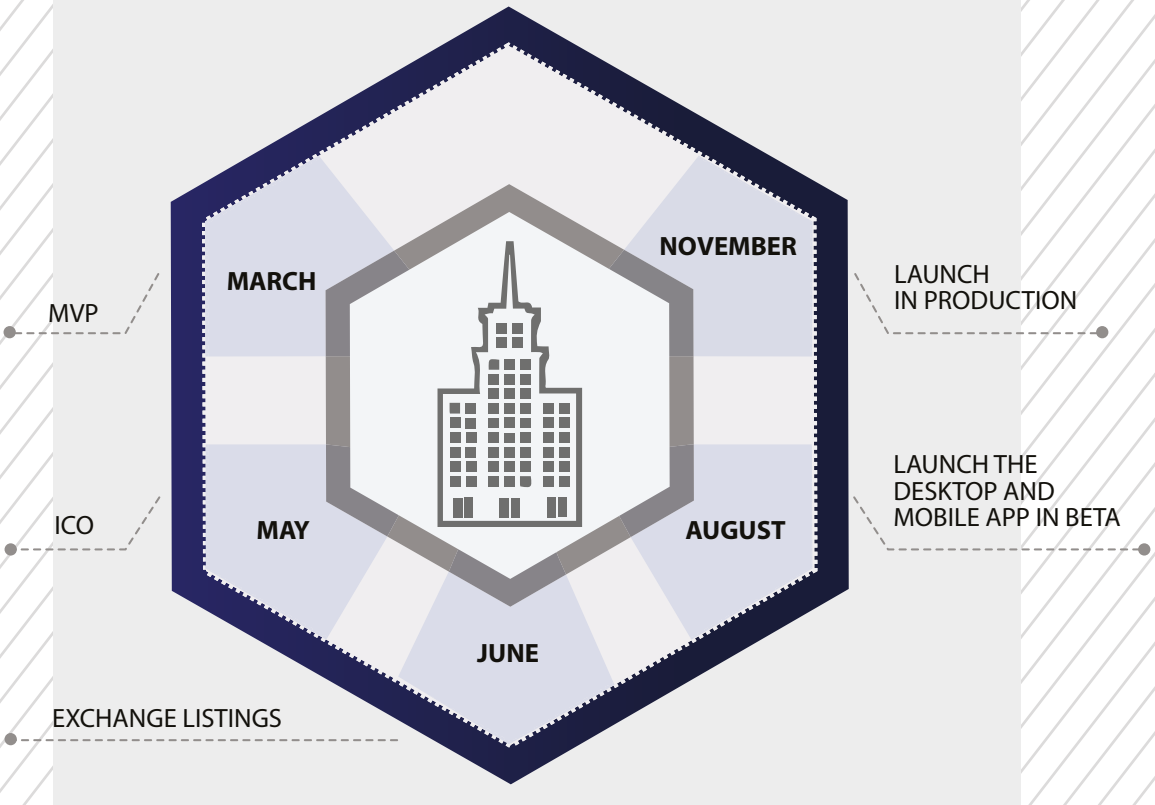
5.1 ITO Cybercoinium details

ITO is held to raise funds for the promotion and development of Cybercoinium software. A total of 180 million CBR-tokens will be issued. At the presale stage, the planned amount of the fee should be $ 2 million. During the ITO, Cap is equal to $ 10 million. All unsold tokens will be destroyed. The dates and details of the ITO will be updated during the further project preparation.

5.2 Token distribution general structure

ITO will be held in two stages, following the results of the first round, work will be carried out on the commercial part of the project idea, upon completion, the second stage will be launched, after the fundraising at which the team will begin to develop a decentralized managed blacklist on the detachment. 16% of the total issue of CBR tokens will be reserved for the team, partners and the fund of loyalty programs, another 2% goes to the bounty program and 8% to the advisory board. 65% is distributed among investors through ITO, 3% goes to the referral program, 6% goes to the project fund for further implementation for marketing tasks and project promotion.

6. PROJECT ROADMAP



Roadmap for the implementation of a decentralized managed blacklist

30-day roadmap:
1. Shift to production environment with redundancy, load balancing and trivial scalability

2. Drill down into transfers between clusters using the transactions view. This will allow the user to see transaction by transaction what funds were sent between two entities. There will be both a table view and a time series histogram of the entire transfer history to allow for the user to see how the flows to and from each cluster have changed over time. The histogram will also provide the user with the ability to focus on a particular time

3. Organization / User separation of privileges:
a. Charts are per user
b. Names are per organization
c. Introduction of Tags (also on organizational level) - check below

4. Introduce category tags. This is where we can expose certain services as being a certain type of entity on the Bitcoin network, i.e. Payment processors, dark markets, gambling sites, etc. These types of tags will be included in the GUI as well as offering easy to integrate API support

5.Ability to search by transaction hash, cluster name, category etc. This will allow for faster investigations via known clusters of interest but also for the API to answer specific questions about transactions or entities of interest. Part of this also allows for easier integrations through the API with the ability to support transaction hash lookups.

6.Ability to merge and split clusters as a user sees fit and for these to be stored in their account. Will make investigations easier and improve the accuracy of any API calls that are made using that user account.

60-day roadmap:
1. Unconfirmed transactions support through the API. Currently customers need to parse transactions and submit the address from the inputs of the transaction to the API to get a response. With a mempool of unconfirmed transactions the user will only need to pass the transactions hash through the API. Clustering over unconfirmed transactions will take place in real time.

2. Shared multi client repositories for known bad actor reporting as well as for subscribers own addresses enabling 0-risk 0-conf transactions as well as enabling travel rule checks.

3. CSV exports of all data.

4. Macro support: Macros enable automated / guided merges of clusters as well as creation of investigation graphs for funds flow / origin. These allow the

user to specify certain parameters such as only looking at min flow / max flow, specific entities or size of transfers to recreate a graph to look further into an investigation. This will also feed into the accuracy and precision of API calls as users can store the results from this analysis.

5. Profiling API improvements
a. Min / Max flow
b. Country of Origin for a transaction
c. ToR / VPN

6. Addition of more intelligence sources and presentation of origin of intelligence and references.
90-day roadmap:

1. Creation of more macros based on user feedback and data

2. Transaction groups / sub transfer view enabling clear visualization of automated investigations with flow of funds etc.

3. User permission graduation (can assign (group) names, can merge, can assign tags, can view
180-day roadmap:
Also, our professional project team will develop and design the following applications under the

Cybercoinium platform:
- Cybercoinium website
- Cybercoinium Windows Application
- Android/MacOS/Windows Phone application.

7. PROJECT TEAM

VLADIMIR LIALINE
Creator of Cybercoinium
Blockchain Powered Cybersecurity, Bitcoin Mining Hosting and Hardware, Blockchain Development

STEVEN GEHRMAN
Stellar and Stellar ICO advisor
Founder and software engineer behind popular independent Mac software firm Cocoatech. I'm the creator of app «Path Finder» for OS X.

ZAKARIA GEORGE
Senior Developer
Full stack web & mobile developer. Love travel, reading and soccer.

AMIT SHEVKAR
UI/UX Designer
Web designer of cybercoinium. Love to design website.

8. TERMS AND PROVISIONS

All statements contained in this White paper, statements made in press releases or in any place accessible by the public and oral statements that may be made by Cybercoinium or their respective directors, advisors, executive officers or employees acting on behalf of Cybercoinium, that are not statements of historical fact, constitute “forward looking statements”. Some of these statements can be identified by forward-looking terms such as “aim”, “target”, “anticipate”, “believe”, “could”,“estimate”, “expect”, “if”, “intend”, “may”, “plan”, “possible”, “probable”, “project”, “should”, “would”, “will” or other similar terms. However, these terms are not the exclusive means of identifying forward-looking statements. All statements regarding Cybercoinium financial position, business strategies, plans and prospects and the future prospects of the industry which Cybercoinium is in are forward-looking statements. These forward-looking statements, including but not limited to statements as to Cybercoinium’s revenue and profitability, prospects, future plans, other expected industry trends and other matters discussed in this White Paper regarding Cybercoinium are matters that are not historic facts, but only predictions. These forward-looking statements involve known and unknown risks, uncertainties and other factors that may cause the actual future results, performance or achievements of Cybercoinium to be materially different from any future results, performance or achievements expected, expressed or implied by such forward-looking statements. These factors include, amongst others: (a) changes in political, social, economic and stock or cryptocurrency market conditions, and the regulatory environment in the countries in Cybercoinium conducts its respective operations; (b) the risk that Cybercoinium may be unable or execute or implement their respective strategies and future plans; (c) changes in interest rates and exchange rates of fiat currencies and cryptocurrencies; (d) changes in the anticipated growth strategies and expected internal growth of Cybercoinium; (e) changes in the availability and fees payable to Cybercoinium in connection with their respective businesses and operations; (f) changes in the availability and salaries of employees who are required by Cybercoinium to operate their respective businesses and operations; (g) changes in preferences of participants of Cybercoinium; (h) changes in the future capital needs of Cybercoinium and the availability of financing and capital to fund such needs; (i) war or acts of international or domestic terrorism; (j) occurrences of catastrophic events, natural disasters that affect operations of Cybercoinium; (k) other factors beyond the control of Cybercoinium; and (l) any risk and uncertainties associated with Cybercoinium and its businesses and operations, including the tokens.

9. LEGAL POLICY

The Cybercoinium does not have the legal qualification of a security, since it does not give any rights to dividends or interests. The sale of Cybercoinium is final and non-refundable. Cybercoinium are not shares and do not give any right to participate to the general meeting of Cybercoinium board of director. Cybercoinium cannot have a performance or a particular value outside the Cybercoinium Platform. Cybercoinium shall therefore not be used or purchased for speculative or investment purposes. The purchaser of Cybercoinium is aware that national securities laws, which ensure that investors are sold investments that include all the proper disclosures and are subject to regulatory scrutiny for the investors' protection, are not applicable. Anyone purchasing Cybercoinium expressly acknowledges and represents that she/he has carefully reviewed this white paper and fully understands the risks, costs and benefits associated with the purchase of Cybercoinium.

The purchaser of Cybercoinium undertakes that she/he understands and has significant experience of cryptocurrencies, blockchain systems and services, and that she/he fully understands the risks associated with this as well as the mechanism related to the use of cryptocurrencies (incl. storage). Cybercoinium shall not be responsible for any loss of Cybercoinium or situations making it impossible to access Cybercoinium, which may result from any actions or omissions of the user or any person undertaking to acquire Cybercoinium as well as in case of hacker attacks.

9.1 Risks' assessment

Acquiring Cybercoinium and storing them involves various risks, in particular the risk that Cybercoinium may not be able to launch its operations and develop its blockchain and provide the services promised. Therefore, and prior to acquiring Cybercoinium, any user should carefully consider the risks, costs and benefits of acquiring Cybercoinium in the context of this whitepaper and, if necessary, obtain any independent advice in this regard. Any interested person who is not in the position to accept or to understand the risks associated with the activity (incl. the risks related to the non-development of the Cybercoinium platform) or any other risks as indicated in this Terms & Conditions should not acquire Cybercoinium.

9.2 Rights and warranties of the token holders

By participating, the purchaser agrees to the above and in particular, they represent and warrant that they:

- have read carefully the terms and conditions attached to the white paper; agree to their full contents and accept to be legally bound by them;
- are authorized and have full power to purchase Cybercoinium according to the laws that apply in their jurisdiction of domicile;

- live in a jurisdiction which allows Cybercoinium to sell Cybercoinium through a without requiring any local authorization;
- are familiar with all related regulations in the specific jurisdiction in which they are based and that purchasing cryptographic coins in that jurisdiction is not prohibited, restricted or subject to additional conditions of any kind;
- will not use Cybercoinium for any illegal activity, including but not limited to money laundering and the financing of terrorism;
- have sufficient knowledge about the nature of the cryptographic coins and have significant experience with, and functional understanding of, the usage and intricacies of dealing with cryptographic coins and currencies and blockchain-based systems and services;
- purchase Cybercoinium because they wish to have access to the Cybercoinium platform.

10. WARNING OF RESPONSIBILITY OBSCURATION

This white paper shall not and cannot be considered as an invitation to enter into an investment. It does not constitute or relate in any way nor should it be considered as an offering of securities in any jurisdiction. This white paper does not include or contain any information or indication that might be considered as a recommendation or that might be used as a basis for any investment decision. Cybercoinium are just utility tokens which can be used only on the Cybercoinium platform and are not intended to be used as an investment. The offering of Cybercoinium on a trading platform is done in order to allow the use of the Cybercoinium platform and not for speculative purposes.The offering of Cybercoinium tokens on a trading platform does not change the legal qualification of the tokens, which remain a simple means for the use of the Cybercoinium platform and are not a security. Cybercoinium is not to be considered as an advisor in any legal, tax or financial matters. Any information in the white paper is provided for general information purposes only and Cybercoinium does not provide any warranty as to the accuracy and completeness of this information. Cybercoinium is not a financial intermediary according to Swiss law and is not required to obtain any authorization for Anti Money Laundering purposes. Acquiring Cybercoinium shall not grant any right or influence over Cybercoinium's organization and governance to the Purchasers. Regulatory authorities are carefully scrutinizing businesses and operations associated to cryptocurrencies in the world. In that respect, regulatory measures, investigations or actions may impact Cybercoinium's business and even limit or prevent it from developing its operations in the future. Any person undertaking to acquire Cybercoinium must be aware of the Cybercoinium business model, the white paper or terms and conditions may change or need to be modified because of new regulatory and compliance requirements from any applicable laws in any jurisdictions. In such a case,

purchasers and anyone undertaking to acquire Cybercoinium acknowledge and understand that neither Cybercoinium nor any of its affiliates shall be held liable for any direct or indirect loss or damage caused by such changes. Cybercoinium will do its utmost to launch its operations and develop the Cybercoinium platform. Anyone undertaking to acquire Cybercoinium acknowledges and understands that Cybercoinium does not provide any guarantee that it will manage to achieve it. They acknowledge and understand therefore that Cybercoinium (incl. its bodies and employees) assumes no liability or responsibility for any loss or damage that would result from or relate to the incapacity to use Cybercoinium, except in case of intentional misconduct or gross negligence.

11. CONCLUSION

The solution of the security issue of personal data and the desire to protect its digital assets from theft or loss became the main problems of mankind with the advent of the Internet. The larger and deeper the penetration of social networks into our lives, the more we risk

The essence of our technology for digital workflow is that it eliminates the need to have any third party or organization that certifies the object has been confirmed by two or more people. The ability to add to the Blockchain, in this distributed database, which is not specifically stored by anyone and nobody owns it individually, allows to provide this necessary level of security and data sharing.

The emergence of blockchain technology and cryptocurrency has led to the emergence of new assets' forms, new scammers and cybercriminals that use the most advanced technologies to achieve their goals, taking advantage of decentralization and anonymity, which can always be used not only for good, but also for harm.

The emergence of new, revolutionary technologies requires both a new format and approaches to address emerging new threats and the development of new protection approaches applicable to decentralized networks.

The Cybeconium Decentralized File Storage development and Cybercoinium Secureness of the concordium will give the cryptosystem a new security level and will solve the most important problem - the data storage security and asset rights to overcome the problem of the stolen funds irrecoverability.