SKRUMBLE NETWORK

SECURE COMMUNICATION-CENTRIC BLOCKCHAIN

WHITEPAPER

CRYP2NOVA

Draft for open community review. Subject to change.

Archived copy · cryp2nova.com

“Free speech is the whole thing, the whole ball game.

Free speech is life itself.”

Salman Rushdie

CRYP2NOVA

SKRUMBLE NETWORK
Archived copy · cryp2nova.com

TABLE OF CONTENTS

EXECUTIVE SUMMARY 4

INTRODUCTION 7

THE PROBLEM 8

THE SOLUTION 11

SKRUMBLE NETWORK 13

TECHNICAL COMPONENT 15

SKM UTILITY TOKEN 26

USE CASES & NETWORK ADDITIONS 29

CONCLUSION 32

ABOUT SKRUMBLE TECHNOLOGIES LTD 33

REFERENCES 36

CRYP2NOVA

Archived copy · cryp2nova.com

PLEASE READ THIS DISCLAIMER SECTION CAREFULLY. IF YOU ARE IN ANY DOUBT AS TO THE ACTION YOU SHOULD TAKE, YOU SHOULD CONSULT YOUR LEGAL, FINANCIAL, TAX, OR OTHER PROFESSIONAL ADVISORS.

The information set out in this white paper may not be exhaustive and does not imply any elements of a contractual relationship. The information is subject to change or update without notice and in no way constitutes the provision of professional advice. Skrumble Technologies LTD.., its subsidiaries and affiliates, do not guarantee and accept no legal liability whatsoever arising from or connected to, the accuracy, reliability, currency, or completeness of any material contained in this white paper.

SKM tokens are not intended to constitute securities in any jurisdiction but may be deemed to constitute securities by regulators in certain jurisdictions. This white paper does not constitute an offer to sell, or a solicitation of an offer to buy, SKM tokens in any jurisdiction in which it is unlawful to make such an offer or solicitation. Residents of Canada and residents or green card holders in the United States are excluded from purchasing SKM tokens, other than in accordance with applicable exemptions from such securities law requirements. Any offer or solicitation related to the SKM tokens will be made only by means of a confidential offering memorandum and in accordance with the terms of applicable securities and other laws.

Skrumble Technologies LTD., its subsidiaries and affiliates do not provide any opinion regarding the purchase, sale, or other distribution of the SKM tokens and readers of this white paper should not use it to form the basis of, or rely upon it, before entering into any contract or making any investment decision.

CRYP2NOVA

Archived copy · cryp2nova.com

EXECUTIVE SUMMARY

Background And Vision:
P2P Social Media Blockchain to Contact And Contract

When we study how and why people get together, we can can examine what the future of connecting is going to be. We have explored the new paradigm of people gathering in the new decentralized world and the next evolution is required. Humankind is maturing and showing great interest in moving beyond current centralized virtual gathering places. The groundswell is building for accessible communications that enable users to connect freely. This means no limits, no government control, no data leaking, no advertisers selling your data and everything fully owned by the community and the user.

The past centralized platforms such as Facebook, WhatsApp, WeChat and Telegram have greatly advanced society and continue to help connect people. However, new thinking and a more secure, global, community driven approach is being demanded as the next growth step. This white paper will outline the strong global impetus to move beyond the traditional paradigm of centralized information exchanges to the community owned decentralized value exchange inherent in the blockchain revolution that is upon us.

Human beings have an inherent need to connect with each other freely and securely. Therefore, a different level of blockchain is required that is optimized for communications to empower platform level applications. Hundreds of other unique applications and use cases can be built on top of this and truly expand the mission of the blockchain ecosystem in new and innovative ways.

The Skrumble Network Solution

Skrumble Network is a secure, communication-centric blockchain, decentralized communication application and a communication layer for developers to add into any application. With no middle entity or centralized server host in between to censor, block or manipulate any data, Skrumble Network will enable open, global private communication and transactions that are truly community owned and operated.

Along with building a proprietary, secure blockchain, Skrumble will also build the first complete full spectrum decentralized communication application that will breakthrough traditional firewalls, enable reputation management while assuring user anonymity, guarantee content and data privacy delivered with features like messaging, calling, video, file sharing, and more. The Skrumble Network blockchain and application will also create opportunities for people to add decentralized communication elements into any ecosystem or platform.

Archived copy · cryp2nova.com

For the good of humankind, a tool to speak freely with each other and freely trade value is necessary. Finally, people can connect globally on the most secure network possible. This will lead to an experience of Skrumble Network being the blockchain version of WeChat.

Technology: How Does Skrumble Network Combine Rich Media Communication and Blockchain?

The internet has enabled exponential progress for globalized information exchanges. However, they currently operate in centralized communication, servers and storage infrastructures. The technology of Skrumble Network aims to advance this to move beyond pure information exchanges into genuine value creation and exchange and true cooperation.

It is widely known that there are significant technical limitations with blockchain for data storage and connection speeds. Therefore, a unique hybrid methodology is required to bring the security and the secure, ledger based infrastructure of blockchain and secure, distributed and encrypted rich media communication together. This will be accomplished by optimizing the Skrumble Network Blockchain for today's modern communication needs of rich multimedia, quick transaction times, security and in-app financial exchanges. It is designed to carry a payload of information that is required to establish a peer-to-peer (P2P) communication as well as financial transaction ledger data. The primary goal of the Skrumble blockchain is to achieve consensus as quickly as possible. Although TPS is critical, the design will allow the Skrumble Network to scale to an eventual 1000 TPS from the current operating level of 500 TPS.

By achieving consensus quickly, the lag typically associated with blockchain transactions are obfuscated from the user experience. The net effect is a consumer-grade, seamless experience that users have come to expect, with the unparalleled security and authentication provided by blockchain technology. This will usher in a new generation of secure and powerful applications that meet and exceed the expectations of today's usability standards.

The Skrumble Blockchain is a P2P network structure, in which nodes can communicate with each other through a hashed messaging protocol. In this structure, there are two different types of nodes: peer nodes and validating nodes. A peer node can broadcast, receive and transfer transactions or blocks, while a validating node can create blocks of data.

Archived copy · cryp2nova.com

Community Strategy

Token Distribution

The one way to get these people together to share and create value together:

Miners, users, contributers

Skrumble Network's secure communication-centric platform is a public blockchain. The Foundation, as a sponsor of the project, is working towards creating the Skrumble Network blockchain ecosystem rather than being focused on corporate profits as traditional enterprise projects do. The platform, which benefits all token holders, does not belong to any single organization or individual and is a platform embracing the entire blockchain token community. It will use token mechanisms and the foundation's resources to continually foster numerous communities such as technical communities, college communities, user communities, investment communities, node participant communities, centralized organizations, data source providers etc. The vision of the SN community is to create an inclusive big family who shares the vision and passion of growing the Skrumble Network.

CRYP2NOVA

Archived copy · cryp2nova.com

INTRODUCTION

The need for simple and secure methods of communication and data ownership has never been greater. It is essential for people to communicate with one another, and its imperative that those people can communicate securely and own their own data. Skrumble Network will innovate decentralized communication with the Skrumble public blockchain. This network will be a powerful, secure communication-centric blockchain with leading TPS leading to rapid connection times. This will enable truly real-time, commercial grade communication with user identities authenticated on the blockchain by providing a secure key that will be a randomized derivative of each participant's public key. The only people with access to these communications would be the actual participants themselves. There is no middle entity in between to censor, block or manipulate any data. This will enable open, global private communication that is truly community owned and operated. This will create opportunities for people to add decentralized communication elements into any blockchain ecosystem, build applications with decentralized communication. Finally, people can connect globally and speak freely on the most secure network possible.

Due to the rise of blockchain and new decentralized global paradigm, it is essential for Skrumble Network to innovate using this technology and demonstrate how decentralized networks have the power to be a catalyst for more secure communication. This will be accomplished through the unique hybrid Skrumble Network blockchain security, patented distributed SSL protocol and rich-media WebRTC based communication technology.

In this whitepaper, topics discussed will include the risks surrounding centralized servers for data storage, threats to user information involving Internet-based communication systems and the difficulty of establishing meaningful connections online. These issues will emphasize the need for a secure and high speed blockchain that enables unified, secure network providing a unique end-to-end experience with complete anonymity, and will create the opportunity for a decentralized communication network to experience infinite growth.

Skrumble Network has the potential to truly democratize communication on a global scale and usher in a new era of applications that have never been done before, leading to advanced and unparalleled forums of innovation and discovery. It will have the ability to connect anyone from anywhere in the world in a secure and simple way. Using blockchain technology and decentralized network protocols, Skrumble Network will be the first to build a secure, complete full spectrum rich media communication ecosystem that will breakthrough traditional firewalls, assure user anonymity, guarantee content and data privacy. Now, any application will have the ability to implement leading decentralized communication features such as group and peer-to-peer messaging, calling, video, file transfers and more with one blockchain network protocol. Much like blockchain disrupted the financial industry with a distributed ledger methodology after dissatisfaction with large centralized financial establishments, we see massive opportunities to do the same to the communications industry. We will do this by bringing data ownership and security back to the people away from large telecommunications companies and centralized app providers (like Facebook, Telegram, WeChat and WhatsApp).

Archived copy · cryp2nova.com

THE PROBLEM

1. Security: Communication systems with centralized servers pose data security challenges

2. Privacy & Data Ownership: Platforms are not private, can be blocked or compromised and users do not own their data

3. Global Access: Marginalized communities seek free discussion and trusted connections

1. Security: Communication Systems with Centralized Servers Pose Data Security Challenges

The Internet has revolutionized the way we communicate and connect. Video chats are possible with the click of a button, businesses can operate and collaborate internationally, banks facilitate international transfers of trillions of dollars everyday, and reaching out to the president of a country is just a tweet away. With e-commerce, an item could be manufactured in Guangzhou, and sold by a company in New York to a woman in Sydney. Social media has changed the face of communication, news reporting and entertainment. The Internet has succeeded in connecting nearly everyone on its network, but it also raises concerns regarding privacy and data security.

Internet users regularly, and sometimes unwittingly submit to terms-of-service agreements that give companies license to share their personal data with other institutions, from advertisers to governments. For instance, Google manages to offer its major consumer services for free by sharing user data such as browser activity and search history, while Facebook sells user data and activity such as post likes and comments to advertisers (Google, 2018; Facebook, 2018). When visiting social media or e-commerce websites, it is a common occurrence for advertisements to reflect the above-mentioned data or even conversations that were had verbally offline, which raises specific concerns about digital eavesdropping and user privacy.

Communication applications are used to manage massive amounts of data traffic everyday. Messaging platform WhatsApp reportedly handles approximately 55 billion messages, 4 billion photos and 1 billion video transfers a day. However, like most other Internet-based communication platforms, all this data is routed through a centralized server with one main point of contact. In this kind of centralized system, breaching a single point of contact is easier and could give malicious parties access to a mass amount of the network's data. This would allow hackers to steal and tamper with information. Due to these issues, in January 2018 cryptographers discovered a backdoor through WhatsApp's security system and were able to infiltrate group chats. With a breach of this magnitude, WhatsApp's credibility became refutable and effectively rendered the chat tool's end-to-end encryption useless (Greenberg, 2018).

It is nearly impossible to use the Internet without yielding on privacy or being at risk for hacking. There is a critical need for a decentralized, impenetrable network through which users can communicate and connect securely without having to worry about their personal information being compromised. This is especially pertinent in the cryptocurrency world where large sums of money are at stake.

Archived copy · cryp2nova.com

2. Privacy & Data Ownership: Platforms Are Not Private, Can Be Blocked or Compromised and Users Do Not Own Their Data

When it comes to communicating with one another, generally people turn to the Internet as the primary source of information transfers. However, with numerous sources of information and discussion forums available on the Internet today, people use several different communication platforms to learn and have discussions about blockchain and other important topics. This leads to a very fragmented and disconnected community experience.

Use of various platforms like Facebook, WhatsApp, WeChat, and others to collaborate and share information make it difficult to have a consistent and trustworthy global standard. Even platforms like Telegram, which have been known to censor and block content, can have data be collected, decrypted and access can be blocked completely due to known VPN URLs or IP addresses (Russell, 2017). In fact, on February 1, 2018, Telegram was removed from the Apple App Store due to 'inappropriate content' and were asked to ensure they have protective measures in place to filter their content (Warren, 2018). Some of these platforms are banned or throttled in certain countries, leading to information inequality. Facebook and WhatsApp are banned in China and there was recently a ban lifted on Telegram in Iran, however Telegram is and has been banned in multiple other countries, like Indonesia (Toronto Star, 2018; Toor, 2017).



- Facebook, WhatsApp, and Google are banned in Mainland China (India Today, 2017).
- WhatsApp was recently found to have a backdoor to infiltrate group chats (Greenberg, 2018).
- WeChat censors user conversations and does not sync across multiple devices (WeChat, 2018).
- Telegram actively censors content and was previously banned in Iran (Toronto Star, 2018).
- Facebook and Google share user activity with advertisers (Facebook, 2018; Google, 2018).
- It was recently reported that over 50 million Facebook users had their data stolen and misused (Sherr, 2018)

Moreover, specific forums focused on the discussion of new technology and other topics may have other forms of censorship. One such example is dedicated forums for discussion on cryptocurrency like Bitcointalk or threads on Reddit. A critical barrier to entry for people interested in cryptocurrency is a lack of information about the legality of cryptocurrency trading. These forums often have limitations when it comes to accuracy, credibility and trust, since they are mostly comprised of personal opinions and not always backed by verifiable facts.

People also turn to video sharing platforms like YouTube for information and education on the cryptocurrency ecosystem and almost everything else. This content has the problem of being unidirectional, untrustworthy and biased as they mostly cover individual preferences, providing only a superficial view on any topic. Also, since these communication platforms use centralized networks, they face all the previously discussed dangers of hacking, social engineering and other security vulnerabilities.

Archived copy · cryp2nova.com

After studying current online communities and communication platform options, flaws and vulnerabilities are obvious within each system. Current solutions are fragmented, disconnected and unreliable, which creates scope for improvement to enhance trust and connectivity worldwide. Through a solution like a globally accessible online community, unified, secure communication would increase and expand opportunities for bringing people together.

3. Global Access: Marginalized Communities Seek Free Discussion and Trusted Connections

With constant apprehension and data insecurity, how are people supposed to feel comfortable to create sustainable online communities and share meaningful information in conversations? One of the challenges of online engagement is developing relationships while protecting your identity, creating comfort, security, and developing actionable activities. People need untethered access to public forums and platforms to exercise their fundamental human right to speak freely, and not feel concerned with intermediaries and unknown third parties having access to their private information.

Simply discussing common interests, sharing stories and networking helps to bring people together. When people are connected, they feel unguarded and comfortable enough to share genuine and honest ideas, personal information and establish meaningful relationships. When people are comfortable and connected, incredible and innovative things can happen.

With sometimes marginalized communities seeking forums for free discussion, it can be difficult to find an open and streamlined medium to share new ideas. One example of a community in need of connectivity and global access is the cryptocurrency community. Public perception of a cryptocurrency is one of the biggest deciding factors behind its adoption and value. While only around nine years old, cryptocurrencies are now at a stage of rapid growth and expansion with currently thousands of different currencies and applications. In such a budding environment, it is increasingly difficult for blockchain technology companies to showcase new ideas and for potential users to connect and learn more about the latest community developments. The best way for blockchain advocates to engage with potential users and the public is through direct communication.

By not only encouraging but facilitating the establishment of meaningful connections, a secure communication network could truly provide essential mediums for anyone from anywhere in the world to come together. They could simply speak freely, share information and transfer data without the implication of being hacked or someone else being privy to their personal information. A global blockchain community would help improve communication worldwide, whether it be between current blockchain users or anyone who needs to connect with someone using a secure network.

Archived copy · cryp2nova.com

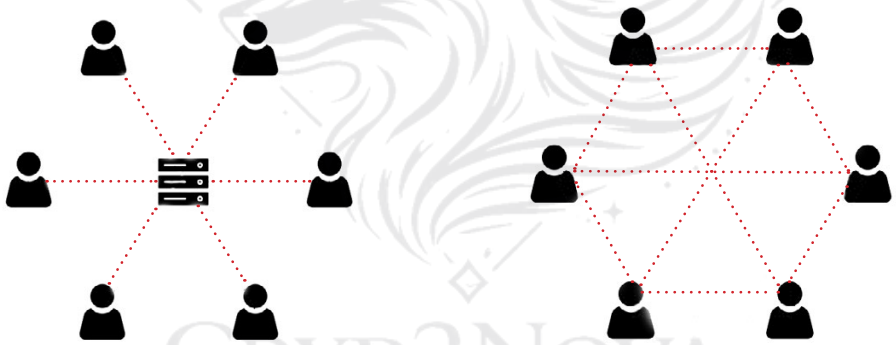
THE SOLUTION

1. Secure: Enhancing security with proprietary communication technology

2. Decentralized: Distributed blockchain ledger supporting secure communication transactions

1. Secure: Enhancing Security with Proprietary Communication Technology

Traditionally, communication platforms rely on a centralized server for information and storage of all data transactions between users. However, on a decentralized network like the blockchain, no information is stored in one central location, which makes it almost virtually impossible for cybercriminals to hack. Hackers and other cybercriminals regularly infiltrate entire computer security systems and networks from anywhere in the world, in a matter of hours. Yet, as soon as information is recorded in a blockchain's distributed ledger it cannot be erased, changed, relocated or tampered with in any way. Attacking one central server is no longer enough to gain control over the entire system. This consensus-based immutability of a decentralized network creates a transparent and secure framework with vast implications.



Centralized Server

Decentralized Network

In the banking sector, a method that secures digital transactions is a necessary investment, and the blockchain technology used in cryptocurrencies is a top contender. Economists studying cryptocurrency have confirmed that money has already begun moving from physical to digital form and governments in countries like Canada, India and Russia have begun exploring avenues for incorporating cryptocurrency into use (Sabbin, 2018). Blockchain's inherent immutability reduces the cost of verifying transactions and its decentralized nature offers the potential to eliminate the middleman from the trading process.

The same can be said for communication solutions and identity management opportunities on a decentralized network. Given the huge scope of applications for blockchain technology use, and the transparency and security those applications will offer, enhanced services and platforms that enable these services to be more accessible to the public have the opportunity for significant growth.

Archived copy · cryp2nova.com

2. Decentralized: Distributed Blockchain Ledger Supporting Secure Communication Transactions

In 1998, Nick Szabo, cryptographer and smart contract pioneer, stated that "doing business on the Internet requires a leap of faith". Trust has always been the fundamental currency of both communication and commerce. Every second new online transactions occur between strangers around the world, usually through a third party enabling the communication transaction, and trust needs to be manufactured between the user and host to complete the operation. Whether a message is sent, or a payment is made, the sender has no choice but to trust that the intermediary will deliver the transaction to the intended recipient safely.

With the distributed blockchain ledger, users can securely and directly connect and perform transactions with each other, without having to rely on an intermediary or worry about protecting their privacy. Blockchain and decentralized networks offer a way to confidently operate in a trust-less environment using its distributed ledger to create transparency and consensus-driven, tamper-proof logs of transactions. Every transactional 'block' is verified by the entire network and then immutably linked to the 'chain' to provide unparalleled security and accountability.

Additionally, there is an overwhelming need to improve identity management protocols on the web. The need to verify one's identity is now essential for numerous online accounts and transactions, including your personal home address, contact information, financial information and more. In 2017 in the United States, there was a record number of 15.4 million Americans subjected to financial fraud and theft of their account information (Pascual, 2017).

Distributed ledgers offer enhanced methods for verifying identity, without having to share contact details, along with the possibility to digitize personal information. The dual-encryption mechanism on a blockchain with public and private keys enables applications to digitally verify the identity of the people using them and eliminates the risk of false key propagation and data tampering or theft.

The clear solution to this problem is leveraging blockchain's distributed ledger, which connects users directly, eliminating the need to place trust in an intermediary or an unknown party. A decentralized communication solution will mean users can securely and directly connect and transact with one another, without having to worry about their privacy.

Archived copy · cryp2nova.com

SKRUMBLE NETWORK: : P2P SOCIAL MEDIA BLOCKCHAIN TO CONTACT AND CONTRACT

There is an undeniable need for secure, streamlined and standardized communication-centric blockchain that is easy to build upon or seamlessly enables secure, commercial-grade decentralized communication for anyone. With a robust, secure framework designed specifically for the blockchain ecosystem and expertise in the field of unified communications, Skrumble Network is best-equipped to fulfil this need.

The first-ever complete communication ecosystem on a decentralized blockchain authentication network will be built by Skrumble Technologies LTD. This unique ecosystem will be an easy-to-use, secure network to connect anyone from anywhere in the world through open communication. With complete unified communication, Skrumble Network community members and development partners can finally establish meaningful, connections in a truly democratized, unquestionably secure, global, decentralized environment.

Using a unique consensus-based algorithm and pseudonymous identification measures where people set their own usernames, users will maintain ownership of their information, data and communication transactions. Users will have the opportunity to bring together large groups of people into online communities or have one-on-one conversations with another user and keep that information completely private and secure. The network will allow users to interact using seamless messaging, calling, video, file transfers, and more and improve users access to communication, identity management, and unlimited secure communication transactions. Skrumble Network intends to leverage its unique and novel security technology to solve the security risks of current Internet-based communication systems through its distributed ledger authentication and patented SSL to rich media protocols.

Due to the rise of blockchain and the new decentralized global paradigm, it is essential for the Skrumble Network community to innovate together using this technology and demonstrate how decentralized networks have the power to be the catalyst for more secure communication.

In today's trust-less world, reputation will be crucial to build, without having to use the traditional means of building relationships to conduct transactions. For example, in the past, if you wanted to build trust and transact with someone, you would need to go out for dinner, maybe grab drinks with someone and read each other's character. In today's trust-less world, you do not even need to know their real name - just having a sense of their reputation through a rating of their past dealings and a simple smart contract obviates the need for anything else.

On Skrumble, unlike other centralized platforms that require a phone number, government identification or email address, you use a secure key generated on the blockchain that only you and your peers in the conversation have access to. Now people will be able to join the blockchain economy with ease and true data ownership.

Archived copy · cryp2nova.com

Skrumble Technologies LTD recognizes the inherent need for a secure communication ecosystem utilizing the consensus-based immutability of decentralized network protocols and will be the driving force behind innovating human connectivity and identity management. Skrumble Network draws upon the expertise and experience of the irreplaceable team behind Skrumble to deliver this ground-breaking and unique functionality. Using open source Software Development Kits (SDKs), the complete communication ecosystem will be built to be easily adaptable for third parties to integrate and develop a multitude of applications that require secure, private and anonymous communication.

One of the first of it's kind, Skrumble Network will operate outside of the financial exchanges that blockchain protocols are traditionally utilized for, and instead will be used to set a new global standard for communication, authentication, and how blockchain technology can be used in applications around the world.

Skrumble Network Blockchain Communication Features

- Messaging
- Audio Calling
- Video Calling
- File Transfers
- Group Conferencing
- Screen Sharing
- User-Controlled Storage
- Screenshot Notifications
- Pseudonymous Identification
- Data Encryption
- Most Functionality Supported On Any Modern Browser
- Wallet for In-Context Money Transfers

CRYP2NOVA

Archived copy · cryp2nova.com

THE TECHNOLOGY POWERING SKRUMBLE NETWORK: TECHNICAL COMPONENT

INTRODUCTION: Secure Communication On a Decentralized Network

Traditional communication networks are based upon centralized servers. Independent of the communication protocols that are used, they all function in essentially the same way. That is, with an information packet that contains handshake and exchange of meta information to establish the communication's media stream. The server will then establish and mediate that communication. Skrumble Network will revolutionize the way that communication happens by completely cutting out the centralized server.

The Skrumble Network Blockchain Overview

The Skrumble Network blockchain is optimized for today's modern communication needs of rich multimedia, quick transaction times, security and in-app financial exchanges. It is designed to carry a payload of information that is required to establish a peer-to-peer (P2P) communication as well as financial transaction ledger data. The primary goal of the Skrumble blockchain is to achieve consensus as quickly as possible. Although TPS is critical, the design will allow the Skrumble Network to scale to an eventual 1000 TPS from the current operating level of 500 TPS.

By achieving consensus quickly, the lag typically associated with blockchain transactions are obfuscated from the user experience. The net effect is a consumer-grade, seamless experience that users have come to expect, with the unparalleled security and authentication provided by blockchain technology. This will usher in a new generation of secure and powerful applications that meet and exceed the expectations of today's usability standards.

The Skrumble Blockchain is a P2P network structure, in which nodes can communicate with each other through a hashed messaging protocol. In this structure, there are two different types of nodes: peer nodes and validating nodes. A peer node can broadcast, receive and transfer transactions or blocks, while a validating node can create blocks of data.

The blockchain protocol is similar to that of Bitcoin, however, the data structure such as blocks or transactions is significantly different because it contains not only financial data but communications instructions and encryption information as well.

An example of the addition payload requirements are data fields that allow the peer to peer communications to be established. This includes fields that identify the session id (SID). This field is required and becomes linked to the "b" leg username. This is used to not only identify the current session but allows the user to see the complete conversation history between the parties.

Archived copy · cryp2nova.com

Obfuscation of the IP and NAT transversal info is accomplished by using hashing algorithm that increments. Incrementation of the algorithm is achieved through two identifier fields. The first is the VID (version ID) which tells the other users what version of the app is being used. The second is the IID (incrementation ID) which alerts the other legs of the communication to which hashing algorithm to use. Hashing algorithms will be updated with each new release of software. Versions of software that are more than two releases apart from each other will generate an error. This is done to ensure users have the latest application software.

A hashed download link is also included for users in geographic locations that might not have access to traditional app stores. This link will constantly change to ensure access for marginalized populations. This link will be hashed using the same technique of VID and IID data to further confuse any attempt by authorities to learn the link destination. Additionally, addresses of validating nodes will be hashed in the same way, that is using the VID and IID.

Identity-Based Network Security

The Skrumble Network blockchain employs novel approach to user identity management in blockchain services. We implement identity-based end-to-end security which extends from the blockchain client to the blockchain fabric. This approach allows for identity-based network segmentation and traffic separation, which enables multiple users to securely share the same blockchain infrastructure, reduces the risk of DDoS attacks, and enables automated regulatory compliance audits. Our solution is based on the Skrumble Network Transport Access Control (SKTAC) technologies, implemented using software application library endpoints Skrumble Network. This approach can easily be generalized to protect many different types of commercial applications.
SKTAC features include permission control and confidentiality, un-linkable identity privacy for blockchain participants, a modular and easily auditable consensus protocol, and improved scalability. SKTAC extends the blockchain in several important ways.

- A new method for identity-based network security, which extends end-to-end from the client to the blockchain fabric. This is realized by authenticating the first packet of a network connection request using cryptographic identity tokens, which are inserted into the packet header by the Skrumble Network application at the client, and later authenticated by a validating node. All unauthorized traffic (including port scans) is dropped at the transport level, so the traffic source does not receive any acknowledgment or feedback which might be used for reconnaissance or enumeration as the first step in a cyber-attack. In this manner, we isolate and protect blockchain services from unauthorized access; this helps prevent cyber-attacks, enables blockchain services, and forms the basis for a zero trust blockchain network.

- SKTAC introduces identity-based network segmentation and traffic separation, which reduces the risk of cyber-attacks. Using the First Packet Authentication described previously, we separate internal traffic between peers and validating node functions used in the Skrumble Network Blockchain. Audit trails for all authorized and unauthorized connection attempts to the blockchain are maintained and can be easily audited using software to parse the log contents.

Without authentication any unauthorized user will receive the message that this site cannot be reached, and no further information is available.

Archived copy · cryp2nova.com

Securing The Conversation

Perhaps the most unique and critical component of the Skrumble blockchain is the encryption scheme. This is used to encode all aspects of a communication. This includes voice, video and even the files that might be exchanged and stored.

Skrumble Network derives its encryption scheme from the data that is traded anomalously via the blockchain. This ensures the highest level of encryption, privacy and user ownership of the data.

The Skrumble Network has developed a protocol called SKRTP (Skrumble Secured Real Time Protocol. The white paper for this protocol will be published at release time.

The Skrumble Network Secure Real-Time Transport Protocol (SKRTP)

The Skrumble Network will employ Secure Real-time Transport Protocol (SKRTP), a profile of the Real-time Transport Protocol (RTP), which provides confidentiality, message authentication, and replay protection to the RTP traffic and to the control traffic for RTP, the Real-time Transport Control Protocol (RTCP).

The Secure Real-time Transport Protocol (SKRTP), a profile of the Real-time Transport Protocol (RTP), which can provide confidentiality, message authentication, and replay protection to the RTP traffic and to the control traffic for RTP, RTCP (the Real-time Transport Control Protocol).

SKRTP provides a framework for encryption and message authentication of RTP and RTCP streams. SKRTP defines a set of cryptographic transforms, and it allows new transforms to be introduced in the future. With appropriate key management, SKRTP is secure for unicast and multicast RTP applications.

SKRTP can achieve high throughput and low packet expansion. SKRTP proves to be a suitable protection for heterogeneous environments (mix of wired and wireless networks). To get such features, default transforms are described, based on an additive stream cipher for encryption, a keyed-hash based function for message authentication, and an "implicit" index for sequencing/synchronization based on the RTP sequence number for SKRTP and an index number for Secure RTCP (SRTCP).

Archived copy · cryp2nova.com

Features

The security goals for SKRTP are to ensure:

- The confidentiality of the RTP and RTCP payloads, and
- The integrity of the entire RTP and RTCP packets, together with protection against replayed packets.

These security services are optional and independent from each other, except that SRTCP integrity protection is mandatory (malicious or erroneous alteration of RTCP messages could otherwise disrupt the processing of the RTP stream).

Other features for the protocol are:

- Low bandwidth cost, i.e., a framework preserving RTP header compression efficiency, and, asserted by the pre-defined transforms:
- A low computational cost,
- A small footprint (i.e., small code size and data memory for keying information and replay lists),
- Limited packet expansion to support the bandwidth economy goal,
- Independence from the underlying transport, network, and physical layers used by RTP, high tolerance to packet loss and re-ordering.

These properties ensure that SKRTP is a suitable protection scheme for RTP/RTCP in both wired and wireless scenarios.

SKRTP provides for some additional features that have been introduced to lighten the burden on key management and to further increase security. They include:

- A single "master key" can provide keying material for confidentiality and integrity protection, both for the SKRTP stream and the corresponding SRTCP stream. This is achieved with a key derivation function, providing "session keys" for the respective security primitive, securely derived from the master key.
- In addition, the key derivation can be configured to periodically refresh the session keys, which limits the amount of ciphertext produced by a fixed key, available for an adversary to crypto-analyze.
- "Salting keys" are used to protect against pre-computation and time-memory tradeoff attacks.

CRYP2NOVA

Encryption

The encryption defined in the SKRTP map the SKRTP packet index and secret key into a pseudo-random keystream segment. Each keystream segment encrypts a single RTP packet. The process of encrypting a packet consists of generating the keystream segment corresponding to the packet, and then bit-wise exclusive that keystream segment onto the payload of the RTP packet to produce the Encrypted Portion of the SKRTP packet. In case the payload size is not an integer multiple of n_b bits, the excess (least significant) bits of the keystream are simply discarded. Decryption is done the same way, except with swapping the roles of the plaintext and ciphertext.

The definition of how the keystream is generated, given the index, depends on the cipher and its mode of operation. Below, two such keystream generators are defined. The NULL cipher is also defined, to be used when encryption of RTP is not required.

Archived copy · cryp2nova.com

The initial octets of each keystream segment may be reserved for use in a message authentication code, in which case the keystream used for encryption starts immediately after the last reserved octet. The initial reserved octets are called the "keystream prefix", and the remaining octets are called the "keystream suffix".

The number of octets in the keystream prefix is denoted as SKRTP_PREFIX_LENGTH. The keystream prefix is indicated by a positive, non-zero value of SKRTP_PREFIX_LENGTH. This means that, even if confidentiality is not to be provided, the keystream generator output may still need to be computed for packet authentication, in which case the default keystream generator (mode) shall be used.

The cipher is the Advanced Encryption Standard (AES), Segmented Integer Counter Mode AES. Let E (k,x) be AES applied to key k and input block x. Conceptually, AES consists of encrypting successive integers. The actual definition is somewhat more complicated, to randomize the starting point of the integer sequence. Each packet is encrypted with a distinct keystream segment, which is computed as follows.

A keystream segment is the concatenation of the 128-bit output blocks of the AES cipher in the encrypt direction, using key k = k_e, in which the block indices are in increasing order. Symbolically, each keystream segment looks like:

E(k, IV) || E(k, IV + 1 mod 2^128) || E(k, IV + 2 mod 2^128) ...

Where the 128-bit integer value IV is defined by the SSRC, the SKRTP packet index i, and the SKRTP session salting key k_s, as below:

IV = (k_s * 2^16) XOR (SSRC * 2^64) XOR (i * 2^16)

Each of the three terms in the XOR-sum above is padded with as many leading zeros as needed to make the operation well-defined, considered as a 128-bit value.

The inclusion of the SSRC allows the use of the same key to protect distinct SKRTP streams within the same RTP session.

In the case of SRTCP, the SSRC of the first header of the compound packet MUST be used, i SHALL be the 31-bit SRTCP index and k_e, k_s is replaced by the SRTCP encryption session key and salt.

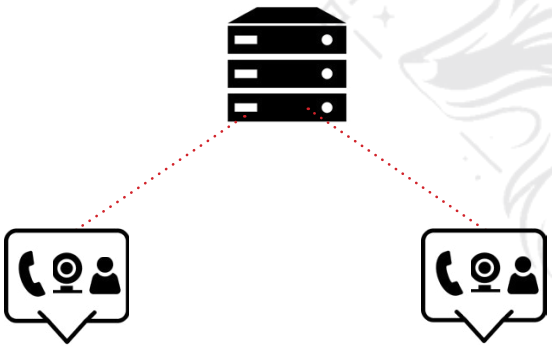
Note that the initial value, IV, is fixed for each packet and is formed by "reserving" 16 zeroes in the least significant bits for the purpose of the counter. The number of blocks of keystream generated for any fixed value of IV must not exceed 2^16 to avoid keystream re-use, see below. The AES has a block size of 128 bits, so 2^16 output blocks are sufficient to generate the 2^23 bits of keystream needed to encrypt the largest possible RTP packet. This restriction on the maximum bit-size of the packet that can be encrypted ensures the security of the encryption method by limiting the effectiveness of probabilistic attacks.

Archived copy · cryp2nova.com

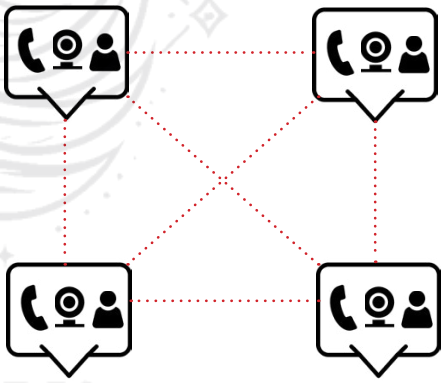
Key Derivation

Key derivation reduces the burden on the key establishment. As many as six different keys are needed per crypto context (SKRTP and SRTCP encryption keys and salts, SKRTP and SRTCP authentication keys), but these are derived from a single master key in a cryptographically secure way. Thus, the key management protocol needs to exchange only one master key (plus master salt when required), and then SKRTP itself derives all the necessary session keys.
Multiple applications of the key derivation function will give security benefits when enabled. They prevent an attacker from obtaining large amounts of ciphertext produced by a single fixed session key. If the attacker was able to collect a large amount of ciphertext for a certain session key, he might be helped in mounting certain attacks.

Multiple applications of the key derivation function provide backwards and forward security in the sense that a compromised session key does not compromise other session keys derived from the same master key. This means that the attacker who can recover a certain session key, is anyway not able to have access to messages secured under previous and later session keys (derived from the same master key). (Note that, of course, a leaked master key reveals all the session keys derived from it.) Detailed papers and source code will be published to coincide with the public release of the Skrumble Network chain.



Current networks with centralized servers.



Skrumble Network –
Decentralized network with no central server.

CRYP2NOVA

Archived copy · cryp2nova.com

Unique Session ID & Data Management Using Skrumble Network's Protocols

Skrumble Network will be an entirely unique blockchain enabled technological ecosystem enabling a completely decentralized and anonymous communication ecosystem. It will leverage real-time communication protocols over peer-to-peer connections using any modern web browser or Skrumble Network's native applications (iOS, Android, PC & Mac).

Skrumble Network's unique security protocols will be delivered through a proprietary key derivative algorithm using the Skrumble Network blockchain. Upon joining the network, users will be asked to enter the public key to the wallet where they hold their Skrumble Network tokens. Additionally, they will be asked to enter a secure passcode and a pseudonym (private user name). A derivative of these elements will be used to generate their unique private Skrumble Network User ID and a Public ID. A QR code and link will be generated for easy sharing of the users' Public Skrumble Network ID.

With unparalleled security, conversations will be encrypted using a derivative of the private Skrumble Network User ID keys from each participant as the seed key for the encryption. The derivative algorithm will randomly select from the associated Skrumble Network keys in the session based on the participants involved, therefore no two keys will be the same. This ensures an added layer of security as no two conversations will use the same key which makes Skrumble Network conversations virtually impossible to decrypt using pattern-based methodologies. For example, a randomized combination of User A's private Skrumble Network User ID key and User B's Private Skrumble Network User ID key will come together to form the conversation seed key and conversation ID.

When a communication is established between users, the Skrumble Network blockchain will replace the handshake protocol that happens on a traditional communication network. In the Skrumble Network, Session Description Protocol (SDP) messages will use the blockchain to establish each session, acting as the handshake and signal for communication to commence, and Real-Time Transport Protocol (RTP) stream for the media (voice, video, message, etc.) to begin transmission.
Once a connection is established between peers, the IP addresses of the users are revealed only to each other and a secure web socket connection will be established to open an interactive communication session between the users' devices to exchange real-time session data for messages, file transfers and notifications. This allows for data to be instantly distributed resulting in a low-latency connection.

Communications on Skrumble Network will be P2P (Peer-to-Peer) and will have the ability to access an ad-hoc high capacity rich communication bridge for voice and video conferencing for larger number of participants.

Skrumble Network will be built to operate on any modern browser, in addition to functioning as a standalone application for most mobile and tablet devices (iOS and Android) and computers (Mac and PC). The standalone application versions will offer additional functionality over the browser-based version.

Archived copy · cryp2nova.com

Skrumble Network Communication Authentication Blockchain Protocols

The Skrumble Network will develop its own blockchain that establishes unique and secure ad-hoc communication sessions. Skrumble Network's blockchain will be utilized in several aspects of the application:

- Establish the initial communication session.
- Synchronize user pseudonyms with the Skrumble Network User ID.

Both functions will require mining efforts to deliver consensus validation and authentication. Skrumble Network will develop a strong reward and outreach program to incentivize master node server hosts, as well as its mining community and partners to actively support the project. These partnerships will help ensure Skrumble Network consensus resolution times are optimized.

Unparalleled Future Data Capacity & Speed

Currently, when users conduct activities using existing blockchain based applications, new transaction and data are saved and stored. The more transactions being saved means slower loading times. For example, a standard financial transaction on Ethereum usually takes about twenty seconds to reach consensus (Yannik, 2017). With an increase in communication transaction volume, Skrumble Network's need for every message, call, video call and file transfer to be considered another transaction would lead to slow down the performance for each user. Therefore, to alleviate this crucial point, Skrumble Network will utilize the Practical Byzantine Fault Tolerance (PBFT) consensus algorithm, to offer a balance between performance and scalability. For transactions to be settled in real-time, Skrumble Network will aim to achieve communication setup in less than ten seconds, supported by incentivized mining efforts.

To ensure Skrumble Network has optimized loading times, these protocols will be developed using sharding technology. By using sharding technology, Skrumble Network will be able to separate very large databases into smaller, faster, more easily managed parts. When data is needed, instead of one record loading at a time, Skrumble Network will load as one layered database by pulling up information in pieces from each shard.

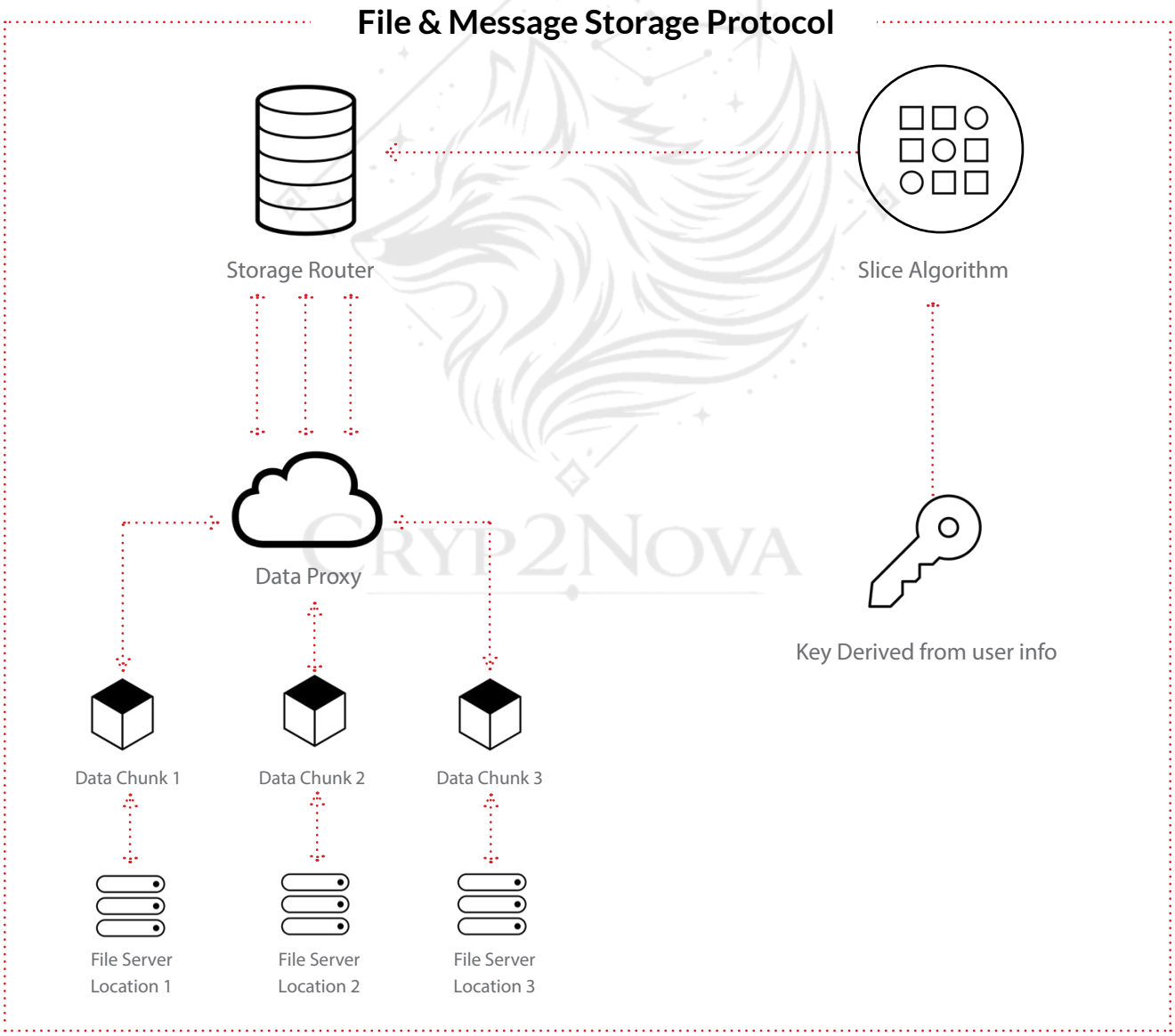
The Skrumble Network team will be constantly researching and evaluating new and faster methods of consensus and blockchain load times reduction. The team will be committed to improving the network on an ongoing basis to ensure user experience always remains seamless and consistent on the Skrumble Network.

Archived copy · cryp2nova.com

Exclusive Encrypted Keys For File Storage On Decentralized Network

Skrumble Network will achieve truly decentralized file storage by utilizing an algorithm that uses unique session identification and randomized key data per user to ensure file information is encrypted. With this algorithm, Skrumble Network can ensure the direct file transfer between users and only users who have participated in the conversations will be permitted access.

The Skrumble Network will employ a novel patent pending method of hybrid storage strategy. This method was created and developed by Skrumble Technologies LTD. Using this hybrid approach, files will be encrypted using an algorithm that will be derived from the unique session ID and its seed key. Once encrypted, the individual files will be sliced into several pieces, distributed and stored on disparate servers. These files can only be re-assembled with the appropriate key. Therefore, if any file server is to be compromised, the data obtained will be unintelligible, further providing secure data storage for all users.



Archived copy · cryp2nova.com

Moreover, features such as the length of time to store and file sizes allowed will be determined by the usage level that the user has unlocked based upon the number of Skrumble Network tokens in their wallet.

High Capacity Rich Communication Bridge

For voice and video conferences that contain greater than 6 participants, anonymous ad-hoc sessions will be established through dedicated bridges that will be situated in key strategic area globally and authenticated via the unique session ID and the derived key. Skrumble Network will use a scheme of IP tunneling to an address, changing randomly selected from a very large pool, that is only revealed during the secure socket connection made between users once they are connected. Per the protocol for connecting to the bridge, users will verify connectivity. Should connectivity not be reached, the user will increment to the next agreed upon address. These protocols will allow for larger scale voice and video conferencing, messaging, screen sharing, file transfers and notifications. To unlock features such as the ability to add a greater number of participants or the length of time allowed will be determined by what usage level the user has unlocked based upon the number of Skrumble Network tokens in their wallet.

LEADING FEATURE SET & USER CONTROLLED RECORD STORAGE

One of Skrumble Network's biggest differentiators is the option for group & peer-to-peer messages to be saved and stored. Conversation records will be stored using file servers in the cloud. Only users with the unique conversation key who participated in the original conversation will be permitted to access the saved information.

When a group message is created, the administrator of that conversation will be given the option to save the records. Select functionality will be unlocked based on certain token ownership amounts. When other participants attempt to enter the conversation, they will first be notified that the administrator has selected to save the conversation and participants can opt not to partake. When participating in a conversation with two participants, there will be two-party consent. Each participant will need to agree to save the conversation for records to be saved and stored.

Moreover, Skrumble Network will also introduce other exclusive functionalities such as a unique algorithm that creates encryption keys based on participants in a discussion, and other factors, to differentiate every conversation. With the intention of connecting anyone, anywhere in the world, users will be able to easily create large community groups. To keep Skrumble Network's anonymous protocol, users will operate through pseudonymous identification. Users will receive notifications when other users have taken screenshots of a screen share or video. Users have access to live video groups and encrypted, decentralized file and data transfer. By publishing open source SDKs, Skrumble Network will encourage and incentivize third party developers to build new blockchain technologies and applications using Skrumble Blockchain's secure, private and anonymous communication ecosystem capabilities.

Archived copy · cryp2nova.com

Skrumble Network: Global Communication, No Firewalls

Among the numerous obvious benefits of utilizing Skrumble Network's decentralized, secure and anonymous communication platform, there are also three notable advantages that are worth calling specific attention to:

1. Skrumble Network cannot be blocked by conventional firewalls.
2. Skrumble Network has user-controlled record storage, and once deleted, data will not be stored on any server.
3. Superior encryption of every conversation, message and file.

There will be no central point to block using a firewall because every user and every conversation is distinctive. This ensures complete anonymity, and unlimited access to Skrumble Network from anywhere in the world. Only jurisdictions where all outside Internet access is blocked will access be limited.



Archived copy · cryp2nova.com

SKM UTILITY TOKEN MEMBERSHIP: POWERING SKRUMBLE NETWORK COMMUNICATION

SKM is a utility token that will offer a certain class of membership based on the number of tokens owned. These membership privileges will enable access to various features and actions on the Skrumble Network ecosystem. Initial usage will be free, and the token will serve as means of access to unlock premium features, membership levels or utilize various extra functionalities.

Example Use Cases for SKM Utility Token



User A in Canada wants to begin a video call with User B in Thailand. Enabling video could be a premium feature. User A and User B would need to possess the set number of SKM utility tokens to perform the requested video call.



User A in France wants to send a file to User B in Brazil. The file exceeds the initial allowed file size requirements. User A must possess a certain token amount to send a larger size file than their current access permits.



User A in Colombia who wants to select to save a conversation they are about to have with User B in Australia. User Controlled Record Storage could be a premium feature. User B has confirmed they will participate in a saved conversation. Both users may then need to possess a token for storage.



User A in Germany wants to send a file to User B in the United States, but User A does not want User B to share the file with anyone. User A possesses a certain amount of token and will receive a notification if the file is transferred.



User A in Finland wants to send a file to User B in Scotland using a gated access key so only User B can access the file. User A owns a certain amount of tokens, User B is sent the file in pieces and only the access key given to User B from User A can unlock the file.

CRYP2NOVA

Archived copy · cryp2nova.com

Building a Self-Sustainable Ecosystem

By offering our open source SDKs and feature-rich product documentation (Open API), many different industries and backgrounds, like entrepreneurs, developers, and community members can leverage Skrumble Network's unique decentralized communication technology to service a vertical of their choosing.

PHASE 1: SKRUMBLE LABS INITIATIVES: INCUBATOR

During the initial phase of the ecosystem process, Skrumble will bring together 2-3 initial strategic partners to hold an incubator. Participants will brainstorm and build additions on top of Skrumble Network, like a Freelance Marketplace and Virtual Showrooms, to create a self-sustainable ecosystem.

PHASE 2: OPEN SOURCE SDKS & API

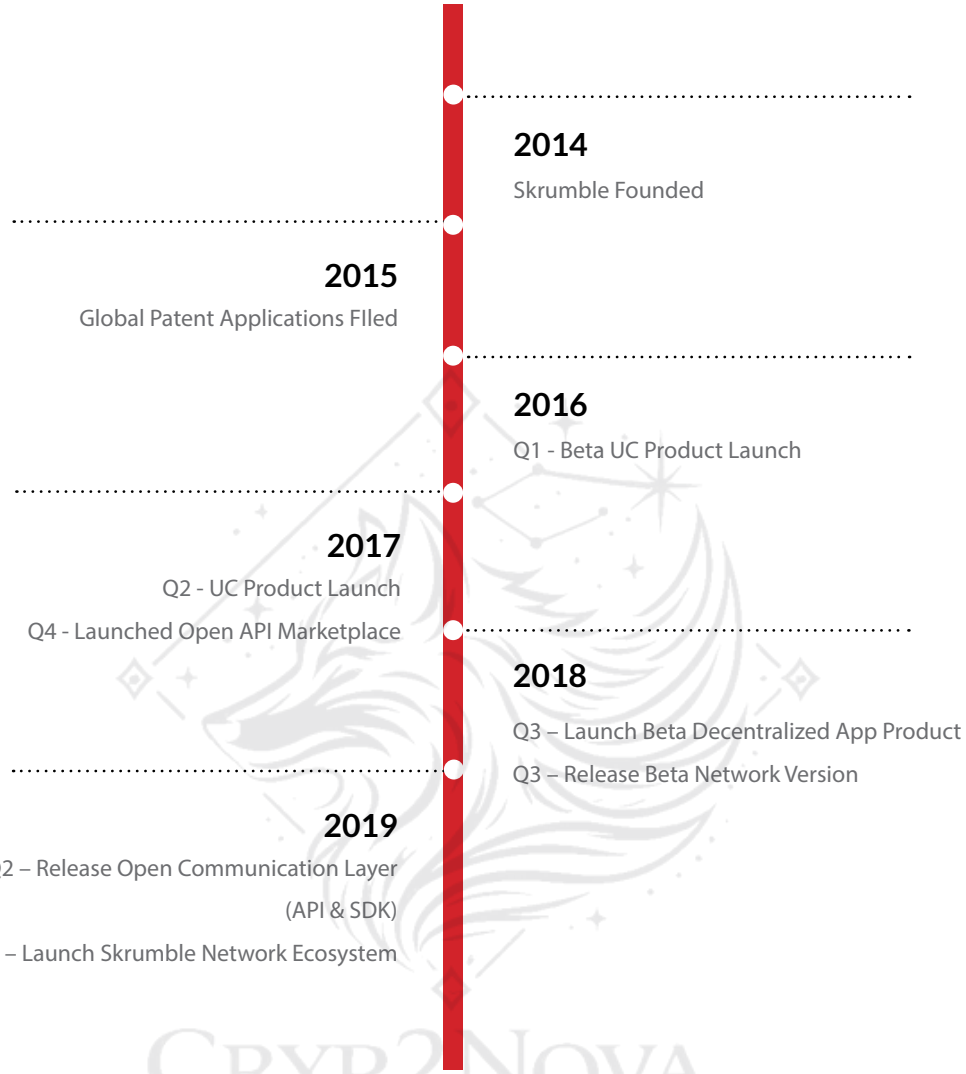
The second phase will include publishing the open source SDKs and API with open access for anyone to utilize the documentation to create their own product or service on top of the Skrumble Network.

The SKM token will be utilized by all users across the many different applications within the Skrumble Network ecosystem and those applications built separately on top. These various applications will also be incentivized for their offerings through SKM tokens. Therefore, the ecosystem will become sustainable through an innovative platform development, cost and reward system.

CRYP2NOVA

Archived copy · cryp2nova.com

SKRUMBLE NETWORK FOUNDATION ROADMAP



BENEFITS OF USING SKRUMBLE NETWORK

- Private
- Decentralized Server
- User-Controlled Storage
- Open API
- Secure
- Encryption
- Secure File Transfers
- Cannot Be Traced
- Anonymous
- Connect Globally
- Screenshot Notifications
- Cannot Be Blocked

Archived copy · cryp2nova.com

SKRUMBLE NETWORK USE CASES



1. Save & Delete Messages

While users will be using Skrumble Network to have private, secure and anonymous conversations, it is crucial to the functionality to include an option for users to save and store their conversation history. This can include messages, call history and file storage. During a P2P conversation, users will need to have two-party consent to approve the conversation being saved. In a group conversation, the administrator of the conversation will choose to save or not and the other participants will be prompted to opt in or not. If chosen not to save, nothing will be saved in the decentralized network. If chosen to save, the requested information will be stored in the cloud and will only be accessible to the participants in the conversation.



2. Secure File Transfers

Skrumble Network aims to provide users with a space to share their own data and send encrypted, secure files. Users will be able to send files using a gated access key, which means files will be sent in pieces from one user to another. The user receiving the file will be given a secret access code to unlock the gated content and bring the file back into one piece. Users will also be able to place notifications on the files they send. This is to ensure that if a file they don't want downloaded or transferred to another conversation is in fact downloaded or transferred, the necessary users will receive an alert immediately.

CRYP2NOVA

Archived copy · cryp2nova.com

ECOSYSTEM ADDITIONS FOR SKRUMBLE NETWORK

The SKM tokens will be consumed by all the users across different applications via the Skrumble Network. The various applications will also be incentivized through their offerings through SKM tokens. Therefore, the ecosystem will become sustainable through innovative platform development, cost and reward system.

The following initial applications are being planned for rolling out via Skrumble, Skrumble Labs Incubation Program or other third-party groups:



1. In-Context & Secure Online Payment Gateways

Most payment gateways are complicated, require high levels of technical expertise to set up and involve a separate and unrelated application or format. Skrumble Network will include an in-conversation end-to-end encrypted payment system. Be it through peer-to-peer money transfers within a conversation, e-commerce payments without leaving the page or simply communication methods like private messages, call and files.



2. Freelance Marketplace

In recent years, there has been an increasing number of Internet-based platforms centered around the idea of hiring freelancers for limited work and signing off on their expected wages. Skrumble Network has the communication and transactional functionality to build a freelance marketplace powered by smart contracts. Interested parties can easily select a freelancer, set the jobs parameters, and the freelancer will be paid accordingly when the requirements of the contract are fulfilled.



3. In-Conversation Smart Contract

Smart contracts are vital for conducting transactions and business remotely. Skrumble Network is poised to house smart contract templates for users to fill out and sign off on during their conversations and communication transactions. Be it agreeing to terms of service for lawyers and clients, documenting project expectations for remote workers, hiring a freelancer from the above-mentioned freelancer marketplace, or any type of transaction that requires the approval of interested parties. Terms get set, the smart contract in signed in-conversation and when the partnership is fulfilled, each party receives what was promised in contract.

CRYP2NOVA

Archived copy · cryp2nova.com



4. Virtual Showrooms

Utilizing video, messaging and presentation capabilities, Skrumble Network can easily customize that functionality to include simple P2P or group interaction points. These points of contact will be to provide users a platform to broadcast live video, share talents and receive in-conversation payments for their content.



5. Technology Partnerships

To further enhance the functionality and offerings of the Skrumble Network ecosystem, Skrumble will partner with key leaders in the blockchain and cryptocurrency industries. Aligning with these industry influencers, such as Aion Network's ecosystem and payment solutions, can enrich the opportunities for Skrumble Network users and further incentivize utility token holders.

CRYP2NOVA

Archived copy · cryp2nova.com

CONCLUSION: REVEALING A MORE HUMAN AND CONNECTED SIDE OF BLOCKCHAIN

Blockchain technology solves a lot of serious problems. Cryptocurrencies promote cross-border financial institutions and trading without hefty banking fees, smart contracts guarantee that professionals are only paid for services rendered and real-time data is accessible to track the transfer and ownership of goods. Due to the indisputable security measures, data management and communication opportunities, a decentralized network is an essential catalyst for more secure communication.

Blockchain combines the security of cryptography and unique data storage and transmission, with peer-to-peer networks to create a decentralized and trusted database. Major concerns about cybersecurity, data storage and threats to user information involving Internet-based communication systems become completely irrelevant with the use of a distributed ledger. Beyond solving these problems, blockchain presents unparalleled opportunities for innovation. To discover new methods for in-context online payment gateways and create new ways for people around the world to establish meaningful connections.

Decentralization presents endless possibilities for innovation and offers a solution for a unified, secure network providing end-to-end encryption, complete anonymity and communication opportunities to allow the world to connect, share and grow.

The Skrumble Network will have the ability to connect anyone from anywhere in the world in a secure and simple way and has the potential to truly democratize communication on a global scale. Using blockchain to establish communications in this way has never been done before. Skrumble Network will transform the use of blockchain technology from being used to process financial transactions to be an integral component in any application. With easily accessible, reliable decentralized communication, people worldwide will have the opportunity in a consensus-based environment to take back data ownership, never worry again about their security, and actively engage within different communities.

CRYP2NOVA

Archived copy · cryp2nova.com

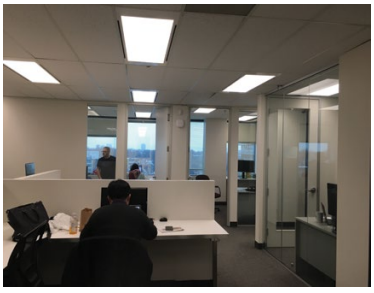


ABOUT OUR PARTNER: SKRUMBLE TECHNOLOGIES LTD

Launched in 2014, Skrumble Technologies LTD has become a well-established cloud communication company in the industry. With over 30 filed global patents, Skrumble leverages exclusive technology to build trusted solutions for Fortune 500 companies, IT consulting firms, call centers, professional services, police forces, security companies, governments, remote business, developers, and more. Over 400,000 users have leveraged Skrumble's various technology and communication solutions. It is Skrumble's mission to innovate methods of communication and create opportunities for people to connect globally on the most secure platforms possible. Skrumble has four main communication solutions. A unified communication platform launched in Spring 2017, published product documentation and a powerful open API for developers to program communication features into any application, white-label custom communication solution for companies in healthcare, law, consulting, and more, to have their own tele-platforms, and a recently released brand-new widget for developers to embed chat, voice and video directly onto any website or platform.

The Skrumble team continues to push communication barriers and innovates solutions for businesses worldwide to come together and grow. Skrumble Technologies LTD will provide development, blockchain expertise and technology licensing to power Skrumble Network. Skrumble Network will focus on decentralized communication technologies and building and fostering the network community. Skrumble believes that with true autonomy and data ownership, they can build trust and further unlock the vast opportunities of a true global network.

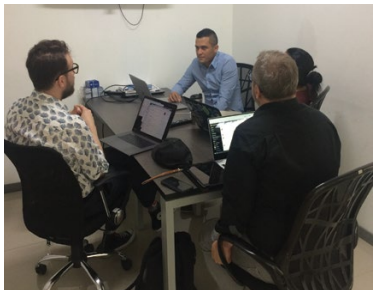
OUR OFFICES



Toronto Business
Development Office



Toronto Technology
Operations Office



Latin America Sales Office
Bogota, Colombia

Archived copy · cryp2nova.com

MEET THE KEY COMMUNITY MEMBERS



Eric Lifson
Co-Founder, Marketing



Michael Dabydeen
Lead Developer



Shelby Pearce
Marketing Manager



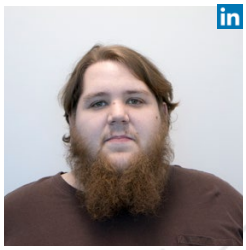
Gabriel Hernandez
Mobile Developer



Avenson Navalta
UI/UX Designer



Mikhail Berezovskiy
Full Stack Developer



Daniel Audino
Full Stack Developer



Danyi Lin
Full Stack Developer



Mauricio Bertanha
Full Stack Developer



Arnaud Ladoucetter
Mobile Developer



Leah Williams
Front-End Developer



Chantale Barnard
Front-End Developer



Eric Eddy
Mobile Developer



Akash Patel
Mobile Developer

CRYP2NOVA

Archived copy · cryp2nova.com

REFERENCES

Cendrowski, Scott (April 14, 2017). Fortune Magazine. China's WeChat is a censorship juggernaut. Retrieved on January 26, 2018 from http://fortune.com/2017/04/14/china-wechat-tencent-censorship-709-crackdown/

Coin Market Cap (2018). Cryptocurrency Market Capitalizations. Retrieved on January 21, 2018 from https://coinmarketcap.com/all/views/all/

CyberScout (December 27, 2017). Identity Theft Resource Center. Data Breach Reports. Retrieved on January 24, 2017 from https://www.idtheftcenter.org/images/breach/2017Breaches/DataBreachReport_2017.pdf

Facebook (2018). Making ads better and giving your more control. Retrieved on January 26, 2018 from https://www.facebook.com/help/585318558251813?ref=notif&notif_t=oba

Google (2018). How Ads Work. Retrieved on January 26, 2018 from https://privacy.google.com/how-ads-work.html

Greenberg, Andy (January 10, 2018). Wired. WhatsApp security flaws could allow snoops to slide into group chats. Retrieved on January 25, 2018 from https://www.wired.com/story/whatsapp-security-flaws-encryption-group-chats/

Hollerith, David (November 6, 2017). Bitcoin Magazine. Survey polls American awareness of cryptocurrencies and ICOs. Retrieved on January 20, 2018 from https://bitcoinmagazine.com/articles/survey-polls-american-awareness-cryptocurrencies-and-icos/

Martin, Ellen (October 2017). The Next Web. Why more people will use blockchain-based payment platforms over banks in the future. Retrieved on January 18, 2018 from https://thenextweb.com/contributors/2017/09/07/blockchain-vs-banks/

Pascual, Al, Marchini, Kyle & Miller, Sarah (February 1, 2017). 2017 Identity Fraud: Securing the Connected Life. Retrieved on January 20, 2018 from https://www.javelinstrategy.com/coverage-area/2017-identity-fraud

Perlroth, Nicole & Haag, Matthew (April 29, 2017). The New York Times. Hacker leaks episodes from Netflix show and threatens other networks. Retrieved on January 24, 2018 from https://www.nytimes.com/2017/04/29/business/media/netflix-hack-orange-is-the-new-black.html

Pullen, John Patrick (November 21, 2017). Fortune Magazine. Jennifer Lawrence reveals why she didn't sue Apple over her nude photo leak. Retrieved on January 24, 2017 from http://fortune.com/2017/11/21/jennifer-lawrence-apple-lawsuit-nude-photo-leak/

Sabin, Dyani (January 3, 2018). Futurism. Everything you need to know about cryptocurrency and why it's the future of money. Retrieved on January 17, 2018 from https://futurism.com/cryptocurrency-future-money-bitcoin/

Sethi, Rahul (September 26, 2017). After Google and Facebook, WhatsApp banned in China. Retrieved on January 26, 2018 from https://www.indiatoday.in/technology/news/story/after-google-and-facebook-whatsapp-banned-in-china-1052534-2017-09-26

Sherr, Ian (March 23, 2018). CNET. Facebook, Cambridge Analytics and data mining: What you need to know. Retrieved on March 26, 2018 from https://www.cnet.com/news/facebook-cambridge-analytica-data-mining-and-trump-what-you-need-to-know/

Toronto Star (January 13, 2018). World News. As protests wane, Iran lifts ban on messaging app Telegram. Retrieved on January 24, 2018 from https://www.thestar.com/news/world/2018/01/13/as-protests-wane-iran-lifts-ban-on-messaging-app-telegram.html

WeChat (2018). WeChat Help Center. Why doesn't my prior chat log appear when I log in to WeChat from a new device? Retrieved on January 26, 2018 from https://help.wechat.com/cgi-bin/micromsg-bin/oshelpcenter?t=help_center/topic_detail&opcode=2&id=1208117b2mai1410242meeYj&lang=en&plat=android&Channel=helpcenter

Yannik (June 26, 2017). Updated January 9, 2018. How long do Ethereum transactions take? Retrieved on February 1, 2018 from https://support.metalpay.com/hc/en-us/articles/115000373814-How-long-do-Ethereum-transactions-take-

SKRUMBLE NETWORK
Archived copy · cryp2nova.com