SKRUMBLE NETWORK

Decentralized Communication Powered By Blockchain

WHITEPAPER

Draft for open community review. Subject to change.

“Every once in a while, a new technology, an old problem, and a big idea turn into an innovation.”

Dean Kamen

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 Inc., 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 Inc., 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.

TABLE OF CONTENTS

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 by leveraging blockchain technology. This network will be a powerful, secure and accessible communication solution. This will enable open, private communication and create opportunities for people to connect globally and speak freely on the most secure platform possible.

There are currently thousands of innovators building world-changing solutions using blockchain technology. Fintech companies and governments are exploring cryptocurrencies, professional services are using smart contracts, supply chain managers are tracking inventory in real-time, and for the first time, assets are protected by indisputable, real-time ownership records. Due in part to the rise of blockchain, it is essential for Skrumble Network to innovate using this technology and take an in-depth look in to how decentralized networks have the power to be a catalyst for more secure communication.

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 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 communication ecosystem that will breakthrough traditional firewalls, assure user anonymity, guarantee content and data privacy, and will include features such as group and peer-to-peer messaging, calling, video, file transfers and more, in one place.

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.

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).

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.

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.

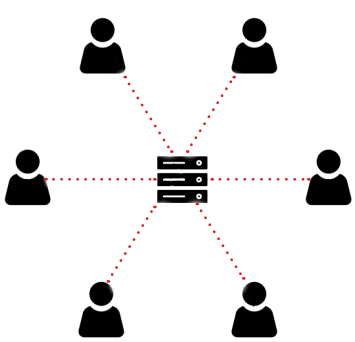
THE SOLUTION

1. Secure: Enhancing security with proprietary communication technology

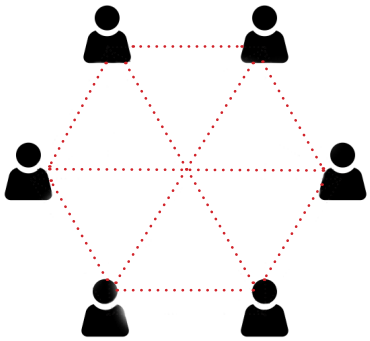
2. Decentralized: Distributed blockchain ledger supporting secure communication transactions

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.

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.

SKRUMBLE NETWORK: THE COMPLETE GLOBAL COMMUNICATION ECOSYSTEM

There is an undeniable need for secure, streamlined and standardized communication that requires minimal technical expertise to work with. 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 fulfill this need.

The first-ever complete communication ecosystem on a decentralized network will be built by Skrumble Technologies Inc. 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 users 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. Solving the security risks of current Internet-based communication systems through its distributed ledger, Skrumble Network intends to leverage unique and novel security technology.

Skrumble Technologies Inc 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.

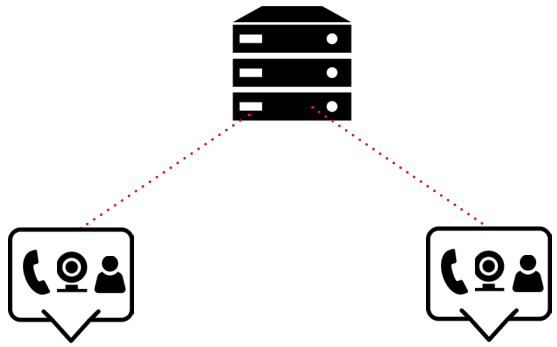
Skrumble Network Communication Features

- 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

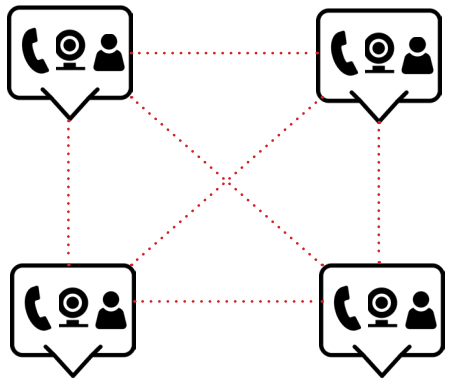
THE TECHNOLOGY POWERING SKRUMBLE NETWORK: TECHNICAL COMPONENT

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.



Current networks with centralized servers.



Skrumble Network –
Decentralized network with no central server.

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.

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:

1. Establish the initial communication session.
2. 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 incentivised 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.

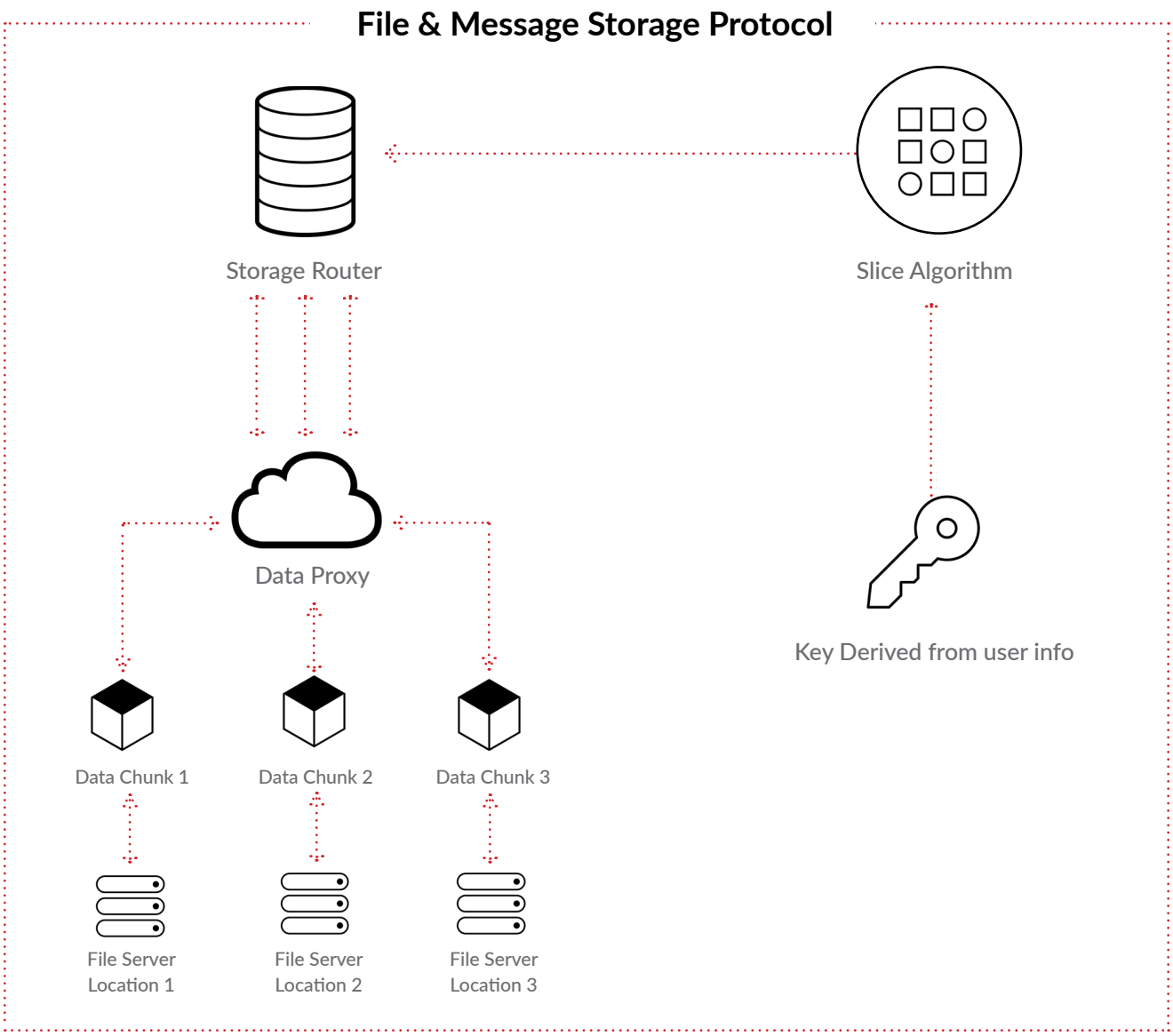
The Skrumble Network team will be constantly researching and evaluating new and faster methods of consensus and blockchain load times reduction. The team will be committed to improving the network on an ongoing basis to ensure user experience always remains seamless and consistent on the Skrumble Network.

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 Inc in 2015. 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.

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.

Industry Leading Features & 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 secure, private and anonymous communication ecosystem capabilities.

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.

SKM UTILITY TOKEN MEMBERSHIP: POWERING SKRUMBLE NETWORK COMMUNICATION

SKM is a utility token that will offer a certain class of membership based on the amount 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.

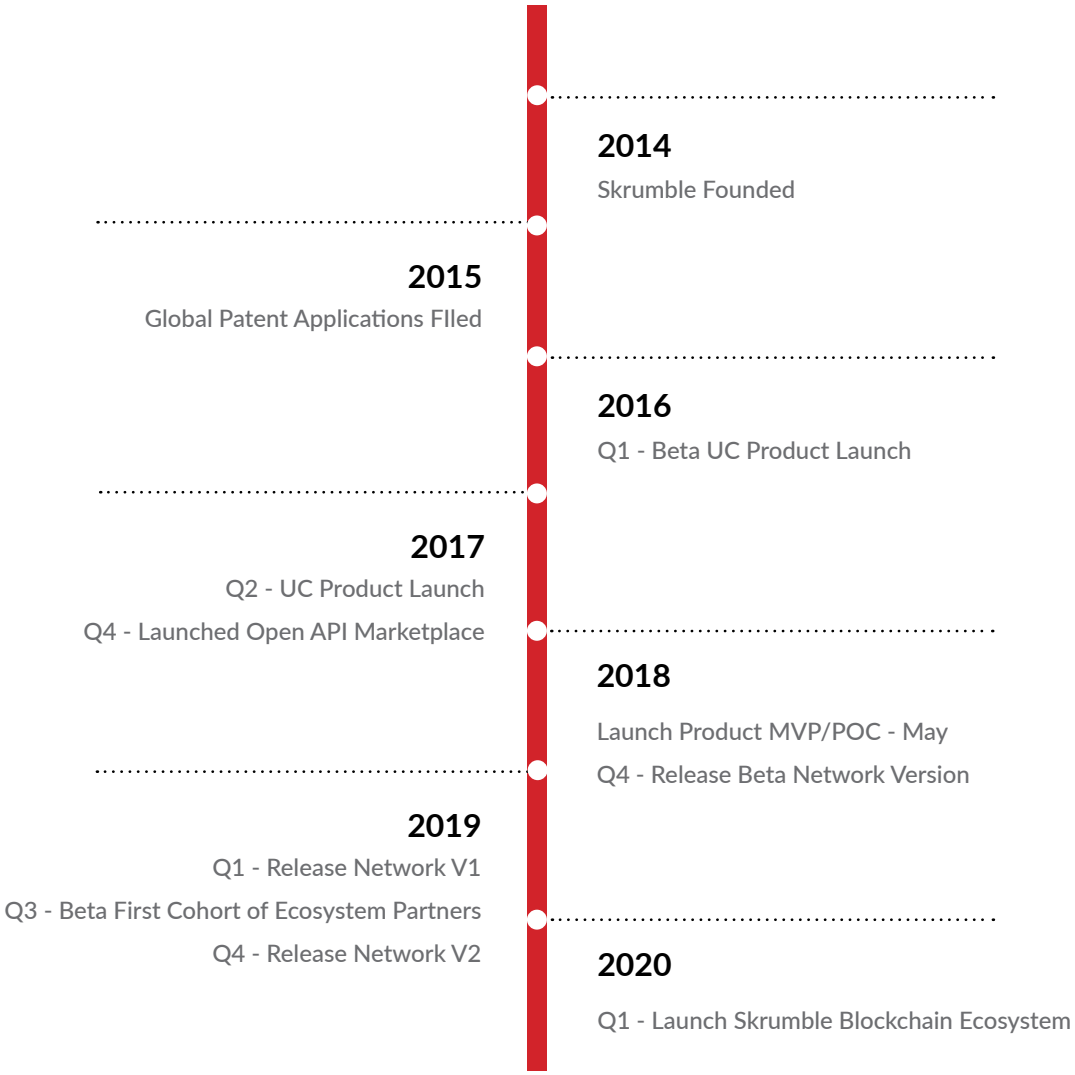
User Rewards: Surprise & Delight

- Active community members will receive surprise token rewards based on specific criteria. For example, a member who has initialized a certain amount of conversations will receive an extra amount of tokens.
- There will be random airdropped rewards for groups to promote community contributors
- Those that help mine, authenticate and promote the network community will also have opportunities to receive rewards.

Building a Self-Sustainable Ecosystem

- By offering our open API/SDKs, the community player/entrepreneur can leverage Skrumble's unique decentralized communication technology to service a vertical that they are choosing.
- The first phase of this process will be to incubate and bring on 2-3 initial strategic partners through the Skrumble Labs Initiatives, such as Vitual Show Room and Freelance Marketplace applications build on top of Skrumble Network.
- The second phase will be to offer the API/SDKs to anyone to create their own product or service.
- he 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.

TECHNOLOGY 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

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.

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.

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.

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.

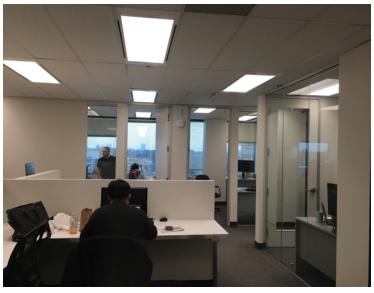
The Skrumble Network will have the ability to connect anyone from anywhere in the world in a secure and simple way and has the potential to truly democratize communication on a global scale. Using blockchain to establish communications in this way has never been done before. Skrumble Network will transform the use of blockchain technology from being used to process financial transactions to be an integral component in any application. With easily accessible, reliable and related 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.

ABOUT SKRUMBLE TECHNOLOGIES INC

Launched in 2014, Skrumble Technologies Inc 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.

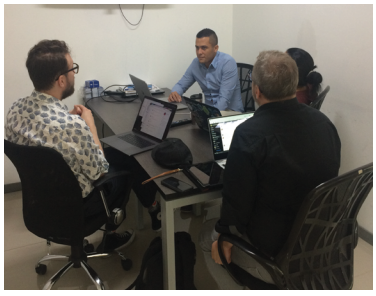
The Skrumble team continues to push communication barriers and innovates solutions for businesses worldwide to come together and grow. Skrumble Technologies Inc will provide development, blockchain expertise and technology licensing to power Skrumble Network. Skrumble Network will focus on decentralized 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

MEET THE TEAM

David Lifson
CEO & President

Tamir Wolfson
Executive Vice President

Vivi Herlick
VP of Operations

Eric Lifson
VP of Marketing

Christine Guo
VP Corporate Development

Johnathan Dwek
CFO - CFA

Aleksandra Mihajlovic
Product Manager

Michael Dabydeen
Lead Developer

Mikhail Khoroshun
Front-End Developer

Mikhail Berezovskiy
Full Stack Developer

Daniel Audino
Full Stack Developer

Danyi Lin
Full Stack Developer

Mauricio Bertanha
Full Stack Developer

Matt Mollon
Front-End Developer

Leah Williams
Front-End Developer

Chantale Barnard
Front-End Developer

Eric Eddy
Mobile Developer

Akash Patel
Mobile Developer

Gabriel Hernandez
Mobile Developer

Arnaud Ladoucetter
Mobile Developer

Siv Sathiyaseelan
Quality Assurance Analyst

Avenson Navalta
UI/UX Designer

Shelby Pearce
Marketing Coordinator

Wendy Lu
Marketing Coordinator

Wei Chen
Business Development Rep

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

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-