EncryptoTel

First secure cloud PBX

Virtual Public Branch Exchange: softphone infrastructure with blockchain-based VoIP communication and integrated traffic encryption for individuals and businesses

Roman Nekrasov

www.encryptotel.com

Table of Contents

Summary

A rapid increase in connectivity via technologies such as the internet, social networking and smartphones has brought about a step-change in our ability to communicate. At the same time, current audio and video calling software and instant messaging are insecure and prone to surveillance and exploitation by governments, corporations and malicious third parties, as well as being less efficient and cost-effective than might be expected.

EncryptoTel will combine the most promising technologies and markets in the telecommunications

sector, linking a virtual PBX (private branch exchange) with encryption, blockchain protocols and cryptocurrency payments to offer significant improvements in performance, functionality and competitive advantage. We believe this will enable us to become a leader in the PBX industry, with a diverse platform suitable for both individual use and office/business applications.

We have already completed a working beta of our core software that is actively being tested. The EncryptoTel application will ultimately be a multiplatform solution that enables users to connect and make VoIP calls using any device (desktop or Android SIP, Zoiper, 3CXPhone, X-Lite and more), and gain access to their PBX via popular messaging apps such as Telegram and Facebook Messenger.

This white paper details the scope and vision of EncryptoTel ahead of our crowdsale in May 2017. In the coming months we will be completing and launching our product, and making a gradual entrance into the global PBX market. The EncryptoTel token (ticker: ETT) will be the native currency for our services, offering discounts and other advantages, though it will also be possible to pay using other cryptocurrencies.

Context

We enjoy an unprecedented level of connectivity. Before the rise of the internet, 25 years ago, communication at a distance was costly and time-consuming. Even local phone calls incurred charges; national calls could be costly during peak times, and international calls prohibitively so for most people. Written communication by letter entailed a delivery time of at least a day, again at a cost. Sending a letter by Airmail typically meant a round trip of over a week.

Twenty years ago, as mainstream consumers first began to access the web, email was considered analogous to sending a letter due to the costs of using a dial-up connection. Bandwidth was limited and relatively expensive. It was not until the advent of ubiquitous broadband that we reached a tipping point. Audio and video calling over the internet – the ability to communicate in real-time and at the fixed cost of the connection – became possible and rapidly accessible for the first time, popularised by applications such as Skype, which was founded in 2003. Alongside this, social networking quickly became established, and with it the opportunity to communicate on a one-to-many and many-to-many basis with an ease that has been unparalleled in human history.

The mass adoption of the smartphone, which began no more than ten years ago, completed the now-clear picture of the ‘Always-On’ culture. We can communicate with anyone, anywhere in the

world, through a range of media including voice and video calls, instant text and picture messaging, individually or in groups, using a range of devices and for essentially zero marginal cost.

'The Internet is the most liberating tool for humanity ever invented, and also the best for surveillance. It's not one or the other. It's both.'

– John Perry Barlow, cyber rights activist

This remarkable serious of technological and cultural step-changes has resulted in opportunities that few would have imagined possible in previous generations: new methods and patterns of working, new structures of business and shifting social norms. But alongside the advantages there have arisen new risks, and the pervasive nature of the Always-On culture means we are often ill-equipped to recognise and mitigate these. Connectivity is so much a part of life that we rarely question it.

The surveillance society

In an environment of such ubiquitous connectivity and communication, data has become extremely valuable. Huge amounts of personal information are now routinely harvested by a range of different actors, including state-backed organisations, corporations and hackers. Whilst each of these have their own motivations, the line between them is frequently blurred. State-sponsored hacking is becoming commonplace, as in the case of the North Korea-instigated hack of Sony Pictures in 2014, in which personal information about employees, their families and the company was released, including emails, information about salaries and even unpublished films. Data held by the state and corporations may be hacked or leaked, by insiders or by malicious external parties, and occasionally released inadvertently through oversight and incompetence.

'Arguing that you don't care about the right to privacy because you have nothing to hide is no different than saying you don't care about free speech because you have nothing to say.'

– Edward Snowden, NSA whistleblower

In 2015, it became public that Samsung's smart TV could be used as a listening device;[1] documents made available by Wikileaks showed that the CIA intended to exploit this capability for a number of similar devices.[2] This is ostensibly being carried out in the name of national security, but the very fact of the leak proves that any data collected is also prone to loss and abuse. Similar strategies will doubtless be used by hackers as new techniques and vulnerabilities are made known. High-profile hacks of large organisations demonstrate that the standards of security are frequently inadequate, with lists of millions of plaintext user emails, passwords, addresses, social security numbers and more dumped on the web.[3] Repeated scandals involving celebrity photos have arisen from cloud storage being compromised, either through poor implementation or user error.

The reality is that in a hyper-connected world, data is not safe. We inevitably trust our personal data to the applications we use and the organisations that own and host them. We are often complacent about our personal security. Re-use of passwords and email addresses; carelessness about signing up for new services with social media accounts; lack of understanding or disregard about what happens to our data: all of these are habitual. More than this, there is an implicit collusion that our personal data is the price of using 'free' platforms and applications. Corporations collect extensive data about their customers, typically with little oversight or explicit permission from users. This information may be stored insecurely, and may be sold or otherwise made available to third parties.

It is our position that privacy is an important and fundamental right for every person. Freedom of speech is a critical check on the accumulation of power, and the ability to communicate freely without fear of surveillance – whether state-backed, corporate or by malicious individuals – is a pre-requisite for wider societal and personal freedoms. In the information age, knowledge truly is power. Data can be and routinely is used for profit or otherwise to the advantage of entities whose values are not aligned with those who involuntarily provide their personal information.

Content and metadata

It is widely accepted that the *content* of unencrypted communications – the text, audio and video

1 https://www.cnet.com/uk/how-to/samsung-smart-tv-spying/
2 http://variety.com/2017/digital/news/wikileaks-smart-tv-surveillance-1202003656/
3 See for example https://arstechnica.com/security/2016/09/plaintext-passwords-and-wealth-of-other-data-for-6-6-million-people-go-public/

material – is monitored, wholesale, by state-backed agencies and other organisations. In many cases this will remain a passive process, save for when specific information is sought and trigger words found. In other cases, the authorities will engage directly to block access to a platform or subvert discussion – a well-known strategy employed by the Chinese government, which is believed to fake hundreds of millions of social media posts per year.[4]

However, as strong encryption becomes more widely available and popular, new techniques have been developed to enable effective surveillance. So-called metadata becomes increasingly important: not the content of *what* is being communicated, but information pertaining to those communications: date, time, type of contact (phone call, email, social media post, video/audio call), location of participants, duration of calls, and any other data provided by apps during their usage. In some cases, there will be financial information that can be acquired, such as data concerning credit card transactions.

Whilst individuals may rightly be concerned about freedom of speech and financial privacy, for businesses the issue becomes acute. Even if the content of a communication remains private, financial records can uncover critical information that can be used by competitors for industrial espionage. Companies, suppliers, employees, contractors and customers are all connected by an intricate web of transactions. Any leaked information can (and inevitably will) be used to the advantage of competitors and malicious third parties.

In the early 1990s, when the Cypherpunk movement began to advocate the use of strong encryption in the interests of protecting financial privacy, concerns about state-sponsored surveillance and corporate control of information, few of even the most forward-thinking critics grasped the sheer volume and breadth of data we would transmit and need to protect a quarter of a century later.

EncryptoTel will launch a suite of tools that will enable user-friendly and secure communication, by combining existing applications and technologies with custom-built new ones. Privacy is a right, but it is one that must be exercised actively and deliberately.

Background and Vision

EncryptoTel's vision is to realise an open, reliable and above all secure means of communication

4 https://www.washingtonpost.com/news/monkey-cage/wp/2016/05/19/the-chinese-government-fakes-nearly-450-million-social-media-comments-a-year-this-is-why/?utm_term=.09a5c955eb20

that can be used regardless of the users' locations. The company's main product is a flexible and comprehensive PBX service – that is, an internal private network that can be shared by a large number of users, but one that can also interface with the external telecommunications network.

PBX and IPPBX

A **private branch exchange** (PBX) is an internal telephone exchange or switching system used within a single office or organisation.

The chief benefits of a PBX are cost and convenience. Using an internal system allows employees to communicate directly without requiring the use and expense of external telephone lines. Outgoing calls by a large number of employees may be shared on just a few lines. Meanwhile, additional services can be integrated with the switching system, such as routing calls to intercoms and other destinations.

Some form of PBX is now the norm for businesses, particularly in large organisations, where it is unnecessary and inefficient to rent many external lines. **Internet protocol PBX** (IPPBX) systems adopt the same approach as the older traditional PBX, with the difference that they use computers and existing internet infrastructure to route calls within an organisation. This allows for greater efficiencies and versatility, since digital facilities can be integrated with the telephone system – including message storage and connection to voice-over-IP (VoIP) services – while still using a limited number of lines to interface with the external telephone network. Since almost every business is connected to the internet and uses high-speed broadband infrastructure, IPPBX offers substantial advantages at a low cost overhead when compared to legacy telecommunications systems.

EncryptoTel will offer a virtual IPPBX, as well as easy integration of encrypted VoIP into existing IPPBX networks.

We want to offer this service regardless of whether our customers are a single individual or a large corporation with many thousands of employees. Our software and underpinning blockchain infrastructure allows us to provide for the needs of anyone, regardless of scale, thanks to the

economies it offers in micro-transactions and in decentralising operations. Without blockchain technology, EncryptoTel's proposition would simply not be economically viable.

The idea for EncryptoTel is rooted in the development Team's experiences of working for a telecommunications company. Familiarity with both traditional telecommunications infrastructure and blockchain technology raised the possibility of creating a product that was superior to anything currently on the market. The Team has worked full-time on the project for several months and has a public beta application. A crowdsale will provide the funds to finish the product to a high standard and market it properly.

The opportunity for EncryptoTel

The Telecoms market is currently one of the fastest-growing sectors of the economy. Whilst the legacy telephone system is seeing reduced usage, new internet-based technologies are rapidly expanding, offering significant benefits of cost and convenience over older approaches. It is now possible to communicate by video chat via Skype, Facebook Messenger and many other platforms using only a smartphone, and at no greater cost than that of the internet connection.

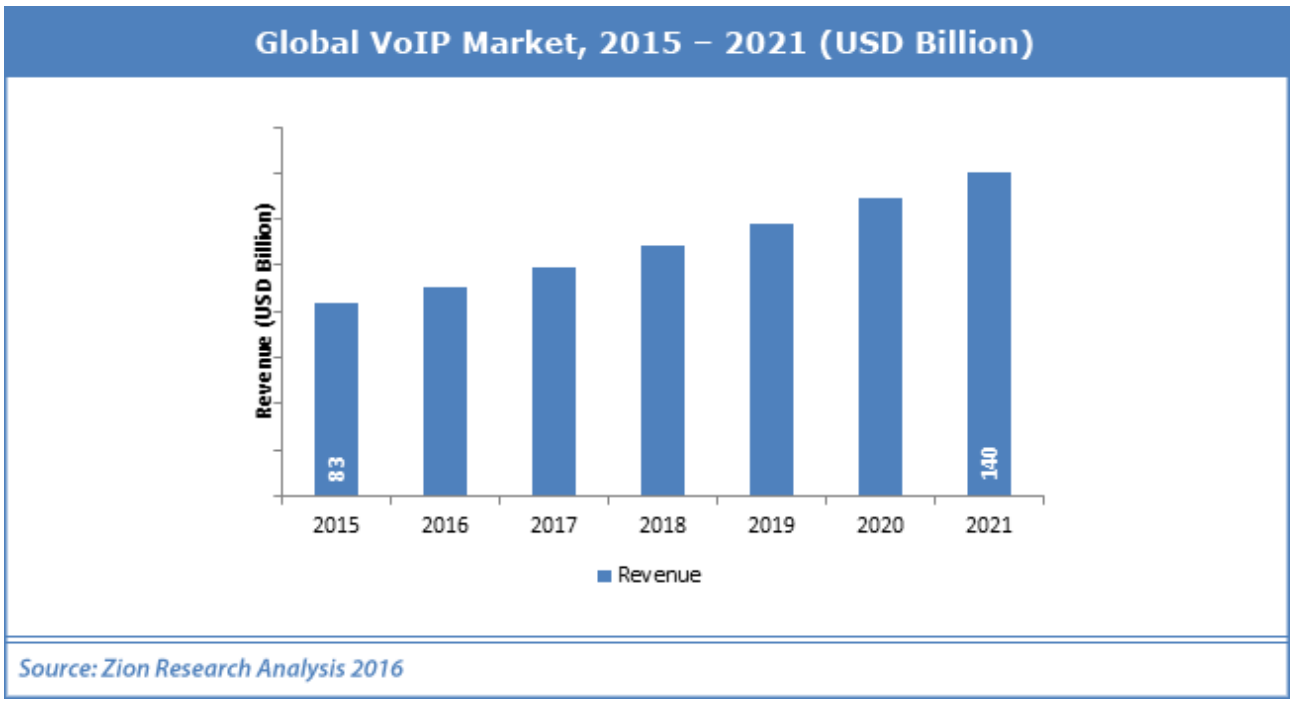
'The telecom sector continues to be a critical force for growth, innovation, and disruption across multiple technology industries.'

– Deloitte[5]

'Global demand for VoIP services market was valued at over USD 83 billion in 2015, is expected to reach above USD 140 billion in 2021 and is anticipated to grow at a CAGR of above 9.1% between 2016 and 2021.'[6] Due to their efficiencies and use of now-ubiquitous broadband infrastructure, VoIP services have the potential to drive traditional calls via both landline and mobile telephones out of the market.

5 https://www2.deloitte.com/us/en/pages/technology-media-and-telecommunications/articles/telecommunications-industry-outlook.html

6 http://www.marketresearchstore.com/news/global-voip-services-market-is-expected-to-reach-above-231



The closest analogue to EncryptoTel would be a company that provides a Virtual PBX service, as EncryptoTel will offer, and be able to sell phone numbers for users anywhere in the world. Companies that do so currently have to collect and disclose customer information when required by regulators. Additionally, no PBX company accepts cryptocurrency payments and leverages blockchain technology for their underlying infrastructure. At the present time this means that EncryptoTel has no direct competitors and offers a unique approach and package of services.

Having worked in the PBX sector, EncryptoTel's Team is familiar with the products that exist on the market, has conducted extensive research and has collected feedback from customers about the major problems with current PBX systems. The Team's combined experience will be applied to creating a new product that is more flexible and wide-ranging than anything currently available, circumventing or solving the drawbacks that exist in mainstream telecommunications systems and offering many new features. The result of the work to date is an application that enables:

- Private communication
- Fast deployment of fully-fledged PBX
- Reduction in call costs to external lines
- Absolutely free and extremely secure communication within the network
- Ability to pay with cryptocurrency

- Additional transparency of control and monitoring due to the nature of blockchain technology.

EncryptoTel's approach avoids all of the existing disadvantages of virtual PBX systems, and adds unique new features. In terms of payment, the use of cryptocurrency offers for the first time genuinely anonymous access to the service. As a result of this collection of features, EncryptoTel stands apart from any existing virtual PBX service, holds a number of competitive advantages, and has the potential to occupy a significant fraction of the market.

Platform and technology

As a virtual PBX, EncryptoTel is designed to be highly accessible to its customers. It will not require any telecommunications infrastructure above an internet-connected device (smartphone, tablet, laptop, desktop). Office equipment such as telephones are not necessary, though these can be connected to the service via a VoIP gateway if desired. Any modern PC can serve this purpose, since it is simply a matter of interfacing the IP network with the regular telephone network.

Multiplatform, unified approach

EncryptoTel takes a multiplatform approach and can be used with Windows, Linux, iOS and Android. It supports video and audio calls, as well as instant messaging. Numerous free apps can be used with EncryptoTel, such as Zoiper, X-Lite and 3CXphone. These are also multiplatform 'softphone' apps that make audio and video calls over the internet, rather than requiring dedicated hardware. The aim is to make EncryptoTel as versatile and accessible as possible, reducing the frictions to getting started with the service to near zero. In due course we will integrate EncryptoTel with other popular messaging apps including Facebook Messenger and Skype.

Call encryption

The beta version of EncryptoTel already offers traffic encryption based on SIP/TLS technologies. This ensures that a basic level of encryption is set up when a client-server connection is established in order to avert interception and unauthorised access.

EncryptoTel is currently working on the development of its own secure connection network, which is based on two network contours (internal and external), and which includes several elements

including certification authority, organisation of VPN, distributed encrypted file system, HTTPS server, and so on. The company will implement its own security protocols using certificate encryption based on blockchain protocols.

User experience

Due to its integration with existing softphone applications, the EncryptoTel user experience will be seamless. Customers who use popular apps like Zoiper will continue to use them in the same way, with the difference that the apps will be integrated with EncryptoTel's software and all of their calls encrypted.

Pseudonymous payments

As explained above, maintaining privacy is not simply a matter of encrypting the content of a call or other communication. If metadata is available then this can be used to glean valuable information about the nature, purpose and participants of a call. Financial transactions are particularly valuable in this regard, since they are generally linked to a credit card or bank account, offering extensive personal data. Cryptocurrency payments will address this flaw in current PBX systems.

Most cryptocurrencies are not strictly anonymous, but pseudonymous. Addresses are essentially random strings of alphanumeric characters. The blockchain is transparent and it is possible to see where money is moving, tracing transactions back to their source. However, without additional information it is impossible to see who those addresses are associated with.

In reality, poor practice on the part of users can leak information and means it is often possible to glean data about who is transacting. Nevertheless, it is quite possible to ensure privacy through best practice. Further services such as mixers radically increase the complexity and cost of tracing transactions. Privacy-centric altcoins such as Dash and Monero provide yet further facilities for protecting the identities of cryptocurrency holders.

EncryptoTel will make it straightforward for users to pay for its services with cryptocurrency, so that not only will it be impossible to know what is being communicated, but also who is communicating. For existing cryptocurrency users, there will be an external plug-in to enable calls directly from the Waves lite client to allow easy payments.

Functionality offered by EncryptoTel

The following services and more will be offered by EncryptoTel. These will be charged on a subscription or per-call basis, with discounts offered for payments with the EncryptoTel token (ETT).

- **Call redirection.** Ability to redirect an incoming call to another phone number. **Example:** The user can redirect calls to a local number, or to multiple local numbers based on who is calling and when.
- **Two-factor authentication (2FA).** An additional layer of protection will be offered for services such as exchanges and crypto-wallets. **Example:** In addition to username-password login, users will receive a call, text message or other authentication details before access is granted.
- **Encryption and traffic protection.** Traffic is reliably encrypted and protected with the latest encryption protocols. **Example:** For instances such as important business negotiations or for individuals concerned about privacy for any reason, this functionality will protect data from audio interception and man-in-the-middle (MitM) attacks.
- **Free communication.** Every subscriber will receive a free internal number for the network. **Example:** Talk within a network, one-on-one or with a group, free of charge.
- **Hide a phone number.** Phone numbers used for outgoing calls will be masked from detection by a receiving device. **Example:** Conduct negotiations and other communication without revealing your direct subscriber's number.
- **Scenario execution.** This makes it possible to create scenarios that are executed via SMS/MMS and calls. **Example:** Users can send cryptocurrency to predetermined address by calling a designated number and entering a pin-code via their phone's keypad.
- **Multiplatformity.** EncryptoTel can be used with all operating systems, IP-phones and gateways. **Example:** Users will have access to deployment and control of their PBX via any device – mobile terminal, desktop workstation, tablet, etc.
- **Conversation recording and data storage.** Recordings of conversations or other important data can be securely stored. **Example:** Optionally turn on storage for all negotiations and files. This stored data can only be decrypted by the owner using EncryptoTel's integrated

blockchain technology.

- **Call tracking.** Monitor traffic resources. **Example:** It is possible to create a unique number for every advertisement resource. Statistics can be downloaded and progress monitored from the user's account.
- **IVR (interactive voice response).** Voice recognition facilities. **Example:** Create pre-recorded instructions for people who call you, optimising processing for incoming calls.
- **Video call.** Face-to-face calling. **Example:** Call someone using a camera or begin a live to-camera broadcast.
- **Reminders.** Synchronise your app with your calendar. **Example:** Prompt reminders for important events via call or SMS.
- **API.** Interact with the EncryptoTel service on the back-end level. **Example:** Integrate your CRM or another system with EncryptoTel's PBX and gain access to all its services, with the opportunity to build new facilities on top of it.
- **AI and text interaction.** Perform basic set-up and control for popular messengers using EncryptoTel's artificial intelligence bot. **Example:** Initialize a call via Telegram, XMPP/Jabber client with the help of a simple message, such as '*Call the number +1 … 1 from the USA zone number, then call me back on the number +1 … 2'.*

Revenue generation and return-on-investment

EncryptoTel will charge users for certain services on either a subscription or pay-as-you-go basis, depending on the customer's preference. Sales and revenues statistics will be clearly visible thanks to the transparency of the blockchain.

We will be occupying the telecommunications market among cryptocurrency and blockchain companies within a year, and will attract a large number of individual users by means of low tariffs, broad functionality and an aggressive advertising policy. Having established a presence we will consolidate and expand this amongst regular users and large companies alike.

ETT tokens will be sold during EncryptoTel's crowdfund. Although different cryptocurrencies will be used, ETT will bring discounts over other currencies, placing it in demand as a way of paying for services. Rising demand from end users will increase the price.

Subscription vs per-minute charging

We want to make EncryptoTel a flexible service that allows customers to pay however they want. We will initially offer two payment structures.

1. **Pre-paid tariff**. This will be a fixed monthly amount suitable for customers such as businesses that make large volumes of calls every month. This can come with a discount on a direct number and additional options such as IVR, answerphone, call tracking, and so on.
2. **Pay as you go**. This will entail making calls at the standard price, so long as your account has sufficient funding. Customers will always be able to make secure calls within their PBX network for free.

Aside from direct buy pressure on the native ETT token as a means of securing discounted services, revenues from other payments will be distributed to investors on a regular basis. The easiest way to achieve this would be via a regular dividend, but this would incur regulatory complications. A similar way to achieve the same ends is to make a periodic buy-back of the ETT token from supporting exchanges, and then burn it, reducing available supply and driving up the price.

Voting rights

Aside from offering a discount over other payment methods, ETT will enable holders to have a voice in the running of the company. Holders will be able to vote on key strategic decisions, albeit in an advisory rather than legally binding capacity.

Funding milestones

EncryptoTel has already completed a working beta version of their product (see www.EncryptoTel.com), with several of its core features implemented. Further funding is required to finish development and market the result. EncryptoTel has outlined a series of budgets that we project will enable us to complete different scenarios:

1. **$100,000+**. This would allow us to create a fully-functional commercial product that could compete in the global PBX market. Funds raised above this milestone would be spent improving stability, implementing new encryption methods and redesigning the user experience for greater accessibility.
2. **$250,000+**. Realisation of EncryptoTel's own traffic encryption protocol based on blockchain

technology. This would include the release of mobile applications for Android and iOS for safe and easy communication within a PBX.

3. **$1,000,000+**. This would enable EncryptoTel's penetration of the international market with an aggressive policy of expansion, allowing us to occupy a more significant fraction of the telecommunications industry, including entry into PBX models that are already configured and customised for the most common tasks in the B2B, B2C and B2G sectors. It would allow us to acquire the necessary licences to allow us to provide customers with telecommunications services and allocate numbers to them ourselves.

EncryptoTel Team

The EncryptoTel Team has extensive experience in the fields of blockchain technology, SIP telephony and cloud PBX development.

Every member of the Team has worked in telecommunications and its associated technologies for a minimum of six years and have together been involved in far-reaching projects – including the creation of information systems from scratch. They are experts in every aspect of the digital currency world, from mining to blockchain integration. The Team used to work together for the same telecommunications company, and its members have known each other for more than five years. It was during their time working together that they realised they could revolutionise the digital market for IPPBX systems.

EncryptoTel has already built a working beta product that can be tested by prospective customers and investors. The Team has previous participated in the realisation of a number of projects across the areas required for successful implementation and launch of EncryptoTel, including the creation of billing systems, softphone and multifunctional ERP systems. Moreover, they have sound experience in the integration of these systems into the business process.

EncryptoTel has already spent considerable time and resources in designing their core product and completing a working beta. The Team's experience will help them to address any issue that arises during the implementation process, and they have the track record to make such a complicated project a success.

For more information, visit www.EncryptoTel.com