Protex: The Future of Exchanging Data Securely

Protex, LLC

September 20, 2017

Abstract

Data runs the world. From analyzing financial trends to recommending a movie, it permeates all aspects of life. For years, databases and memory units have been used to store this data. Because of this, data has become highly centralized - living primarily in the databases of large corporations and governments. Over time, individuals have lost the ownership of their digital footprints, and the rights to its privacy. The existing structure has led to the monopolization of data, and has considerably decreased the privacy, security and anonymity of individuals.

Until now.

The Protex platform builds on Ethereum's idea of decentralization and smart contracts [1]. By removing the need to store user data in vulnerable locations, Protex saves companies money, time and liability, while providing users significantly increased privacy, and a new stream of income. Protex is the future of exchanging data securely.

Contents

1 Market Analysis **3**
- 1.1 Introduction . . . 3
- 1.2 Web Browsing Data . . . 3
- 1.3 Mobile Application Data . . . 4

2 Use Cases **5**
- 2.1 Location and Movement Data to Improve City Infrastructure 5
- 2.2 Targeted and Effective Advertising Based on Web Searches . 5
- 2.3 Accurate Recommendation System Based on User Data . . . 6

3 Protex Token **6**
- 3.1 Profit Sharing . . . 7

4 Protex Blockchain **7**
- 4.1 Features . . . 7
- 4.2 Data Fields . . . 8
- 4.3 Secret Sharing . . . 8
- 4.4 Plasma and Scalability . . . 13
- 4.5 Data Science Functionality . . . 13

5 Protex Chrome Extension **13**

6 Protex Mobile App **14**

7 Protex Exchange Portal **16**

8 Token Sale **18**
- 8.1 Pre-Sale . . . 18
- 8.2 Token Sale . . . 18

9 Future Plans **20**
- 9.1 Roadmap . . . 20
- 9.2 Budget Plan . . . 23

10 Team **24**

11 FAQs **25**

1 Market Analysis

1.1 Introduction

As the world has become increasingly reliant on data and analysis, security has become one of the most important features of technology. Since 2013, there have been 9,053,156,308 examples of notable data breaches on the internet [2]. Some of these data breaches have inconsequential effects, but many can be potentially devastating. For instance, in 2011 hackers compromised data from up to 75 clients of marketing giant Epsilon International, including Best Buy, JP Morgan and Target. Together, this headache cost Epsilon over $4 billion in damage [3]. Each year, corporations are recording more personal information about individuals, and without a significant improvement in privacy and security, the number of people impacted will increase. Not only will sensitive data be at risk, but companies will be liable to more billion-dollar attacks such as the one on Epsilon. Fortunately, the contributions of cryptography and blockchain have torn down existing assumptions about security and privacy and have opened the floodgates for exciting innovation in this space.

Currently, the majority of corporations and governments store personal records in traditionally structured databases [4]. While there are levels of security implemented into these databases, there are still several vectors through which they can be attacked. In addition to sub-optimal security levels, databases also present an issue of data monopolization and centralization. As most corporations and governments keep data in dedicated computing centers, the access to it has become very privatized and poorly distributed.

1.2 Web Browsing Data

The problem of centralized data storage is especially prevalent when it comes to web browsing data. By now, everyone is familiar with the idea of targeted advertising. Companies are able to cater their campaigns to individuals specifically based on their interests. They do so by monitoring and analyzing web searches with browser cookies. In short, browser cookies are small pieces of data used to store state information about a web browsing session [5]. While they provide several benefits, they also introduce the threat of several serious attacks [6].

- **Cross-site Scripting:** Attackers can place exploits in a cookie, usually before being set, which will fetch the payload from the cookie later

on.

- **Cookie Tossing:** Attackers are able to craft subdomain cookies and send them along with legitimate cookies, making the website accept both. Sometimes, the website might accept the malicious subdomain cookie first, making it the valid one.

- **Session Fixation:** Attackers can encourage users to accidentally log-in as the attacker on several application levels by using a different session ID.

- **XSRF attacks:** Cookies allow for something called a cross-site request forgery (XSRF) attack, exploiting the fact that websites cannot distinguish whether actions are performed by a user or not. Attackers can deliberately perform actions as if the user initiated it, by essentially spoofing their identity.

By storing all the useful information that cookies provide on a secure blockchain, Protex can take advantage of the same benefits, without exposing any user to the attack vectors above.

1.3 Mobile Application Data

Another common source of data that lends itself to significant attacks is mobile app data - specifically location tracking data. Synack, a crowd-sourced security company, conducted security research on the safety of location tracking in mobile apps. Synack researchers compiled tracking data from tens of thousands of app users, all without any personal information attached. Even with the personal information removed from the tracking data of each individual, researchers at Synack were able to identify thousands of users. This was done by using context clues such as the knowledge of a specific location like the address of a celebrity, athlete or politician [7]. Compromising this location data is not only a serious breach of safety, but potentially life-threatening. Introducing a layer of security with blockchain technology helps both sides of this issue. Clearly it allows users peace of mind knowing that their identities and locations are safe, but it also alleviates any legal concerns of the app companies using location tracking. By using a distributed, peer-to-peer storage model, blockchain solutions can make this data substantially more protected, fault-tolerant and easier to access securely.

2 Use Cases

While the use cases for the Protex platform are endless, here are a few common examples to illustrate the scope of this project.

2.1 Location and Movement Data to Improve City Infrastructure

Using data to improve infrastructure in large cities has become a very important and prominent issue in the 21st century [8]. With the advent of GPS tracking devices like mobile phones, it is now easier than ever to gain information about how and when people move throughout a city. There are already efforts to execute on this idea, however, Protex makes it significantly easier and more secure to do so. For instance, as Protex scales, its blockchain will aggregate tremendous amounts of movement data from individuals in large cities. Because of the layer of privacy, governments and civil engineers will be able to benefit from this information without ever putting an individual's identity at risk. In addition to the increased privacy of users, the platform also makes it easier for these entities to perform their data analysis, as all of the data is stored in a standardized and efficient manner. Finally, the platform relieves governments and companies of the liability and moral implications of storing an individual's movement history. By decentralizing and anonymizing this information, Protex benefits both parties.

2.2 Targeted and Effective Advertising Based on Web Searches

Advertising companies are invasively using web searches to target their campaigns more effectively [9]. They do this by retrieving and storing information via a user's cookies, explained above in section 1.2. However, the introduction of blockchain technology allows for a paradigm shift in how to safely exchange information from users to corporations. There is no longer a need for advertising companies to monopolize search data and store sensitive information like cookies in insecure locations. Protex allows users to send their cookies to the blockchain with the confidence of security and anonymity. Additionally, advertising companies are no longer required to store this data on their own, eliminating the liability associated with a potential data breach. Protex can bridge the gap between users and ad companies by serving as a layer of security and standardization between the two.

2.3 Accurate Recommendation System Based on User Data

The Netflix Recommendation problem is commonly studied in the field of data science [10]. In its simplest terms, the task is to intelligently recommend a movie to a user, based on inputs like viewing history. In 2007, Netflix exposed a fundamental flaw of storing its users data centrally. Netflix offered a prize for groups to perform interesting machine learning tasks on their data. For obvious privacy reasons, personal information was dissociated from each user's viewing history. Despite this step, researchers at the University of Texas at Austin were able to identify the users because of other context clues on sites like IMDB. As stated by author Robert Lemos, "... the research demonstrated that information that a person believes to be benign could be used to identify them in other private databases" [11]. We propose that Protex solves this problem entirely. The Protex platform is able to provide all the machine learning tasks that Netflix requires without needing to locally store data by each user in a central hub. Protex eliminates the risk of identifying an anonymous user because the data is protected on the blockchain and separated from any external personal information.

3 Protex Token

Protex uses an ERC-20 Token (PTX) to perform data exchange on its platform [12].

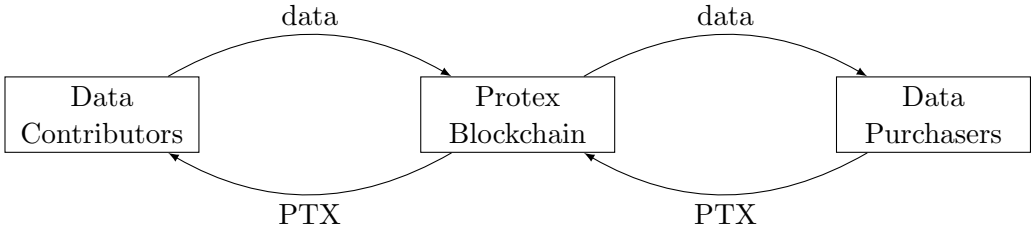


Figure 1: Data Pipeline

The value proposition of the PTX token, at a high level, is as follows: users willing to contribute their data to the Protex blockchain are rewarded in PTX, and companies or individuals purchasing market data from the Protex blockchain pay in PTX. Protex contributors (or data volunteers) are

able to set sharing preferences in both the Google Chrome extension and Protex mobile app described below in sections 5 and 6. With the app and extension, users can select to share all, none, or a particular combination of the data fields that Protex supports - listed in section 4.2. Depending on the sharing preferences, Protex contributors are paid via a profit sharing model.

3.1 Profit Sharing

When data is purchased from the Protex blockchain, the PTX tokens are distributed evenly among the users who contributed the data that was purchased. The only extra fee associated with data purchases on Protex is the gas for the execution of the smart contracts. This way there is no need for Protex data contributors to pay any extra fees for volunteering their information.

Because the Protex platform offers individuals an additional stream of income, PTX incentivizes users to adopt the platform. We believe this will make the Protex blockchain the market standard in storing user data, and the go-to source for large companies to buy user data.

4 Protex Blockchain

In 2014, the Ethereum project introduced "an open blockchain platform that lets anyone build and use decentralized applications that run on blockchain technology" [1]. One of the key innovations of Ethereum is the ability to safely execute smart contracts, opening a door to even more interesting applications of blockchain technology.

4.1 Features

Protex takes advantage of the Ethereum platform by building a decentralized app to more securely exchange data. Heres what the blockchain allows Protex to do:

- Security: With modern cryptography, Protex is able to keep all user records secure on the blockchain. Any piece of data is divided and shared according to Shamir's Secret Sharing algorithm (explained below in section 4.3) [13].
- Privacy: Using onion routing, Protex is able to obfuscate the existence of any data contribution or data purchase on the platform. In other

words - no one will know when data is given or taken, so context clues cannot be used to identify users [18].

- Anonymity & Fungibility: Protex can offer anonymity with every data contribution by hiding all personal information associated with it. The blockchain stores the data and only the data - there is no record of any one user's contributions. Protex can still offer insights based on demographics, however, by sharing this information in shards.

4.2 Data Fields

Listed below are the data fields which the Protex blockchain currently supports. The blockchain is easily extensible, however, to other future sources of data. For example, an intended use case for Protex is to securely store state and location information about self-driving vehicles as more end points are built.

- **Location:** For location-based applications, Protex can store a JSON of (x, y) coordinates for a user's movement. These can be stored and exchanged on the Protex platform over any length of time.
- **Web Searches:** Protex is able to store information about search engine queries and sequences.
- **User Activity:** When using the mobile app or Chrome extension (sections 5 and 6), Protex users can share sequences of actions - like which links they click on, which apps they use, or how far they scroll.
- **Impressions:** The Protex Chrome extension (section 5) can store the length of impressions for any piece of media on a website. This data can provide ad companies insights on which pieces of media resonate most with different demographics.
- **Other:** As explained above, the Protex platform is capable of extending to many other fields of data. Among data fields we plan on supporting in the future are: self-driving car data, health-care information and wearables data.

4.3 Secret Sharing

We propose that data contributions to the Protex private chain are cryptographically secured by a secret sharing algorithm. By using a threshold

scheme explained below, the data can be more efficiently retrieved without the sacrifice of security [13]. Below we show how to divide any data D into n pieces in such a way that D is easily reconstructable from any k pieces, but even complete knowledge of $k-1$ pieces reveals absolutely no information about D. This technique enables the construction of robust key management schemes for cryptographic systems that can function securely and reliably even when misfortunes destroy half the pieces and security breaches expose all but one of the remaining pieces [14].

The data, or secret S can be divided into n pieces of data $S_1, ..., S_n$ such that:

1. Knowledge of any k or more S_i pieces makes S easily computable.
2. Knowledge of any $k-1$ or fewer S_i pieces leaves S completely undetermined.

This scheme is called a (k, n) threshold scheme. If $k = n$ then all participants are required to reconstruct the secret.

Suppose we want to use a (k, n) threshold scheme to share a secret S, without loss of generality assumed to be an element in a finite field F of size P where $0 < k \leq n < P; S < P$ and P is a prime number.
Choose at random $k-1$ positive integers $a_1, ..., a_{k-1}$ with $a_i < P$, and let $a_0 = S$. Build the polynomial:

$$f(x) = a_0 + a_1 x + a_2 x^2 + a_3 x^3 + ... + a_{k-1} x^{k-1}$$

Let us construct any n points out of it, for instance set $i = 1, ..., n$ to retrieve $(i, f(i))$. Every participant is given a point (a non-zero integer to the polynomial, and the corresponding integer output) along with the prime which defines the finite field to use. Given any subset of k of these pairs, we can find the coefficients of the polynomial using interpolation. The secret piece of data is the constant term a_0.

To illustrate a simple example, suppose our secret is 1234 ($S = 1234$). (Note that this example uses an integer to demonstrate more clearly, so this is not perfectly secret). We wish to divide the secret into 6 parts ($n = 6$), where any subset of 3 parts ($k = 3$) is sufficient to reconstruct the secret. At random we obtain two $(k-1)$ numbers: 166 and 94.

$$(a_0 = 1234; a_1 = 166; a_2 = 94)$$

Our polynomial to produce secret shares is:

$$f(x) = 1234 + 166x + 94x^2$$

We construct 6 points $D_{x-1} = (x, f(x))$ from the polynomial:

$D_0 = (1, 1494); D_1 = (2, 1942); D_2 = (3, 2578); D_3 = (4, 3402); D_4 = (5, 4414); D_5 = (6, 5614)$

We give each participant a different single point (both x and $f(x)$). Because we use D_{x-1} instead of D_x the points start from $(1, f(1))$ and not $(0, f(0))$. This is necessary because $f(0)$ is the secret.

Recovery of the secret is then straightforward. In order to reconstruct the secret any 3 points will be enough.

Let us consider $(x_0, y_0) = (2, 1942); (x_1, y_1) = (4, 3402); (x_2, y_2) = (5, 4414)$.

We will compute Lagrange basis polynomials:

$$\mathcal{L}_0 = \frac{x - x_1}{x_0 - x_1} \cdot \frac{x - x_2}{x_0 - x_2} = \frac{x - 4}{2 - 4} \cdot \frac{x - 5}{2 - 5} = \frac{1}{6}x^2 - \frac{3}{2}x + \frac{10}{3}$$

$$\mathcal{L}_1 = \frac{x - x_0}{x_1 - x_0} \cdot \frac{x - x_2}{x_1 - x_2} = \frac{x - 2}{4 - 2} \cdot \frac{x - 5}{4 - 5} = -\frac{1}{2}x^2 + \frac{7}{2}x - 5$$

$$\mathcal{L}_2 = \frac{x - x_0}{x_2 - x_0} \cdot \frac{x - x_1}{x_2 - x_1} = \frac{x - 2}{5 - 2} \cdot \frac{x - 4}{5 - 4} = \frac{1}{3}x^2 - 2x + \frac{8}{3}$$

Therefore

$$f(x) = \sum_{j=0}^{2} y_j \cdot \mathcal{L}_j(x) = 1234 + 166x + 94x^2$$

and the secret is the free coefficient, which means $S = 1234$ in this case.
In order to improve the efficiency of finding $L(0)$ we can use:

$$L(0) = \sum_{j=0}^{k-1} f(x_j) \prod_{m=0}^{k-1} \frac{x_m}{x_m - x_j}$$

where $m \neq j$.

Note: The example above is using integer arithmetic, and therefore not perfectly secret. The Protex implementation of secret sharing uses finite field arithmetic to provide secrecy.

The Protex platform uses **Quantum Secret Sharing (QSS)** as an added precaution against adversaries with unlimited computing ability [15]. Based on two-step quantum secure direct communication (QSDC)[16], a proactive QSS scheme was proposed recently[17], in which a dealer Alice prepares Einstein-Podolsky-Rosen (EPR) pairs and then sends all the second particles to every agent in sequence, and the agents code their shares on these particles with four local unitary operations. The key piece of the QSS scheme is the distribution phase which works as follows:

1. Alice generates m EPR pairs $|\Psi\rangle = \bigotimes_{i=1}^{m} |\Psi\rangle_{x_i,y_i}$,
   $x_i, y_i \in \{0,1\}, i = 1,2,...,m$, each is randomly in one of the four Bell states:

$$|\Psi_{00}\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle), |\Psi_{01}\rangle = \frac{1}{\sqrt{2}}(|10\rangle - |11\rangle),$$

$$|\Psi_{10}\rangle = \frac{1}{\sqrt{2}}(|10\rangle + |01\rangle), |\Psi_{11}\rangle = \frac{1}{\sqrt{2}}(|10\rangle - |01\rangle),$$

   hereafter the first particles of all EPR pairs $|\Psi\rangle$ are called $[x]$ sequence and the second are called $[y]$ sequence. Then she prepares some decoy particles $|0\rangle, |1\rangle, |+\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle), |+\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$ (BB84 particles) and inserts them into the $[y]$ sequence. After that, she sends the $[y]$ sequence to Bob_1, and keeps a record of the insertion positions and initial states of the decoy particles.

2. After confirming that Bob_1 has received the $[y]$ sequence, Alice publicly announces the position of the decoy particles and asks Bob_1 to measure these particles with the base $Z = \{|0\rangle, |1\rangle\} or X = \{|+\rangle, |-\rangle\}$ according to their bases and publish his measurement results. Then Alice computes the error rate through comparing the measurement results to the initial states. If the error rate exceeds the preset threshold, shes asks Bob_1 to abort the process and start a new one. Otherwise, they continue to perform the protocol.

3. Bob_1 randomly chooses a binary number $K^1 = (u_1^1, v_1^1, ..., u_m^1, v_m^1)$ as his private key and then performs the unitary operation $U_{u_i^1, v_i^1}$ on the ith particle in the $[y]$ sequence, $i = 1, 2, ..., m$, where $U_{u_i^1, v_i^1}$ is one of the Pauli operators:

$$U_{00} = I = |0\rangle\langle 0| + |1\rangle\langle 1|, U_{01} = \sigma_z = |0\rangle\langle 0| - |1\rangle\langle 1|,$$

$$U_{10} = \sigma_x = |0\rangle\langle 1| + |1\rangle\langle 0|, U_{11} = i\sigma_y = |0\rangle\langle 1| - |1\rangle\langle 0|.$$

Note that the $[y]$ sequence is denoted as $[y_1]$ sequence after Bob_1's operation hereafter. Then he prepares some BB84 particles and inserts them into the $[y_1]$ sequence. After that, he sends the $[y_1]$ sequence to Bob_2.

4. Bob_2 does the similar actions as Bob_1. This process is continued until Bob_n sends $[y_n]$ sequence to Alice.

5. After confirming the security of the $[y_n]$ sequence, Alice performs a Bell measurement on each EPR pair of the sequence $|\Psi'\rangle = \bigotimes_{i=1}^{m} |\Psi\rangle_{x_i', y_i'}$, where $|\Psi'\rangle$ is the evolution of $|\Psi\rangle$ after all the agents' operations. According to the measurement outcome, she gets the secret S by computing

$$S = (x_1, y_1, ..., x_m, y_m) \bigoplus (x_1', y_1', ..., x_m', y_m'),$$

where $\bigoplus$ denotes the bitwise exclusive OR (XOR).

The use of the QSS algorithm and distribution method above provides secrecy even in the presence of malicious users with unlimited computing power.

Protex uses SHA3-256 hashing in all other cases for security throughout its entire data pipeline. Protex is able to communicate the demographics of each individual data contributor to purchasers, though, by encrypting and sending this information to them through a secure communications channel using the secret-sharing methods described above.

The Protex blockchain maintains a different hashmap for each of the supported data fields. This hashmap is used so that Protex only ever needs

to store references to data on the blockchain, drastically improving storage efficiency and gas costs. All of the references to data are stored in structs to optimize storage costs as well.

4.4 Plasma and Scalability

In August 2017, Vitalik Buterin and Joseph Poon proposed a method for drastically scaling a smart contract blockchain to potentially billions of state-changes per second [19]. Protex is being built to scale perfectly as a private, Plasma child chain on Ethereum. The scalability of the Plasma proposal will enable Protex to robustly support large streams of data and even allow for the exchange of real-time data. Plasma will also assist in the trustlessness of the protocol as the private chain will be built on top of the Ethereum platform as the basis and reinforcement of truth.

4.5 Data Science Functionality

One major advantage of the Protex blockchain is the uniformity with which it stores usage data. Regardless of the data field Protex stores, the formatting follows a simple-to-use API. The Protex API makes it extremely easy for data analysts to get exactly what they need from the data they purchase. All data maintained by the Protex platform is managed with an eye for data science.

5 Protex Chrome Extension

Protex contributors are able to share their web browsing data to the platform via the Google Chrome extension. Rather than forcing users to switch web browsers to collect usage data, Protex collects, cleans and stores user data via a Google Chrome web browser extension. By using an extension to obtain this data, it encourages users to adopt the platform without needing to change anything about their web browsing experience.

The extension provides access to a Google Chrome toolbar button with a drop-down panel. In the panel, users are given options to open settings, change their PTX/ETH address, view their PTX earnings in PTX, ETH and USD, or turn contributing for different data fields on/off.

- Settings: Users can update or uninstall the Protex extension, open log files and set a schedule for turning data field volunteering on/off.

- Contributing: Rows of the four data fields that Protex currently provides to purchasers are displayed with a simple on/off button for users to select each day. These rows also provide users the ability to set a recurring or one-time schedule for turning a field on/off.

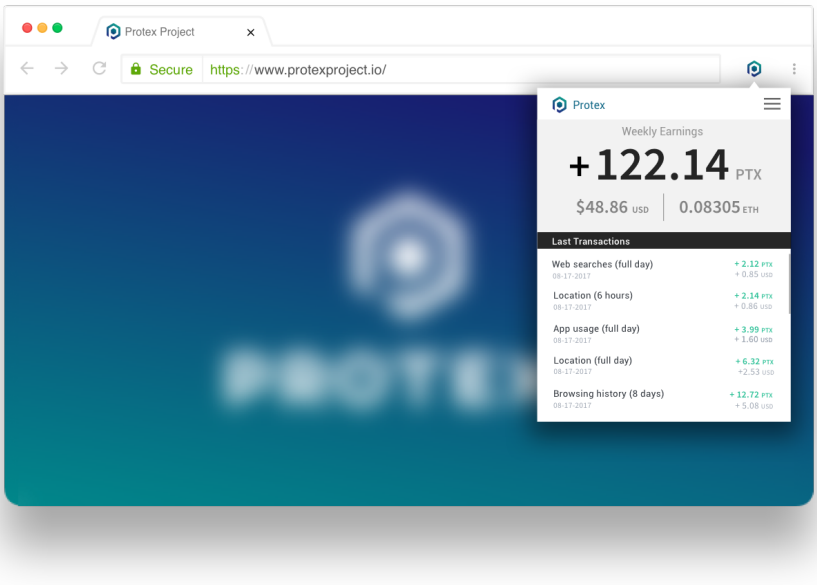


Figure 2: Google Chrome Extension

Protex completely separates any personal information from the data a user contributes before adding it to the blockchain. Because of this, users have no risk of compromising their anonymity. The data they provide is never associated with any public record throughout the entire data pipeline.

After installation, the Protex Chrome extension runs completely in the background and does not alter the functionality of Google Chrome. There is a very small barrier to entry, and thus promotes adoption and makes using the platform as easy as possible. The goal of this extension is to make users do as little work as possible to capitalize on their data.

6 Protex Mobile App

Similar to the Google Chrome extension, Protex also supports a mobile app for Android and iOS devices. This app serves as the source for Protex

contributors to volunteer data to the blockchain. The app dissociates any personal information from data just like the Google Chrome extension. The Protex app provides a settings page for users to set or change their Ethereum address for payments, as well as select the data fields they wish to contribute to the blockchain.

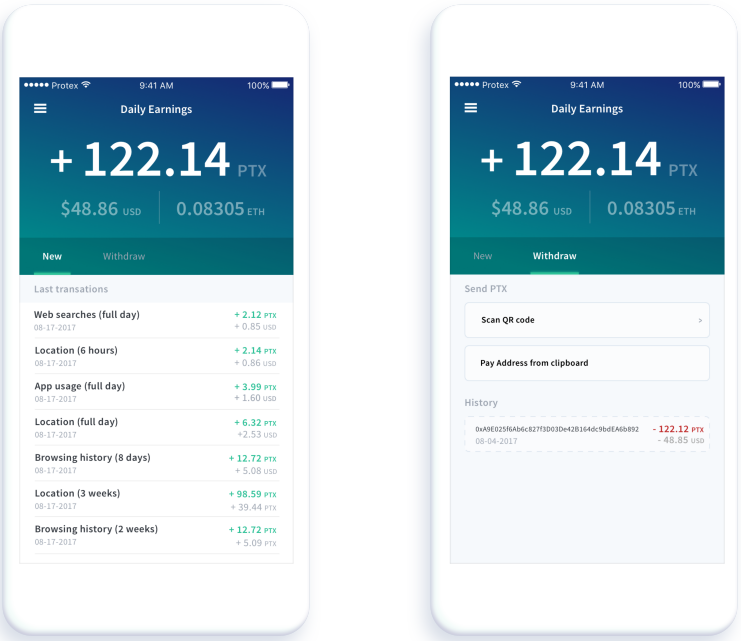


Figure 3: Mobile Application Home page

Mobile app users are able to set a schedule for sharing as well, offering the capability to only contribute data some days of the week or some hours of the day.

The Protex app standardizes all data it stores on the blockchain in an effort to maximize the ease of data analysis by companies who wish to purchase it.

7 Protex Exchange Portal

Protex provides a mechanism for purchasing data through its Exchange Portal. This portal runs as a web application that behaves similarly to a cryptocurrency exchange. The one major difference, obviously, is that instead of crypto-for-crypto, users are exchanging crypto-for-data.

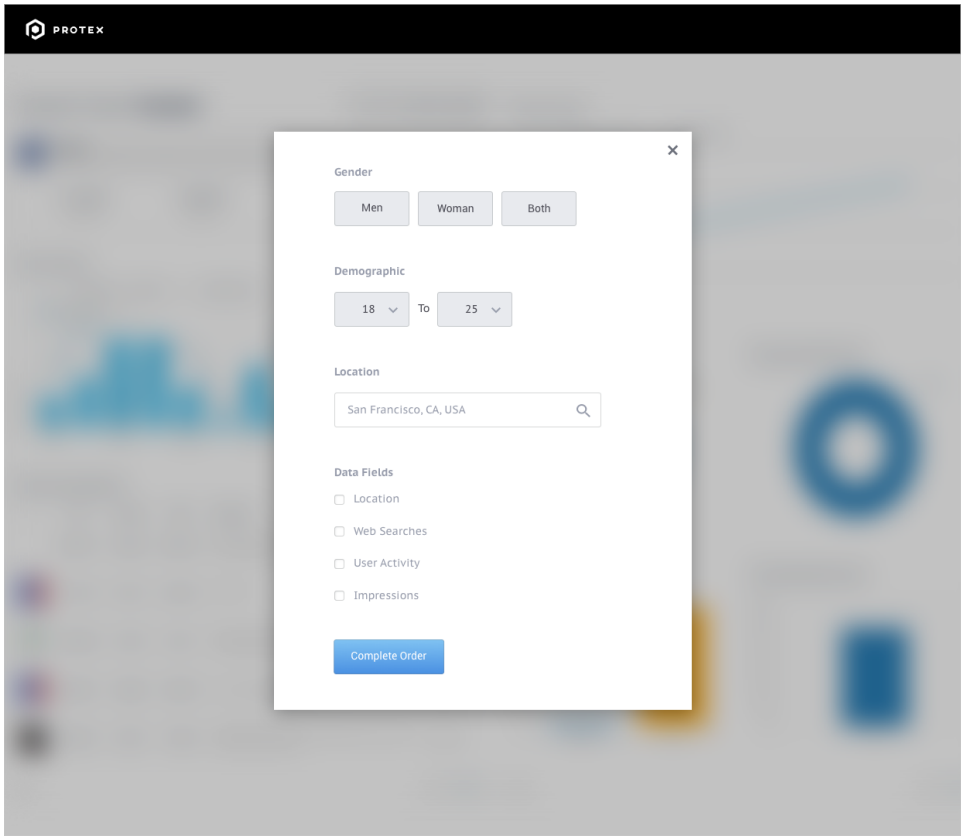


Figure 4: The ordering form for data purchasing. After selecting a demographic, purchasers select which data fields they want.

When ready to pay for their data order, purchasers are provided with a PTX address that is specifically mapped to their order. This way purchasers can receive their order via instant download once that smart contract triggers a fulfilled payment.

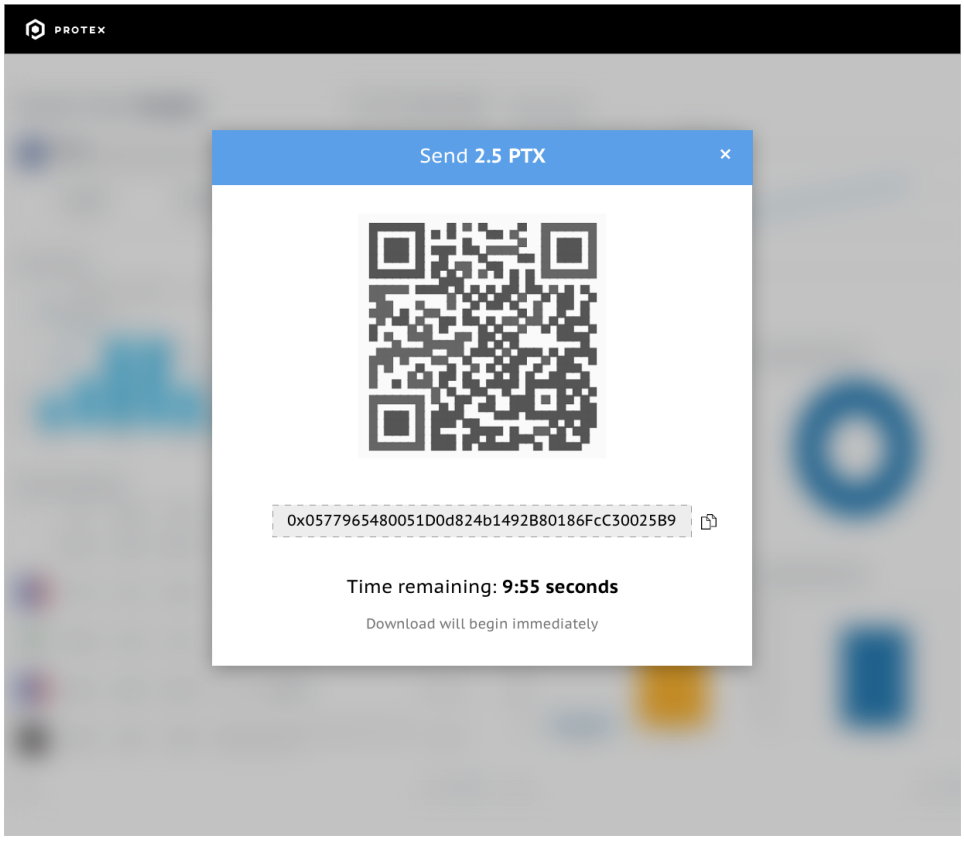


Figure 5: The payment page for data purchasers.

Because the Protex platform standardizes all data inputs from contributors, it lends itself perfectly to data analysis and machine learning. The formatting of Protex data is all done with data science in mind, to make it as easy as possible once purchased.

8 Token Sale

All the ideas above will take money to execute. While the Protex team has put extensive time into developing the project and building as much as possible, growing the Protex platform will require extra funding. As opposed to alternative crowdfunding mechanisms like Kickstarter, Protex will be hosting a sale of the PTX tokens to the public [20]. The nature of our platform lends itself perfectly to a public token sale. By using an Ethereum smart contract to issue tokens in the Pre-Sale and Token Sale Protex gives early investors an opportunity to invest in and capitalize on the bright future of the Protex platform. Below are the details for the issuance of the tokens in the Pre-Sale & Token Sale:

- **Circulating supply:** There will only ever be 1,000,000,000 PTX tokens in circulation. 900,000,000 PTX tokens are available for purchase in the Token Sales, while 100,000,000 PTX will be withheld by Protex, LLC to encourage and incentivize long-term contributions to the project. The breakdown of tokens will be as follows:

Note: All dates provided below are rough estimates of the Ethereum block number listed, and subject to change.

8.1 Pre-Sale

- Pre-Sale Launch Date: **active now**
- Pre-Sale Ends: Ethereum block # 4,520,000
- PTX available for Pre-Sale: 200,000,000
- PTX Exchange Rate: 1 ETH = 20,000 PTX
- ETH Address: 0xed14DA241e034d94d090A4842356628DAE40047B

8.2 Token Sale

The primary token sale will offer 700,000,000 tokens to the public. Tokens purchased during week 1 of the Token Sale will receive a 10% bonus on all tokens purchased, and tokens purchased during week 2 of the Token Sale will receive a 5% bonus.

- Token Sale Launches: Ethereum block # 4,570,000

- Token Sale Ends: Ethereum block # 4,720,000
- Token Sale Exchange Rate: 1 ETH = 12,000 PTX
- ETH Address: 0xed14DA241e034d94d090A4842356628DAE40047B
- PTX available for Token Sale: There will only be 700,000,000 PTX for sale in the Token Sale, regardless of if the Pre-Sale sells out.

Restrictions: Please refer to the Terms & Conditions to see restrictions on the Pre-Sale and Token Sale.

9 Future Plans

9.1 Roadmap

The Protex team has outlined a detailed plan for the engineering sub-teams and adoption strategy team to grow the platform at scale. Although the project will be constantly evolving and all items are subject to change, below is a projected roadmap:

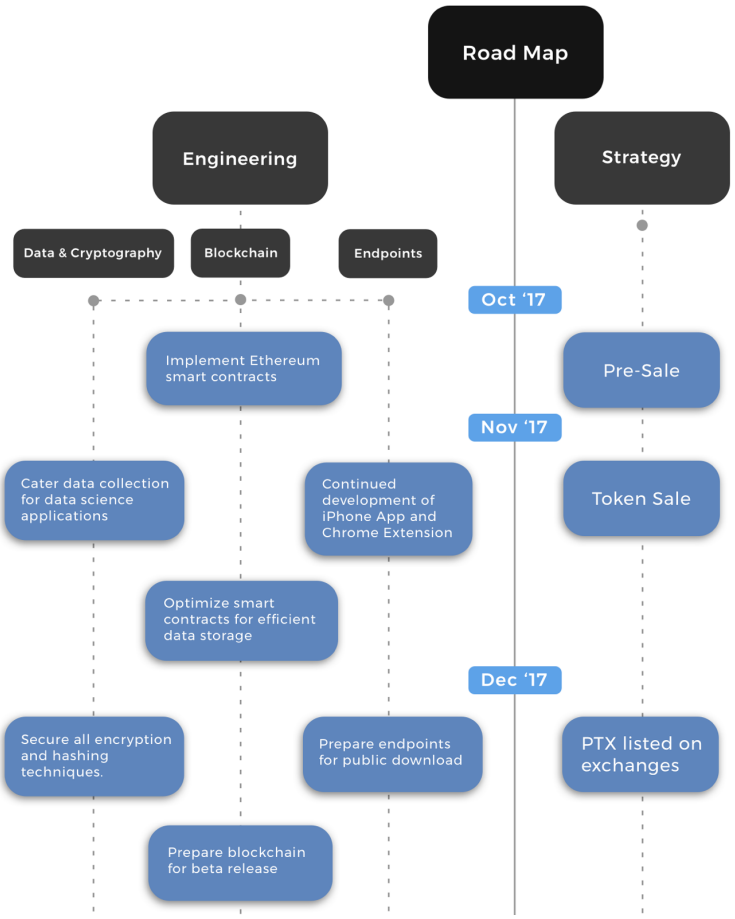


Figure 6: Roadmap Part 1

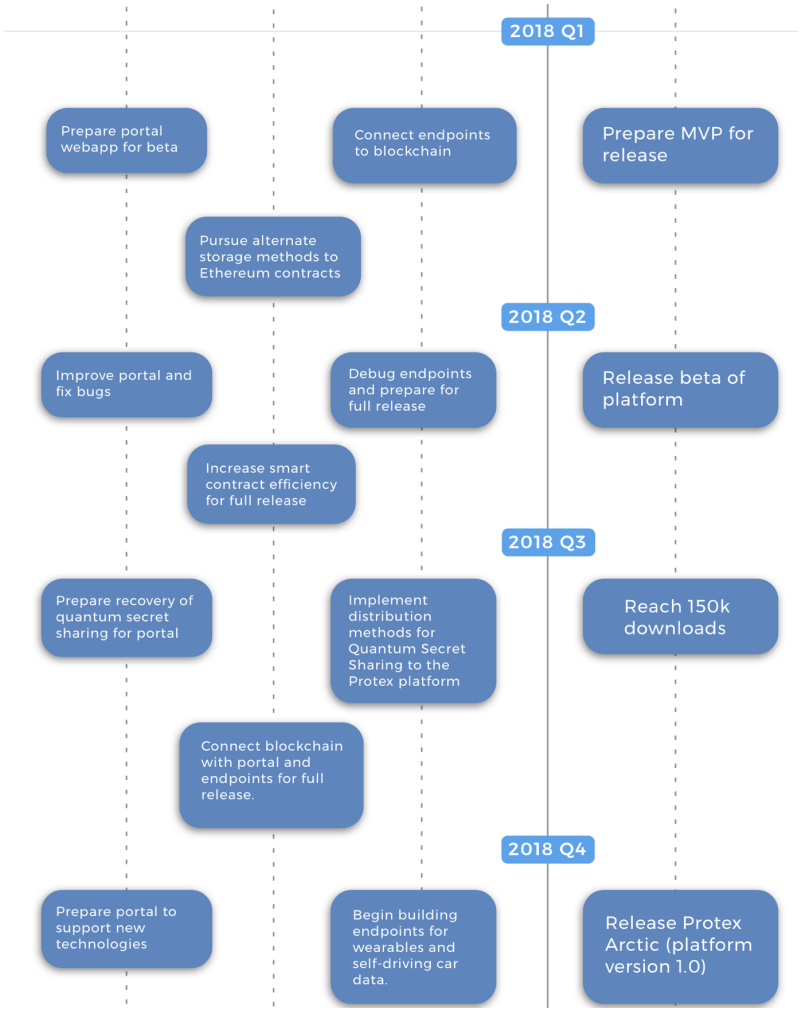
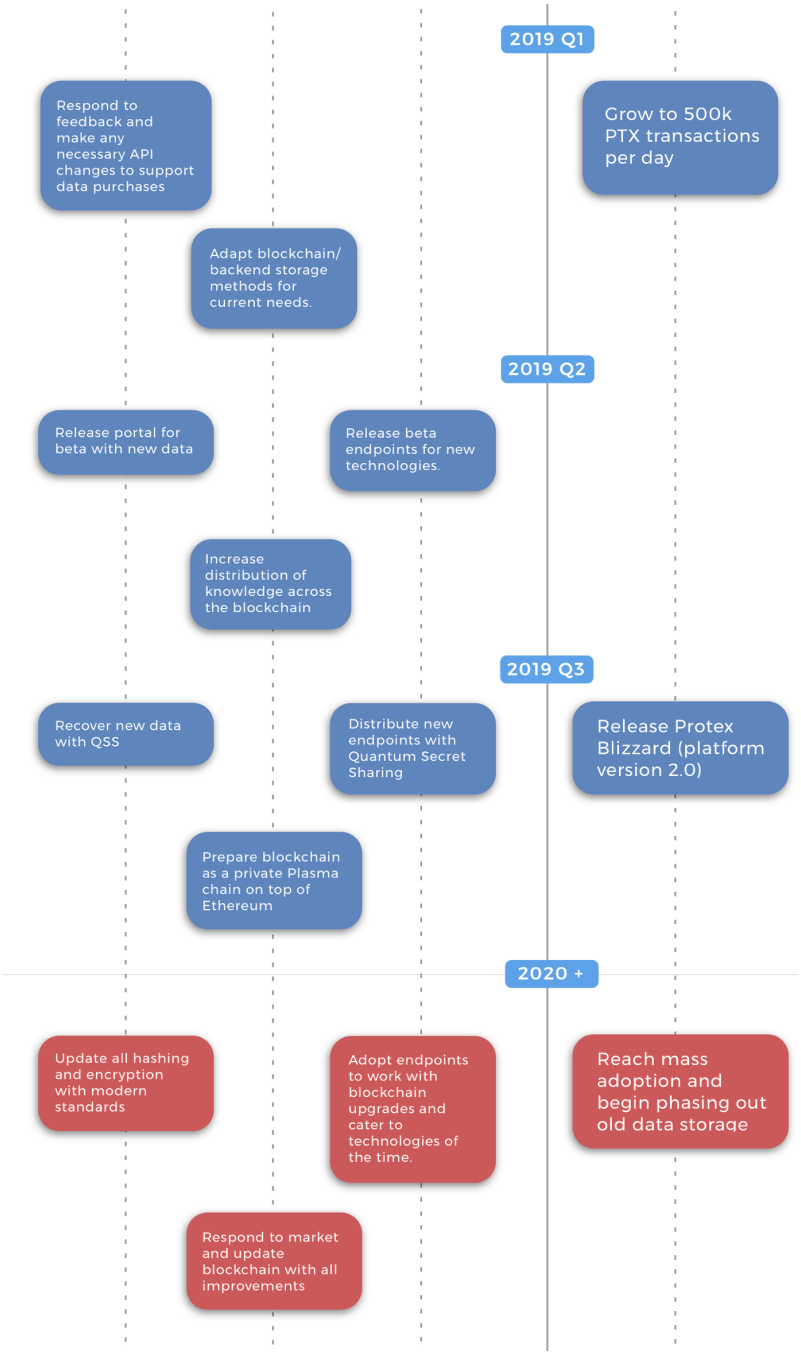


Figure 7: Roadmap Part 2


2019 Q1
Respond to feedback and make any necessary API changes to support data purchases
Grow to 500k PTX transactions per day
Adapt blockchain/ backend storage methods for current needs.
2019 Q2
Release portal for beta with new data
Release beta endpoints for new technologies.
Increase distribution of knowledge across the blockchain
2019 Q3
Recover new data with QSS
Distribute new endpoints with Quantum Secret Sharing
Release Protex Blizzard (platform version 2.0)
Prepare blockchain as a private Plasma chain on top of Ethereum
2020 +
Update all hashing and encryption with modern standards
Adopt endpoints to work with blockchain upgrades and cater to technologies of the time.
Reach mass adoption and begin phasing out old data storage
Respond to market and update blockchain with all improvements

9.2 Budget Plan

After careful deliberation, the Protex team concluded the circulating supply and price figures above based on the wide scope of the project. The pricing provides the highest value to data contributors comparative to the current price of raw market data as well as an opportunity for favorable returns to investors. The Protex team has spent considerable time strategizing executable plans once funds are raised. The team plans to spend the funds raised from the Token sales in the following manner, though the budget remains flexible as the amount of available funds is currently unknown.

- **Product Development and Staffing: 61%**
  This portion of the budget plan consists of hiring top tier talent within the highly competitive Silicon Valley area. With our current team and the addition of talented members including software developers, brand strategists, administrative assistants, HR specialists and a head of security, the development of our platform will be expedited.

- **Marketing: 23%**
  A primary goal of Protex is to reach critical mass and grow adoption to compete with existing institutions.

- **Security: 9%**
  The security portion of the funds will go towards ensuring our head of security has all necessary components for Protex to be held to the standards of SaaS companies around the world. Considering the premise of the project, this is not something our team takes lightly. One of the goals with our security sector is to become SOC2 compliant, a high level security requirement [21].

- **Legal: 7%**
  It is necessary for Protex to be comprehensive with its legal department and assure all legalities are covered. This means hiring outside legal counsel to reinforce all legal measures.

Budget Plan Summary	
61%	Product Development and Staffing
23%	Marketing
9%	Security
7%	Legal

10 Team

The Protex project is led by a Silicon Valley based team with extensive knowledge and experience in software development, blockchain architecture, design and entrepreneurship. Surrounded by the constantly adapting and competitive environment of the Silicon Valley, the passion of our team lies within the opportunity to change the world with cutting-edge technology like blockchain. Our upbringing in the technology epicenter has provided us unique opportunities to work for tech giants, connect with industry experts and also develop our own successful businesses. Our team has an abundance of resources and skill-sets that are supported by drive and hyper-vision. With a combined background of 20+ years in the blockchain space, we have directed our mission towards the creation of a decentralized exchange of data.

Kieran Stolorz - Chief Architect & Lead Developer

A passionate member of the blockchain community, Kieran joins Protex with over a decade of software development experience. Kieran graduated *cum laude* from the University of Southern California with a B.S. in Computer Engineering and Computer Science where he was a key leader for several on-campus teams. As the Computer Vision lead for the USC Aerial Robotics team he developed a strong background in neural networks and machine learning models. Serving as the Software Team Lead for the award-winning USC Hyperloop team Kieran has experience overseeing the development of breakthrough technology and coordinating large groups of people. Kieran brings with him software engineering experience from companies like Google and Cisco where he was responsible for leading the development of large, scalable data science projects. He was also one of the first employees of Second Spectrum, where he learned key lessons about velocity and growth of tech start-ups. Kieran has been an involved cryptocurrency investor and community member since 2013. With an extensive data science skill-set, and a deep familiarity with blockchain protocol he is uniquely prepared to spearhead the development of the Protex project.

Jason Spielman - Chief Creative Officer

Jason is a multidisciplinary designer specializing in user interface design, user experience and impactful video production. With experience as a UX Designer at Google, he is constantly striving to create inspiring and engag-

ing content. Jason holds a B.A. in Design Media Arts from UCLA, where he co-founded College Weekly and was the Creative and Marketing Strategist at Pingtank. He was also the Chief of Design at LA Hacks, the biggest hackathon in the nation. Combining his love for blockchain tech and design, Jason handles all creative responsibilities with the Protex project.

Steve McLean - Chief Operating Officer

Steve has directed his business-oriented mind and fanaticism with technology towards the creation of the Protex platform. Steve graduated from Baylor University with a B.B.A. in Management Information Systems where he served as the captain of the baseball team. Steve's experience leading a team ranges from the classroom with software development projects to the baseball diamond in a highly competitive Division I atmosphere. Following university studies, Steve began his career in Business Development at Jobvite, a SaaS company located in the Silicon Valley, but has since ventured away to pursue the success of Protex and his passion for blockchain technology.

Eric Heintzen - Administrative Director

Eric is a creative and driven individual with experience in numerous facets of the tech, marketing and educational industries. Eric has experience working on hardware and software engineering teams at prominent companies including GoPro. He also has worked at companies like Bodin & Associates and MSA Systems as a marketing team lead. Eric brings over 4 years of experience in the blockchain space and a unique array of skills to take advantage of. He leverages his creative and technical skills to think outside the box and push the innovation of Protex forward.

11 FAQs

What are PTX?

The Protex Token, or PTX, is an ERC-20 compliant token used to perform transactions on the Protex platform. It is the way data contributors are paid, and the way data purchasers buy data.

Why should I use Protex?

Users: Protex gives users the right to finally control their own data.

Users are able to profit by sharing data, all with the comfort of knowing it is protected by cryptography on a secure blockchain.

Purchasers: Protex saves purchasers the liability of potential data breaches (significant legal and economic costs) and also provides data analytics companies and divisions with easy-to-use tools to analyze the data they purchase.

How does Protex keep the data safe?

Protex removes all personal information from your data before hashing and adding it to any blockchain. Protex uses the SHA3-256 hashing standard to secure all data and prevent any attacks [22]. Nothing is ever stored in plain-text and Protex implements a Quantum Secret-Sharing algorithm for all data contributions. This algorithm makes it impossible to compute any of the data without all (or some threshold number of) shards of it. Similarly, this algorithm is used on the data-purchasing end of the platform to obfuscate who any potential purchaser is.

How do I get paid for my data?

Protex data contributors are paid via PTX tokens when their data is purchased. 100% of the money spent on the data is shared among all individuals who contributed to the data cluster with profit sharing. The only fee associated with a Protex transaction is the gas to use the Ethereum platform.

Do I need to give Protex all my information?

NO! This is one of the advantages of Protex - you only share what you want to. Protex even enables users to share nothing if they wish.

Do I need Ethereum to buy PTX?

Yes and no. For our pre-sale and Token sale we are only accepting Ethereum directly, however, we provide a tutorial here (hyperlink) on how to exchange most other cryptocurrencies to Ethereum. If this is your first time using Ethereum we also have a guide here (hyperlink) on how to set-up a wallet and receive ERC-20 tokens.

Where will my money go?

Protex has developed a road map (Section 9.1) and intended budgeting plan (Section 9.2). In summary, the funds raised via our token sale will be used to advance the Protex platform and grow its user base. This

includes further development of the products and technology discussed in this whitepaper, as well as staffing, marketing and legal objectives for the team.

Why is this valuable?

Each year, companies lose billions of dollars suffering through the headache of costly data breaches. Protex wont just eliminate attacks on data, it offers individuals who browse the web and use mobile devices the right to decline to share data, as well as compensation for the data they do share. Protex is a major disruptor in one of the biggest sectors in the world.

References

[1] Ethereum Foundation: *Ethereum Project*
https://www.ethereum.org/

[2] Breach Level Index: *Data Breach Statistics by Year*
http://breachlevelindex.com/

[3] The Deal Room: *The 10 most expensive data breaches in Corporate history*
https://www.firmex.com/thedealroom/the-10-most-expensive-data-breaches-in-corporate-history/

[4] Patrick McFadin: *Internet of Things: Where Does the Data Go?*
https://www.wired.com/insights/2015/03/internet-things-data-go/

[5] Wikipedia contributors: "HTTP cookie." *Wikipedia, The Free Encyclopedia.*
https://en.wikipedia.org/wiki/HTTP_cookie

[6] Mazerick, Ryan: *Risk Associated with Cookies*
http://resources.infosecinstitute.com/risk-associated-cookies/#gref

[7] Bradley, Tony: *Location Tracking in Mobile Apps Is Putting Users at Risk*
https://www.csoonline.com/article/2871933/mobile-security/location-tracking-in-mob

[8] Adler, Laura: *Learning from Location*
http://datasmart.ash.harvard.edu/news/article/learning-from-location-806

[9] Cameron, Darla: *How targeted advertising works*
https://www.washingtonpost.com/apps/g/page/business/how-targeted-advertising-works

[10] Wikipedia contributors: "Netflix Prize." *Wikipedia, The Free Encyclopedia.*
https://en.wikipedia.org/wiki/Netflix_Prize

[11] Lemos, Robert: *Researchers reverse Netflix anonymization*
http://www.securityfocus.com/news/11497

[12] Reiff, Nathan: *What is ERC-20 and What Does it Mean for Ethereum?*
http://www.investopedia.com/news/what-erc20-and-what-does-it-mean-ethereum/

[13] Wikipedia contributors: "Shamir's Secret Sharing." *Wikipedia, The Free Encyclopedia.*
https://en.wikipedia.org/wiki/Shamir%27s_Secret_Sharing

[14] Shamir, Adi: *How to share a secret*
https://dl.acm.org/citation.cfm?doid=359168.359176

[15] Wang et al. : *Security of a kind of quantum secret sharing with entangled states*
https://www.nature.com/articles/s41598-017-02543-0

[16] Deng, F. G., Long, G. L. & Liu, X. S. : *Two-step quantum direct communication protocol using the Einstein-Podolsky-Rosen pair block.*
https://journals.aps.org/pra/abstract/10.1103/PhysRevA.68.042317

[17] Qin, H. W. & Dai, Y. W. : *Proactive quantum secret sharing.*
https://link.springer.com/article/10.1007%2Fs11128-015-1106-x

[18] Wikipedia contributors: "Shamir's Onion routing." *Wikipedia, The Free Encyclopedia.*
https://en.wikipedia.org/wiki/Onion_routing

[19] Vitalik Buterin and Joseph Poon: *Plasma: Scalable Autonomous Smart Contracts* http://plasma.io/plasma.pdf

[20] Kickstarter: *About - Kickstarter*
https://www.kickstarter.com/about?ref=nav

[21] Imperva, Inc: *What is SOC 2*
https://www.incapsula.com/web-application-security/soc-2-compliance.html

[22] Wikipedia contributors: "SHA-3." *Wikipedia, The Free Encyclopedia.* `https://en.wikipedia.org/wiki/SHA-3`