Insights Network

A Blockchain Data Exchange

Brian Gallagher and Darwin Lo

19 October 2017 (v0.4)

Abstract

In the present day, data brokers collect data on individuals around the world from a wide array of sources, both online and offline. The data is packaged into profiles, which they sell to organizations who can use them to make decisions that impact the lives of ordinary people without them ever being aware of it. Recent technological advances, such as the blockchain, are making it possible to build a superior platform for conducting market research while putting control, as well as monetization, of the data into the hands of the people who generate them.

info@insights.network

Contents

Disclosure

Nothing herein constitutes an offer to sell, or the solicitation of an offer to buy, any tokens, nor shall there be any offer, solicitation or sale of Insights tokens in any jurisdiction in which such offer, solicitation or sale would be unlawful. You should carefully read and fully understand this whitepaper and any updates. Every potential token purchaser will be required to undergo an on-boarding process that includes identity verification and certain other documentation, which you should read carefully and understand fully because you will be legally bound. Please make sure to consult with appropriate advisors and others.

This white paper describes our current vision for the Insights platform. While we intend to attempt to realize this vision, please recognize that it is dependent on quite a number of factors and subject to quite a number of risks. It is entirely possible that the Insights platform will never be implemented or adopted, or that only a portion of our vision will be realized. We do not guarantee, represent or warrant any of the statements in this white paper, because they are based on our current beliefs, expectations and assumptions, about which there can be no assurance due to various anticipated and unanticipated events that may occur.

Please know that we plan to work hard in seeking to achieve the vision laid out in this white paper, but that you cannot rely on any of it coming true. Blockchain, cryptocurrencies and other aspects of our technology and these markets are in their infancy and will be subject to many challenges, competition and a changing environment. We will try to update our community as things grow and change, but undertake no obligation to do so.

Problem

There are organizations, called data brokers, that collect data on people from various sources, both online and offline. Most notably, they purchase data from Internet services and mobile applications that collect information on their users and track their in-app behavior.

The data is used to create profiles for individual consumers. Acxiom, a top data broker, has on average 1,500 pieces of information on more than 200 million Americans. Acxiom and other data brokers are able to combine all the information it has on each individual to generate in-depth consumer behavior reports across a wide range of industries, which they sell.

Data brokers make a lot of money. In 2012, Acxiom was reported to have made $1.13 billion in sales, earning a profit of $77.26 million. Forbes reports that Big Data Analytics is a $200 billion per year industry and that by 2019 nearly all businesses will be customers of a data broker such as Acxiom.

But consumers, who are actually driving the industry, do not share in the profit. At the same time, they actually experience many negative consequences. Centrally managed databases allow hackers to steal large amounts of personally identifying information in just one attack, which allows for large-scale identity theft and fraud. Recently, hackers breached Equifax's systems and stole personally identifiable data on more than 140 million Americans. This is not an isolated incident. There have been several attacks in the past, including on Acxiom, and if unchecked there will be more in the future. Consumers must demand a new standard for the storage of personally identifiable and sensitive information that is being used in market research.

Solution

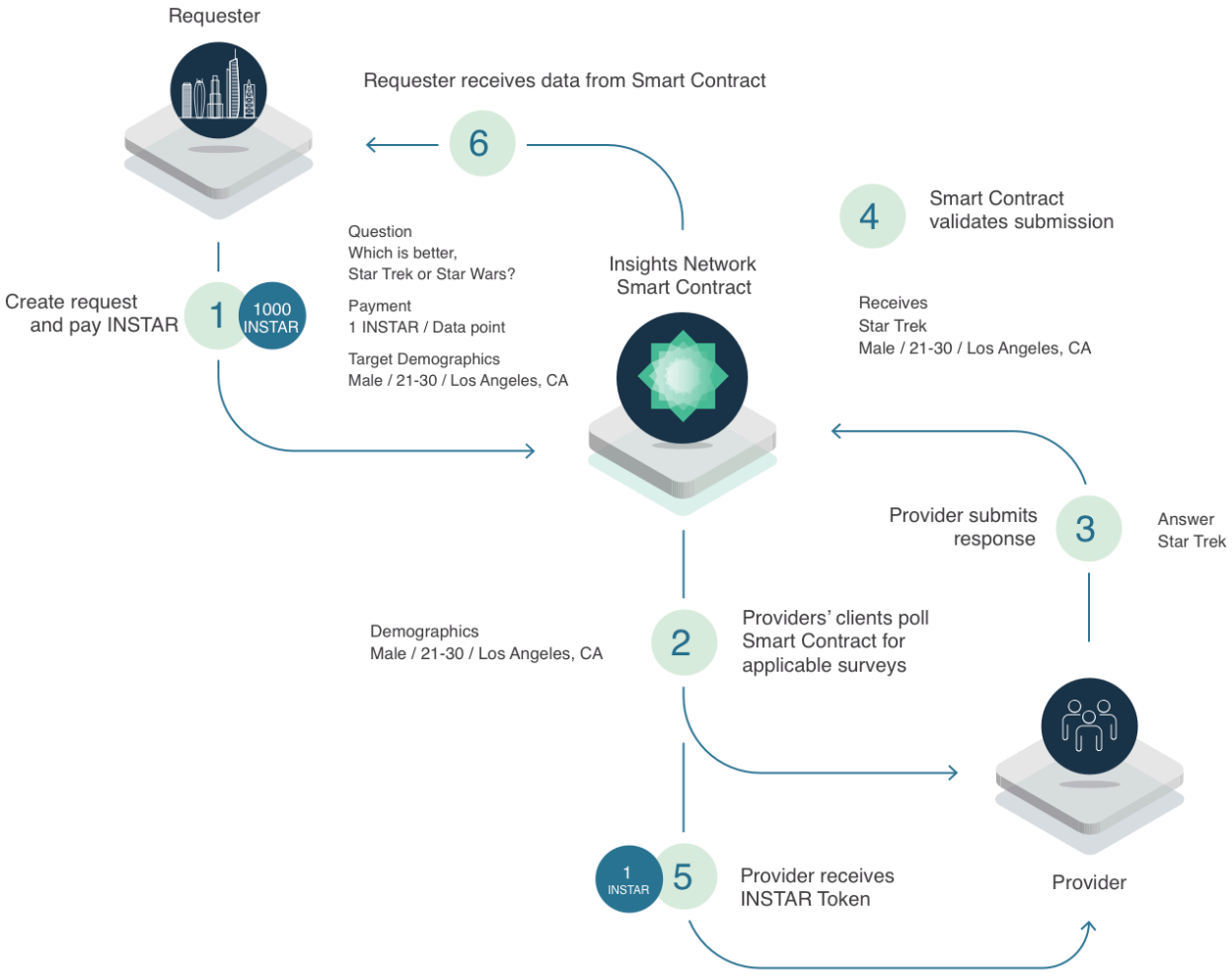
Recent advances in decentralized storage, digital currencies, and smart contracts enable us to create a decentralized, incentivized platform for conducting marketing research and securely storing consumer data. Organizations will be able to use our platform to make requests for data from precisely defined populations amongst members of the Insights Network.

Insights Network users, not data brokers, would sell their data. By using smart contracts, which execute transactions between anonymous parties, users would be able to sell their data without disclosing their identity, only broad demographic information.

We believe that by allowing participants to profit from their participation organizations will acquire data that is both more relevant and more actionable. At the same time, profits currently going to data brokers will instead go to the rightful owners of the data, the consumers.

Overview

Primarily, we are serving two types of users: those who request data, which we call requesters, and those who provide it, which we call providers. Requesters are typically organizations, but anyone can buy Insights tokens and use them to submit a request for data to the Insights Network. Providers are users who comply with a data request by providing data; the ones who fit a data requests' target demographic are compensated for their data in Insights (INSTAR) tokens.



Requesters want to be able to collect data that is:

1. Relevant. They want to be able to gather data from specific populations, for example, only those between the ages of 20 to 35.
2. Trustworthy. The data that is collected is free from fraud. That is, the data is collected from targeted providers who have provided their data honestly. For example, requesters expect their surveys to be answered truthfully by their target demographic, and not say, a bot.
3. Timely and convenient. Requesters should be able to get answers to their questions quickly without worrying about the details of how to reach their target demographic.

And providers want assurance of the following.

1. Their data is not collected without their explicit permission.
2. Sensitive information, such as who they are, is not provided, only broad demographic details.
3. They are paid for the data they provide.
4. Their data is handled securely.

Traditional marketing research firms collect data over a fixed period of time and provide a single report to their clients. On our platform, requesters would never have to close their request for data. Their reports, which they would be able to view at any point during data collection, are updated as data from providers is received and forwarded by the smart contract.

As more data is submitted to our network, the data that the platform makes available to requesters becomes more comprehensive, which in turn gives the ability to design reports that are more comprehensive, including ones that combine data from more than one data request.

Here are several examples on how the Insights Network could be used.

- A polling firm may want to run a poll to see who would win if the presidential election were re-run at this moment in time.
- McDonald's may want to run a survey to solicit feedback on a new menu item.
- University classes can administer surveys throughout the quarter or semester to get feedback on the quality of instruction on an ongoing basis.
- Political polling firms can use the Insights Network to get anonymous, unbiased data on specific political beliefs.

User profiles

Users maintain an Insights Network profile. They can view their profile, which contains demographic information and other general, non-identifying information. They can make corrections, fill in missing details, and delete information. Furthermore, other than deleting information, they are paid in Insights tokens to perform these actions.

For example, a 25-year-old woman living in Los Angeles may want to receive ads related to her political interests, so she may choose to keep the line that indicates she is a Republican. But she may not wish to receive surveys in relation to being a single mom, so she would delete that line. She can also see that her profession is unknown, and she may choose to fill it out in exchange for Insights tokens.

Surveys

Anyone on the Insights Network, whether they are an individual or an organization, can publish a survey to the platform. The platform gives them the ability to specify a target demographic, as well as how many tokens users in the target demographic will receive when they submit a valid response. The process is as follows:

1) A requester publishes a survey, specifying a target demographic.

2) Users of our app who fit the target demographic get notified.

3) Users fill out the survey, submit it to the Insights Network, and funds are transferred to their account.

Third-party apps: Secure login and rewards

A common practice among apps today is to allow their users to log in using their Facebook account. We are building a similar service for apps to allow their users to log in using their Insights Network account. This would appeal to users who do not want to disclose their identity to their apps. As an added benefit, apps can use the Insights Network to give tokens to their users as part of a reward program and allow them to cash them in for rewards, such as airline miles.

Example: Gambeal

Gambeal, an iOS application, is an Insights Network partner application that will be the first to integrate with Insights to begin conducting their existing market research targeted at quick serve

restaurant dining experiences. We are using the Mobius Universal Protocol API to integrate our Insights token into the Gambeal application in order to facilitate thousands of fast, low cost reward payments to Gambeal's existing user base every week in exchange for data. This ensures our reward token begins circulating into the open market as soon as we make the token issuance to the public. The Insights Network login API broadcasts only the users' demographic data into Gambeal's analytics systems. This ensures a user's privacy protections and ensures that the user's data will end up in their Insights profile under their ownership, where it is monetizable -- rather than in a company like Acxiom's database -- where it is sold without their knowledge or approval.

In addition to our technology providing better privacy protections for our users, it currently takes several days and costs a user fees of up to 3% to redeem their cash rewards into their PayPal account inside the Gambeal App. Instead, smart contracts release tokens directly into a user's wallet address, saving time and costing a fraction of the fees. This represents a clear improvement for a user's experience.

Technology Overview

A requester is a user who places a request on the Insights Network to get information from a specific population of users. Anyone can place a request on the Insights Network, but the typical requester will be an organization that wishes to conduct a survey for market research. Providers are users who fulfill such a request. The following features of the Insights Network serve to enable requests, which we call data requests, as well as the fulfillment of those requests.

Identity verification. Providers prove they are real people by submitting their identity documentation and getting a digital proof of authenticity from the Insights Network, which they can use to prove their authenticity. They are compensated in tokens for doing this.

Incentivized market research. Requesters can publish a survey and receive survey responses using the Insights Network smart contract. The smart contract sends tokens to providers in the target population who have submitted a valid data point.

Blockchain-verifiable results. At requesters' discretion, the data points of a data request could be recorded in the ledger for anyone to look at. Since the ledger is implemented using a blockchain, anyone looking at these records would have reasonable assurance that the data points have not been tampered. This feature is important for certain kinds of surveys, such as polls and votes.

Private semantic validation of privileged data. Using Secure Multiparty Computation (SMC) in conjunction with a blockchain-based smart contract, a provider is able to withhold data until she receives payment and a requester is able to withhold payment until the data is proven to be valid -- without requiring the provider to entrust her data in a third party.

Secure Multiparty Computation

Various features of our system make use of Secure Multiparty Computation, which is a scheme for several independent parties to jointly carry out a computation without learning what the inputs of the computation are. This is done by breaking up the computation into sub-computations for the independent parties to perform and using a technique called secret-sharing to derive inputs for the sub-computations from the original inputs that cannot be used to figure out the original inputs.

In our system, the independent parties who perform the sub-computations are a class of token holders we call SMC parties. They are paid using INSTAR tokens and are randomly selected on a daily basis, a scheme known as proof-of-stake.

In classical SMC, each party broadcasts the result of their sub-computation to the other parties, and each party assembles the intermediate results into their own copy of the overall result. In contrast, SMC parties in our system send their intermediate results either to the Insights Network smart contract or to the intended recipient of the output directly. This modification has the following benefits.

- There is no intermediary between the assembly of the overall result of the SMC and the execution of a transaction, such as sending tokens to an account.

- An SMC party is unable to assemble the overall result without sending their own intermediate results to the other parties, which fixes a fundamental flaw with classical SMC.

As it turns out, SMC and blockchain-based smart contracts are a natural fit. Secure Multiparty Computation has long been a mere theoretical curiosity in academia, but it is beginning to see use in the industry. Frameworks like FRESCO are making it possible to use it in production. We are partnering with Partisia, a company that provides commercial support for FRESCO, to help with our implementation.

Proof of authenticity

Providers preserve their anonymity while participating in the Insights Network. But requesters need to know that, even though they are anonymous, the providers who are fulfilling their data requests are real people. This is the process by which a provider confirms they are a real person.

Our system uses information from multiple parties in order to verify a provider's identity. For example, one party might be the provider's employer. Another party might take the provider's state-issued identity document and validate it.

We call these parties verification partners. If the provider passes verification, the system issues a digital proof of authenticity signed by the Insights Network to be included in transactions that take place in the system. The digital proof of authenticity is a piece of data containing the provider's public key, which can be used to verify the provider's signatures, as well as the provider's account information on the blockchain operating system, which would be needed for sending tokens to the provider.

Our system is designed to allow each party to provide the information they hold as an input to the verification process without disclosing it to anyone else. This is enabled by a technique in cryptography called Secure Multiparty Computation (SMC), which as mentioned in a previous section is a scheme for breaking up a computation into sub-computations and deriving inputs for those sub-computations that cannot be used to figure out what the original inputs are.

As regards identity verification, the inputs are the confidential information held by the verification partners, and the computation to be performed is verifying that information and generating a digital proof of authenticity. The sub-computations are performed by SMC parties, which we introduced in the section on Secure Multiparty Computation. When the SMC parties are finished with their sub-computations, they send their intermediate results to the provider, who assembles them into the digital proof of authenticity, which in effect delivers the digital proof of authenticity to the provider.

The Insights Network is not assigned a computation but contributes its private key as an input. It is used in the computation to generate the signature for the proof of authenticity.

Submitting a data request

This describes how a requester would submit a data request.

1) The requester sends a message to the smart contract containing the survey, a pattern describing the target population, and how much to pay a provider from that target population for a valid data point. The requester also sends tokens to the smart contract to be held in escrow for use as payment to providers. For extra security, since a large number of tokens could be involved, the requester could stipulate that each request be approved by multiple parties from their organization using the blockchain operating system's permission system.

2) Qualified providers fulfill the request. The process for this is described in the section, "Fulfilling a data request."

3) The requester closes the data request once they have received enough data points. If there are tokens remaining after the data request has been closed, they are returned to the requester's account.

Fulfilling a data request

Periodically, the Insights Network client will check with the smart contract to see if there are data requests. It downloads them locally and uses the provider's profile to select which ones to display to the provider. This is the process by which a provider makes a submission for a data request.

1) The provider fills out a survey, producing a data point.

2) The provider sends her proof of authenticity to the requester, which the requester checks for validity. The account name in the proof of authenticity should match the provider's account name. And the signature is validated using the Insights Network's public key.

3) If the proof of authenticity is valid, the provider and the requester engage in a joint computation to see if the provider is qualified to fulfill the data request. For more details on this step, see the section, "Profile matching."

4) If the provider is qualified to fulfill the data request, the provider, the requester, and the smart contract engage in a joint computation to encrypt the provider's data point using the requester's public key, store it in the state of the smart contract, and send tokens to the provider according to

the terms of the data request. For more details on this step, see the section, “Private exchange of validated, encrypted data.”

Profile matching

In our system, a provider must obtain approval from a requester in order to make a submission for a data request. Requesters are expected to give approval to providers whose profiles fit a desired pattern.

One way that this could work is for providers to send their profiles to requesters for vetting. But this could be a breach of privacy, since profiles may contain information that providers would prefer not to disclose. And in any case, the extent to which requesters need to know what is in a profile is whether it fits the pattern they are looking for; they don't actually need to know the profile's exact contents. For example, a requester may only need to know that a provider's age is from 21 to 30, not that the provider is 25 years old.

We plan on using a technique in cryptography called Secure Multiparty Computation (SMC). A mere curiosity in academia for many years, it is beginning to see use in industry. Partisia, a company that implements practical SMC implementations, has used it to implement auctions and surveys for use in production, and we are partnering with them for our implementation.

SMC allows multiple parties to to jointly perform a computation without knowing what all the inputs are. It is suitable for situations in which some of the parties have inputs they do not want to disclose to the others but in which none of the parties object to sharing the final result.

SMC works by breaking up a computation into sub-computations for each party to perform. Inputs for the sub-computations are derived from the original inputs, but they cannot be used to figure out what the original inputs were. At the end, the result of the overall computation is obtained by combining the results of the sub-computations.

In the situation we are facing, there are two parties, a provider and a requester. The inputs to the computation are the provider's profile and a profile pattern provided by the requester. In our system, the requesters and providers would be able to communicate with each other directly over a peer-to-peer protocol, and they would use SMC to compute whether the profile fits the profile pattern, which does not disclose the profile to the requester.

For SMC, we've partnered with FRESCO, which is undergoing active development by the Alexandra Institute in Denmark. Commercial support for FRESCO is provided by the aforementioned company Partisia, also based in Denmark.

Summary

1. Communicating directly over a peer-to-peer protocol, the requester and the provider use SMC to compute whether the requester's profile fits the provider's desired pattern.

2. If the profile is a match, then the requester sends a signed message to the provider that it can include in submissions to the Insights Network smart contract. The signed message contains the account that was approved as well as the survey that the account was approved for.

Private exchange of validated, encrypted data

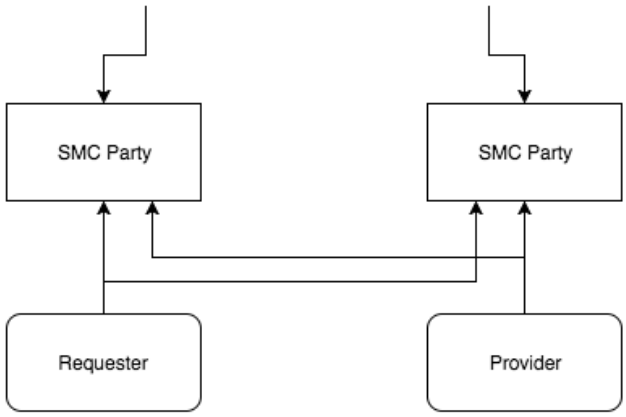
The requester is willing to buy data from the provider if the data meets certain requirements. But the provider is not willing to let the requester see the data prior to receiving payment, because if the requester is in possession of the data, the requester may choose to take it without paying. At the same time, the requester is not willing to pay for the provider's data unless they know the data is "good," which the requester defines as fitting a pattern.

In our system, we will use SMC to resolve this problem. As mentioned previously, SMC is capable of breaking up a computation on inputs into sub-computations on inputs that, while derived from the original inputs, cannot be used to figure out the original inputs. Each party is assigned a sub-computation and the results computed by each party is assembled into the final result. In this scenario, the inputs are the provider's data and the requester's pattern, and the computation is whether provider's data fits the requester's pattern.

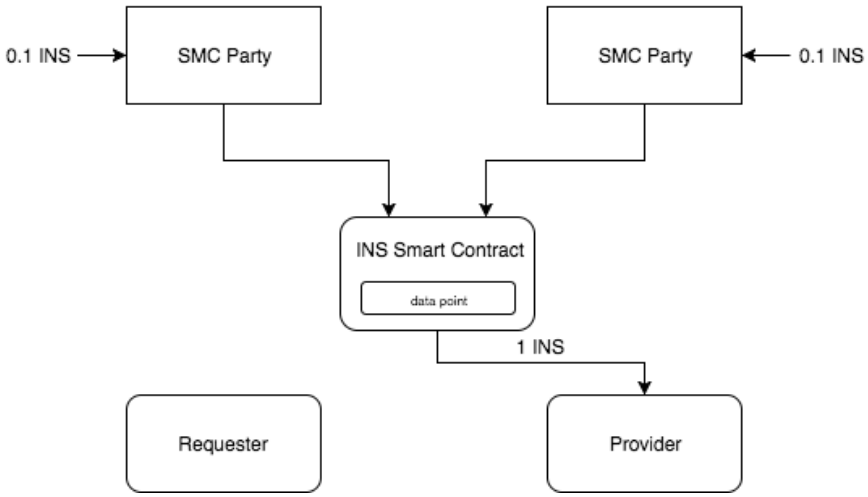
But we do not just want to know if the provider's data fits the requester's pattern. If it is a fit, we would also like the data to be transferred to the requester and for tokens to be transferred to provider's account. So we will make the output of the computation, if the data is a fit, the provider's data encrypted using the requester's encryption key. The SMC parties will send their results, which are intermediate results of a Secure Multiparty Computation, to the Insights Network smart contract, which will assemble them into the final result. If the final result is an encrypted data point, the smart contract will send tokens to provider, and the requester will be able to retrieve the data, which only she would be able to decrypt, from the state of the smart contract. The entire process is captured by this diagram:

1. SMC breaks up the computation into sub-computations and assigns each sub-computation to an SMC party. The requester and the provider use secret-sharing to derive inputs for the sub-computations.

```
function encrypt(providers's data point,
                 requester's pattern,
                 requester's encryption key) {
  if fits(provider's data point, requester's pattern)
    return encrypt(provider's data point, requester's encryption key)
  return Nil
}
```



2. The SMC parties send their results to the INS Smart Contract, which assembles them in the data point, encrypted using the requester's public key, and sends payment to the provider. The provider can read the state of the smart contract for the data point. The SMC parties are paid for their work.



Storage

The major categories of data that pass through the Insights Network are providers' profiles, providers' data points, and the information used during the identity verification process for providers.

Profiles will be stored on provider's local devices. Data points will be stored in the state of the Insights Network smart contract, which is recorded on the ledger, but they will be encrypted. Profiles are used for population targeting, but SMC ensures they are kept private.

The identity verification process entails checking sensitive documents, such as identity documentation, utility bills, and so on. We will store these in encrypted form with strict access control and maintain an access log, which we will regularly audit for unauthorized or inappropriate access. Furthermore, we will only keep this data as long as it is needed. We will delete providers' data after we have issued their digital proofs of authenticity. As soon as blockchain-based ID verification platforms, such as Civic, become operational, we will incorporate them in order make our solution fully decentralized.

EOS Blockchain Platform

We are building on EOS, an upcoming blockchain operating system. Though it is unreleased, it is being developed rapidly, and as of this writing, we are currently building on a test node, as well as hedging our bet by simultaneously building on Ethereum. This section goes into why we have chosen EOS.

Prior to EOS, Dan Larimer, the architect of EOS, was the architect of two highly successful blockchain projects, Steemit and BitShares. Steemit is the only blockchain app that handles a realistic workload, 17,000 daily active users (dau). Graphene, the blockchain used in BitShares, has shown it can handle 20,000 transactions per second on a network. When released, EOS will have the greatest throughput of any blockchain network currently in existence, which will be needed to handle the level of activity we expect in the Insights Network.

In addition, EOS will have several features that make it friendly for operating an app such as the Insights Network.

1) In contrast to Ethereum, users do not need to pay each time they use an app. EOS allocates resources, such as transaction bandwidth, to each account according to the number of EOS tokens held by that account. We plan to use 5% of the funds raised during the ICO to acquire enough EOS tokens for the smart contract to hold in order to support the expected amount of traffic. In other words, the Insights Network will pay for their users to use the smart contract, a concept EOS calls "receiver pays."

Users can also use this resource allocation scheme to ensure access to the Insights Network smart contract in high-demand times. In the event of an ICO or even a denial-of-service attack, users are still entitled to their share of the transaction bandwidth. EOS calls this "rate limiting."

2) Smart contracts and decentralized apps (dApps) can be upgraded to introduce new features and fix bugs, which will allow us to improve the Insights Network rapidly in response to real-world usage.

3) Many of our users are ordinary people, and there is no guarantee that their devices are secure. Inevitably, some of their accounts will be compromised. Unlike other blockchain networks, EOS allows compromised accounts to be recovered with the help of a designated partner, identity documentation, and multi-factor authentication.

Another consideration that is important to the Insights Network is security. Putting out a data request may involve paying out a large number of tokens. If someone were to make an unauthorized data request, our users could be out a lot of money. EOS provides a couple of features that would help in this and other security-critical situations.

1) EOS allows our users to require that some operations are approved by multiple parties. In the case of a data request, our users could stipulate that making a request requires approval by several people within their organization. According to the EOS whitepaper, this feature, which it calls "multi-user control," "is the single biggest contributor to security, and, when used properly, it can greatly eliminate the risk of theft due to hacking."

2) EOS allows apps to add a delay before sensitive operations are recorded in the blockchain, which is when they become irreversible. During the waiting period, users are notified by email or text that the operation is occurring, and they are given a chance to stop it if they did not authorize it. In the case of a data request, our users would be alerted to unauthorized data requests and be given the opportunity to cancel them.

EOS has a bright future. It is well-funded, having raised $185 million in just the first five days of its year-long token distribution. Furthermore, we are well-supported by the EOS team. Given these features and others, we have determined EOS to be the closest fit for our needs.

Token Economics

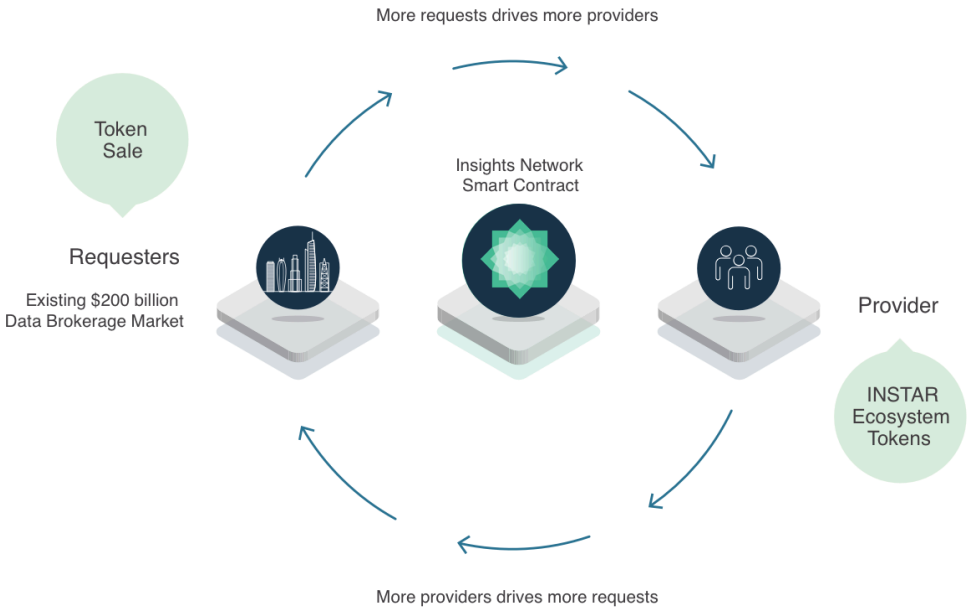
Two-sided Marketplace

The Insights Network is a platform that facilitates transactions between two distinct groups: requesters and providers. Requesters need information from providers and are willing to pay to get it. This dynamic is known as a two-sided marketplace.

Two-sided marketplaces are notoriously difficult to start up. The primary reason for a requester to place a request on the Insights Network is that it has providers who will fulfill it. At the same time, the primary reason for providers to join the Insights Network is that there are enough requests placed in order to make money. At the beginning, there are not enough of either group on the platform to attract the other.

To help with starting up the marketplace, we are issuing a new ERC-20 Insights token. Users who place their data into the Insights Network and participate in market research will be rewarded with Insights tokens. Holders of Insights tokens will be able to place data requests or sell them to people who want to.

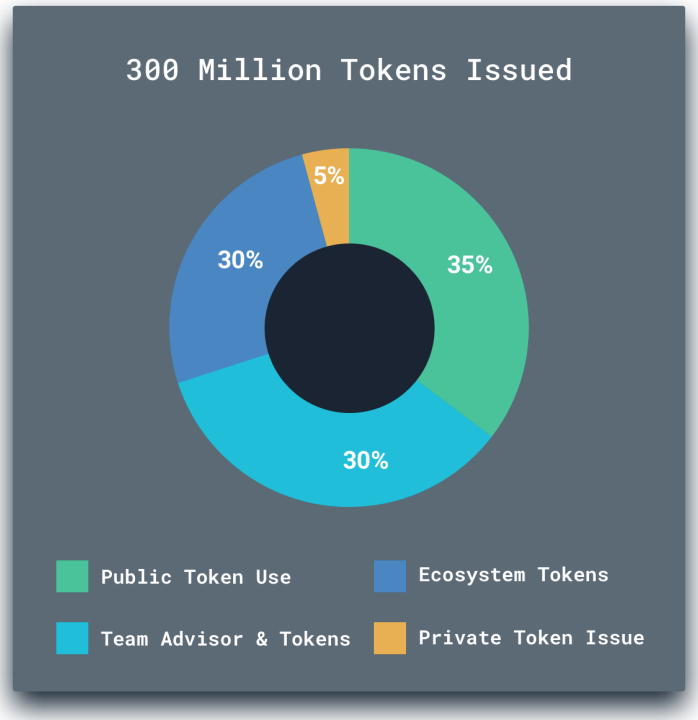
Providers will be able to sell the tokens paid out to them to future requesters, cash them out for things like airline miles or branded gift cards in the reward store, and send them to other users using the Insights Network wallet. As providers join the Insights Network, more requesters will be attracted to join and place data requests, which in turn would attract even more providers. This is known as a network effect, resulting in the network growing very large.



Distribution of Tokens

Tokens will be distributed in the following way:

Total Supply of INSTAR Tokens: 300MM



- 5.0% of tokens will be sold in a pre-sale at a discounted rate to the token sale.
- 35.0% of tokens will be sold in the token sale.
- 30% of tokens will be dedicated to the ecosystem.
- 30% of tokens will be reserved by the company for team, advisors, operations, future engineering hires, R&D

90 million tokens will be issued to the *ecosystem* to be used as payment for early users to fill out their profiles, as well as participate in market research conducted by the Insights Network and early partners. By minting ecosystem coins to early adopters, we create hundred of millions of data points that create a viable data network for requesters to tap into. For example, if each early adopter receives a token for importing ten simple pieces of verified data into their client, these 90 million tokens generate 900 million data points for the Insights Network.

90 million INSTAR tokens will be set aside for the *Company* to be used as compensation for the Insights Network team, including the founders, employees, and advisors, which will incentivize

them to increase the demand for the services offered by the Insights Network, and thus the demand for Insights tokens, by making it a compelling place to conduct market research.

It should be noted that during beta testing of the Insights Network Desktop Client an Insights ERC-20 token will be used until the EOS platform is fully functioning and public. At the time of this release, there will be a one-time migration for token holders to swap their ERC-20 Insights tokens for the equivalent Insights EOS currency.

Token Sale Cap - 25,000 ETH

Use of Funds

Development - 50%

Operations - 25%

Marketing - 15%

Legal - 10%

Team

Brian Gallagher - W.P. Carey School of Business, Y-Combinator

Darwin Lo - Stanford Computer Science, Y-Combinator

Brandan Zaucha - W.P. Carey School of Business, Y-Combinator

Dylan Herman - Univ. Illinois, Engineering

Dino Amaral - Ph.D. Cryptography

If you have a passion for big data, are a computer scientist and love startups, contact us

team@insights.network

Advisors

Kurt Nielsen

Jesper Blue Nielsen

Peter Frands Frandsen

Andrew Rosener

Jason Hamlin

David Goboud

Roadmap Draft

Insights: Q1-Q3 2017

-Proof of Concept

-Launch the Insights Network website

-Development work initiates on EOS test net

Insights: Q4 2017

-Announcement of Project at BlockCon

-Release final draft of white paper

-Token Pre-sale

-INSTAR Wallet Integration Gambeal App

Insights: Q1 2018

-Token Crowd sale

-INSTAR Network Desktop Client Beta ERC-20 tokens redeemable in client

Insights: Q2 2018

-Secure Multi Party Computation

Insights: Q3 2018

-EOS Platform Beta Opens

Insights: Q4 2018

-INSTAR EOS blockchain Desktop Client Fully Functional Publicly Available Polling Daily

Conclusion

Data brokers collect intimate information on individuals without their permission and sell them to anyone who is willing to pay, even organizations that have considerable influence over the course of their lives, including universities, hospitals, and insurance companies. This is not just an invasion of privacy; it is surveillance. And there is little that consumers can do to stop this practice, even if they are among the few who know it is happening.

Fortunately, governments throughout the world are cracking down on data brokers. The European Union has enacted the Data Protection Directive, which regulates how organizations should handle what it calls “personal data.” Brazil prohibits transmitting data to another party that contains Personally Identifiable Information (PII). In the United States, Senator Edward Markey (D-MA) is sponsoring a bill called the Data Broker Accountability and Transparency Act of 2017.

We will work to promote regulations that demand a higher standard for the handling of sensitive, personal information. But even in the absence of regulations, we believe that our solution will be superior to existing data brokers and will win in a free market competition by providing superior information and putting consumers in control of their own data.

We predict that, in 10-20 years, due to the rise of decentralized technology, there will be no intermediaries. Organizations will use our platform to transact with consumers directly for their data. Organizations currently pay $200 billion per year for this data -- Forbes predicts that this will only grow. We think the Insights Network will grow to meet this demand and shift control and profit away from middle men such as Acxiom to the data’s rightful owners, the consumers.

Sources

1. EOS.IO Technical White Paper

2. Multi Party Computation: From Theory to Practice

3. The secretive world of selling data about you (Newsweek)

4. 6 predictions for the $125 billion Big Data Analytics market in 2015 (Forbes)

5. Acxiom database hacked (Computerworld)

6. Equifax announces cybersecurity incident involving consumer information (Equifax)