통찰 네트워크

- 블록체인 데이터 교환
2017 년 12 월 29 일 (v0.5)

브라이언 갤러거
통찰 네트워크
bg@insights.network

다윈 로우
통찰력 네트워크
darwin@insights.network

피터 프란츠 프란슨
파르티시아
pff@partisia.com

제스퍼 부스 닐슨
파르티시아
jbn@partisia.com

커트 닐슨
파르티시아
kn@partisia.com

개요

현재 데이터 브로커들는 온라인과 오프라인의 다양한 출처를 통해 전 세계 개인에 대한 데이터를 수집한다. 데이터는 프로파일로 패키지화된다. 이 프로파일들은 다양한 업체들에게 판매된다. 업체들은 받은 데이터를 통해 하는 결정들이 아무도 모르게 평범한 사람들의 삶에 영향을 줄 수 있다.
블록체인과 시큐어 멀티파티 계산과 같은 최근의 기술적 진보로 인해 데이터를 생성하는 사람의 손에 데이터를 제어하고 수익화하는 동시에 시장 조사를 수행하기 위한 우수한 플랫폼을 구축할 수 있다.

info@insights.network

컨텐츠

info@insights.network

info@insights.network

1 폭로

여기에서 어떠한 것도 토큰을 판매하거나 구매하기 위한 제안의 권유를 구성하지 않으며, 이러한 불법적인 제공, 권유 또는 판매가 이루어지는 모든 관할 구역에서 통찰 네트워크 인스타 토큰을 제공하지 않는다. 본 백서와 모든 업데이트를 주의하여 읽고 완전히 이해해야 한다. 모든 잠재적 토큰 구매자는 신분 확인 및 기타 특정 문서를 포함하는 온보드 프로세스를 거쳐야 한다. 이 프로세스는 법적 구속력이 있으므로 주의 깊게 읽고 완전히 이해해야 한다. 반드시 적절한 조언자 등과 상의해야 한다.

이 백서에서는 통찰 네트워크 플랫폼에 대한 우리의 비전을 설명한다. 우리가 이 비전을 실현하기 위해 노력하는 동안, 이것이 상당히 많은 요인에 의존하고 있고 상당히 많은 위험에 노출될 수 있다는 것을 인식해야 한다. 통찰 네트워크 플랫폼이 결코 구현되거나 채택되지 않을 수도 있으며, 또는 우리 비전의 일부만 실현될 수도 있다. 당사는 본 백서의 어떠한 진술도 보증, 대표 또는 보증하지 않다. 이 요소들은 우리의 현재의 신념, 기대, 가정에 근거하고 있으며, 예상치 못한 여러가지 사건이 발생할 수 있기 때문에 장담할 수 없다.

부디 우리가 이 백서에서 제시한 비전을 달성하기 위해 열심히 노력할 계획이지만, 그 어떤 것도 실현되지 않을 수도 있다는 것을 알아 두기를 바란다. 블록체인, 크립토 통화와 우리 기술의 다른 측면과 이 시장들은 그들의 걸음마 단계에 있고 많은 도전, 경쟁을 거쳐야 하고 변화하는 환경에서 영향을 받을 것이다. 우리는 상황이 커지고 변화함에 따라 우리 지역 사회를 업데이트하기 위해 노력할 것이지만 그렇게 할 의무를 떠맡지 않을 것이다.

2 배경

2.1 문제

데이터 브로커라고 불리는 조직들은 온라인과 오프라인의 다양한 출처에서 사람들에 대한 데이터를 수집한다. 가장 주목할 만한 점은 사용자 정보를 수집하고 그들의 앱 내 동작을 추적하는 인터넷 서비스와 모바일 애플리케이션에서 데이터를 구매한다는 점이다.

이 데이터는 개별 소비자에 대한 프로필을 생성하는 데 사용된다. 최고의 데이터 중개인인 Acxiom 은 2 억명 이상의 미국인에 대한 평균 1,500 개의 정보를 가지고 있다. Acxiom 및 기타 데이터 브로커들은 각 개인에 대한 모든 정보를 결합하여 광범위한 업종에서 판매하는 소비자 행동 보고서를 심층적으로 작성할 수 있다.

데이터 브로커들은 많은 돈을 번다. 2012 년에 Acxiom 은 13 억 2 천만달러의 매출을 올려 7726 만달러의 이익을 낸 것으로 알려졌다. 포브스에 따라서, 빅 데이터 분석이 (Big Data Analytics) 연간 2,000 억달러 규모의 산업이며, 2019 년 쯤에 거의 모든 기업이 Acxiom 과 같은 데이터 브로커의 고객이 될 것이라고 보도했다. 그러나 실제로 그 산업을 주도하고 있는 소비자들은 이익을 함께 챙기지 못하고 있다.

동시에, 그들은 결론적으로 많은 부정적인 결과들을 경험한다. 중앙 집중식으로 관리되는 데이터베이스를 사용하면 해커가 단 한번의 공격으로 많은 양의 개인 식별 정보를 도용할 수 있으므로 대규모의 ID 도용 및 사기가 허용된다. 최근에 해커들이 Equifax 의 시스템을 침입해 1 억 4 천만명 이상의 미국인에 대한 개인 식별 가능 데이터를 훔쳤다. 이것은 고립된 사건이 아니다. 과거에도 Acxiom 을 포함하여 여러건의 공격이 있었으며, 만약 확인되지 않은 경우에는 앞으로 더 많은 공격이 있을 것이다.

소비자들은 시장 조사에 사용되고 있는 개인 식별 가능하고 민감한 정보를 저장하기 위한 새로운 표준을 요구해야 한다. 이는 현재 유럽 전역의 GDPR 에서 구현되고 있으며 곧 미국도 이에 동조하게 될 것이다.

2.2 해결책

최근 분산형 스토리지, 디지털 통화 및 스마트 계약의 발전으로 인해 우리는 마케팅 연구를 수행하고 소비자 데이터를 안전하게 저장하기 위한 분산형 인센티브 플랫폼을 구축할 수 있다. 기업들은 우리의 플랫폼을 이용하여 정확하게 정의된 인구 집단인 통찰 네트워크의 데이터를 요청할 수 있을 것이다.

데이터 브로커가 아닌 네트워크 사용자가 데이터를 판매하게 될 것이다. 익명 파티 간 거래를 실시하는 스마트 계약을 통해 사용자들은 자신의 신원을 밝히지 않고도 오직 광범위한 인구 통계학적 정보만을 대상으로 데이터를 판매할 수 있게 된다. 익명 파티 간 거래를 실시하는 스마트 계약을 통해 사용자들은 자신의 신원을 밝히지 않고도 오직 광범위한 인구 통계학적 정보만을 대상으로 데이터를 판매할 수 있게 될 것이다. 블록체인 및 시큐어 멀티파티 계산 (SMC)의 고유한 조합을 통해 타사의 개입 없이 공급 업체 (공급자/제공자)와 데이터 요청자 간에 데이터 교환 및 지급을 적용할 수 있다. 블록체인이 교환을 투명하게 하는 동시에, SMC 은 계약이 체결되고 지불될 때까지 진정으로 데이터를 안전하게 유지한다.

소비자가 참여함으로써 수익을 낼 수 있기 때문에 조직에서는 더 적절하고 실용적인 데이터를 확보하게 될 것이라고 믿는다. 이와 동시에, 데이터 브로커에 의해 현재 획득된 이익은 대신에 정당한 데이터 소유자인 소비자에게로 갈 것이다.

3 우리 제품

3.1 개요

주로 다음 두가지 유형의 사용자를 대상으로 일한다. 데이터를 요청하는 사용자와 이를 제공하는 공급자 또는 제공자라고 불리는 사용자이다. 요청자는 일반적으로 조직이지만 누구나 INSTAR 토큰을 구매하여 통찰 네트워크에 데이터 요청을 제출하는 데 사용할 수 있다. 공급자는 데이터 제공을 통해 데이터 요청을 준수하는 사용자이며, 데이터 요청자의 목표 인구 통계학적 목표에 부합하는 사용자는 INSTAR 토큰으로 자신의 데이터를 보상 받는다.

요청자는 다음과 같은 데이터를 수집하고자 한다.

●**관련된 정보.** 예를 들어, 20 세에서 35 세 사이의 사람들만 특정 모집단에서 데이터를 수집할 수 있기를 원한다.

●**신뢰할 수 있는 정보**. 수집된 데이터는 사기 행위가 없다. 즉, 데이터를 정직하게 제공한 대상 공급자에게서 데이터를 수집한다. 예를 들어, 요청자는 봇이 아닌 실제 표적 인구 통계학에 의해 사실적으로 설문 조사가 답변되기를 기대한다.

●**시간대에 맞고 편리한 정보.** 요청자는 목표 고객 통계학적으로 도달하는 방법에 대한 세부 정보를 걱정하지 않고도 신속하게 질문에 대한 답을 얻을 수 있어야 한다.

공급자들은 다음과 같은 사항들의 보증을 원한다.

●**찬성.** 이들의 데이터는 이들의 명시적인 허가 없이는 수집되지 않는다.

●**프라이버시.** 개인 정보(예:자신의 존재)와 같은 중요한 정보는 제공되지 않으며, 폭넓은 인구 통계학적 세부 정보만 제공된다.

●**지불.** 제공하는 데이터에 대해 지불을 받는다.

●**보안.** 데이터를 안전하게 처리한다.

기존의 마케팅 조사 회사들은 일정 기간에 걸쳐 데이터를 수집하여 고객에게 단일 보고서를 제공한다. 저희 플랫폼에서는 요청자가 데이터 요청을 끝낼 필요가 없다. 그들이 데이터를 수집하는 동안 언제든지 볼 수 있는 보고서는 스마트 계약에 의해 수신되고 전송되는 제공자의 데이터로 업데이트된다.

네트워크에서 더 많은 데이터를 사용할 수록 플랫폼이 요청자에게 제공하는 데이터는 더욱 광범위해지며, 이를 통해 두개 이상의 데이터 요청 데이터를 결합하는 보고서를 포함하여 보다 포괄적인 보고서를 설계할 수 있다.
다음은 통찰력 네트워크를 사용할 수 있는 몇가지 예시이다.

●여론 조사 회사는 현재 대통령 선거가 다시 실시된다면 누가 이길 것인지를 알아보기 위해 여론 조사를 실시하고 싶어 할 수 있다.
●맥도널드는 새로운 메뉴 항목에 대한 피드백을 구하기 위해 설문 조사를 실시하고 싶어 할 수 있다.
●대학교들이 분기 또는 학기 전체에 걸쳐 강의에 대한 설문 조사를 실시하여 지속적으로 지침의 품질에 대한 피드백을 받고 싶어 할 수 있다.
● 최고급 경매는 KYC 를 실시하지 않고도 검증된 개인의 익명 입찰을 받고 싶어 할 수 있다.

관련된 사용 사례 그룹은 개인과 회사를 프로파일링 하여 소위 비대칭 정보를 다룬다. 금융적 예시: 돈을 빌려준 사람이 대출 받은 자 갚아주는 능력에 대해 대출 받은 자보다 덜 알고 있는 상황이다. 이런 상황은 평균 예상 위험을 보상하기 위해 다른 방법으로는 낮은 위험 차입자에 대한 더 높은 이자율을 야기할 수 있다. 이 문제에 대한 해결책은 위험성이 높은 대출자로부터 위험도가 낮은 것과 같이 분리하기 위해 가능한 한 많은 개인과 기업을 프로파일링 할 수 있는 정보이다. 보험 회사가 보험 계약자의 신상 정보에 대해 덜 알고 있는 보험 사업에서도 비슷한 문제가 발생한다. 또 다른 예시는 제품 차별화로, 제품이나 계약의 가장 적합한 메뉴를 정의하기 위해 공급 업체가 고객의 선호도에 대한 정보를 부족하게 만드는 것이다. 후자의 한가지 예시는 가격 및 데이터 등과 관련하여 모바일 가입자의 올바른 메뉴를 설계하는 문제일 수 있다.

통찰 네트워크는 개인이나 기업이 은행 및 보험 회사와 등 협력하여 이 문제를 동등한 조건으로 해결할 수 있는 플랫폼을 제공한다. Insights Network(통찰 네트워크)는 개인과 회사를 프로파일링 하는 데 사용되는 고유한 정보 소스가 될 수 있다.

3.2 기능성

Insights Network 는 다양한 애플리케이션이 있는 분산된 데이터 교환을 위한 보안 인프라이다. 처음에는 설문 조사에 집중하겠지만 로열티 제도, 광고, 로열티 제도와 같은 다른 애플리케이션의 기반도 될 것이다.

Insights Network 는 다음과 같은 구성 요소로 이루어진다.
●인증
●사용자 프로필
●분산형 데이터 중개
●설문 조사
●양측 평가

요청자는 특정 사용자 집단의 정보를 얻기 위해 Insights Network 에 요청을 하는 사용자이다. 공급자들은 그러한 요청을 이행하는 사용자들이다.

3.2.1 버전 인증

오늘날 앱들 사이에서 흔히 볼 수 있는 것은 사용자가 페이스북 계정을 사용하여 로그인할 수 있도록 하는 것이다. 우리는 사용자가 Insights Network 계정을 사용하여 로그인할 수 있도록 하기 위해 애플리케이션에 대해 비슷한 서비스를 구축하고 있다. 이는 자신의 신원을 앱에 공개하고 싶지 않은 사용자에게 어필할 것이다. 또 다른 이점으로 Insights Network 를 사용하여 보상 프로그램의 일환으로 사용자에게 토큰을 제공하고 항공사 마일과 같은 보상을 위해 이들을 현금으로 바꿀 수 있다.

info@insights.network

인증은 SMC 을 사용하여 비공개로 수행된다.

3.2.2 사용자 프로필

사용자는 Insights Network 프로파일을 유지한다. 사용자들은 자신의 프로필을 볼 수 있는데, 그 프로필은 인구 통계학적 정보와 다른 일반적인 식별할 수 없는 정보를 포함하고 있다. 사용자들은 수정하고, 누락된 세부 정보를 입력하고, 정보를 삭제할 수 있다. 게다가, 정보를 삭제하는 것 외에도, 사용자들은 이러한 행동을 수행하기 위해 주조된 INSTAR 토큰도 사용한다.

예를 들어, 로스 앤젤레스에 사는 25 세 여성이 자신의 정치적 관심사와 관련된 광고를 받고 싶어 할 수도 있기 때문에, 그녀가 공화 당원이라는 것을 보여 주는 노선을 유지하는 것을 선택할 수 있다. 하지만 그녀는 싱글 맘이 되는 것과 관련한 설문 조사를 받고 싶어 하지 않을 수도 있다. 그래서 그녀는 그 과목을 삭제할 수 있다. 그녀는 또한 그녀의 직업이 알려지지 않았다는 것을 원한다면 INSTAR 토큰의 교환으로 직업을 기입하는 것을 선택할 수 있다.

사용자 프로필은 클라이언트 측 또는 SMC 을 통해 기밀로 유지된다.

3.2.3 분산 데이터 중개

Insights Network 의 기본적인 목적은 다음으로 구성된 공급 업체와 요청자 간에 분산된 데이터 교환을 가능하게 하는 것이다.
●제공 업체의 프로필을 요청자의 요구와 일치시키기
●보안 데이터 전송
●보증금

교환할 데이터는 처음에 설문지에 대한 관련 배경 정보 및 사용자가 제공한 답변으로 구성된 조사 데이터이다. 블록체인과 SMC 의 고유한 조합은 타사의 개입 없이 비밀 정보 교환과 지불을 보장한다.

3.2.4 조사

통찰 네트워크에 있는 사람이라면 누구나 개별적인 사람이든 조직적인 사람이든 간에 설문 조사를 플랫폼에 게시할 수 있다. 이 플랫폼은 대상 인구 통계학적 데이터를 지정할 수 있는 기능과 더불어, 대상 인구 통계학적 데이터 스토어에 있는 사용자가 유효한 응답을 제출할 때 수신할 토큰의 수를 제공한다. 이 과정은 다음과 같다.
1. 요청자는 대상 인구 통계학적 목표를 명시하는 설문 조사를 발행한다.
2.우리 앱의 사용자들은 목표 인구 통계학적으로 적합한 사용자들에게 통지를 받는다.
3. 사용자들은 설문 조사를 작성하여 Insights Network 에 제출하면 자신의 계정으로 자금이 이체된다.

3.2.5 양측 평가

원치 않는 행동을 다루기 위해, Insights Network 는 양면 평가 시스템을 구현하며, 요청자는 제공자를 평가하거나 그 반대의 경우도 가능하다.

제공자로서, 시스템을 오용하고 거짓 데이터를 제공하는 것이 가능하다. 이러한 원치 않는 행동 중 일부는 데이터를 분석하는 동안 요청자가 탐지할 수 있다. 요청자에게 제공자의 등급을 매길 수 있는 기회를 제공하는 것은 그러한 행동에 대응할 것이다.

요청자로서 데이터는 합의된 목적을 벗어나서 사용할 수 있다. 최종 보고서가 발간되면서 제공자가 이러한 원치 않는 행동 중 일부를 탐지할 수 있다. 공급자에게 요청자를 평가할 수 있는 기회를 제공하면 이러한 행동에 대응된다.

양측 평가 결정을 통해 원하지 않는 행동을 분산적으로 통제하는 것은 Uber 및 Airbnb 와 같은 서비스로부터 친숙하다.

3.2.6 예시:

감비알 감비알(Gambeal)은 식당의 고객들에게 설문지를 관리하고 그들이 기입하는 각각의 설문 조사에 대한 소액의 현금 보상을 제공하는 iOS 앱이다. 자신의 후원을 입증하기 위해, 각 사용자는 자신의 영수증 사진과 각 제출물을 첨부해야 하며, 이는 보상이 발행되기 전에 입증된다. 감비알은 어떠한 의도적인 마케팅 노력 없이 상당한 성장을 보았고, 매주 수천건의 거래를 처리한다. 이는 첫번째 Insights Network 파트너 앱이 될 것이며, 지금까지의 성공은 다른 파트너 앱에 좋은 징조이다.

통합의 일환으로 감비알은 사용자들이, 예를 들어, 페이스북으로 로그인하는 것처럼, 자신들의 ID 를 포기하지 않고 로그인할 수 있게 해 주는 Insights Network 의 SMC 기반 인증 시스템으로 인증 시스템을 교환할 것이다. 사용자는 이 앱에 광범위한 인구 통계학적 세부 정보만 공개되며, Insights Network 의 일부이기 때문에 원하는 대로 데이터를 수익화할 수 있다.

또한 감비알은 통합을 위해 Mobius Universal Protocol API 를 사용하여 현금 보상에서 INSTAR 토큰으로 전환할 것이다. 감비알은 현재 페이팔을 사용하여 사용자들에게 결제하고 있으며, 이것은 사용자들이 그들의 페이팔 계정에 보상이 나타날 때까지 기다리는 과정을 거쳐야 하고, 거래 수수료의 3%까지 지불한다. 더 나은 개인 정보 보호 기능을 제공하는 것 외에도, Insights Network 를 사용하면 감비알이 사용자에게 저렴한 비용으로 신속하게 거래를 처리할 수 있게 됩된다. 인증 및 보상을 위해 Insights Network 와 통합하면 사용자 환경이 대폭 개선된다.

3.3 기술 과제

해결해야 할 몇가지 과제가 있다. Insights Network 의 다음 기능은 요청을 실행하고 이행하는 데 도움이 된다.

- **신원 확인.** 공급자가 여러 검증 파트너의 인증을 통해 자신이 실제 사용자임을 입증한다 --신원을 확인하는 회사, 신원 조사를 수행하는 서비스, 또는 고용주까지도 포함한다 --그리고 요청자와의 거래에서 그들의 진실성을 증명하기 위해 사용할 수 있는 Insights Network 에서 진실성의 디지털 증명을 얻는 것이다. 검증 파트너는 분산 암호화 기술을 사용하여 공급자의 개인 정보를 보호하는 다른 업체에 정보를 절대 넘기지 않으며, 제공 업체가 이 과정을 거친 데 대한 토큰으로 보상 받는다.
- **인센티브 보상 시장 조사.** 요청자는 Insights Network 스마트 계약을 통해 설문 조사를 게시하고 설문 조사 응답을 받을 수 있다. 스마트 계약은 유효한 데이터 포인트를 제출한 대상 모집단의 제공자에게 토큰을 전송한다.

● **블록체인-검증 가능한 결과**. 요청자의 재량에 따라 데이터 요청의 데이터 포인트는 누구나 열람할 수 있도록 원장에 기록할 수 있다. 원장은 블록체인을 사용하여 작성되기 때문에, 이 기록을 보는 사람이라면 누구나 데이터 포인트가 변조되지 않았다는 합당한 보증을 할 수 있을 것이다. 이 특징은 투표나 투표와 같은 특정한 종류의 조사에 중요하다. 필요한 경우, 블록체인에 대한 보안 암호화를 이론적으로, 정보 목적으로 데이터를 암호화할 수 있다.

●**시멘틱 비공개 데이터 검증.** 제 3 자와 관련하지 않고, 제공자는 요청자가 대금을 수령할 때까지 데이터를 보류할 수 있으며, 요청자는 제공자의 데이터가 유효한 것으로 입증될 때까지 지급을 보류할 수 있다.

4 기술적 솔루션

이 솔루션의 두가지 주요 기술 구성 요소는 블록체인과 SMC(SecureMultiparyComputing)을 수행하기 위한 프로토콜이다. 이 두 기술은 거래를 실행하기 위해 제 3 자에게 중요한 역할을 맡길 필요를 제거하기 위해 분산 암호화를 사용한다. 즉, 둘 다 '신뢰할 수 없는' 기술이다. 이와 동시에 두 기술은 다음과 같은 상호 보완적인 특성을 제공한다. 블록체인은 투명함을 제공하는 동시에 SMC 은 개인 정보 안전 보호를 제공한다.

SMC 은 30 년 이상 학계에 관여해 왔다. 산업에서의 사용은 SMC 의 계산적인 비용 때문에 사용이 제한적이었다. 그러나 2008 년에 덴마크에 있는 회사인 파르티시아(Partisia)는 처음으로 SMC 의 상용 구축을 발표하고 기존 경매인을 이중으로 교체했다. 그 이후로, 규모의 순서에 의해 성능이 향상되었으며, 현재는 업계에서 채택되기 시작하고 있다.

블록체인은 비코인으로 시작했다. 그리고 나서 에테럼(Ethereum)은 스마트 계약을 지원하는 블록체인을 소개했다. 블록 생산에 사용되는 새로운 알고리즘을 사용하여 비트코인 (Bitcoin)및 Ethereum 둘 다보다 훨씬 더 높은 트랜잭션 처리량을 달성하는 EOS 가 다음 주요 블록체인이 될 것으로 장담한다.

우리는 블록체인과 SMC 기술이 함께 빠른 성장을 예상하고 있다. 게다가, 우리가 우리의 시스템에서 하고 있는 것처럼, 우리는 종종 블록체인과 SMC 의 보완적인 특성을 위해 결합될 것이라고 생각한다. 저희 시스템의 디자인과 구현을 돕고 있는 파트너인 파르티시아와 함께 우리는 '신뢰할 수 없는' 컴퓨터 분야에서 새로운 트렌드를 시작하고 있다고 생각한다. 이 섹션에서는 SMC 을 사용하는 방법과 섹션 3.3 에 나와 있는 문제를 해결하기 위한 블록체인에 대해 다룰 것이다.

4.1 블록체인

블록체인은 변조 방지 공개 원장의 구현이다. 원장의 상태는 독립적으로 운영되는 서버들 사이의 합의에 의해 결정되는데, 이 서버들은 블록체인 네트워크라고 불리는 네트워크를 형성한다. 단일 서버나 심지어는 작은 서버 그룹이 공모하여 다른 서버에 의해 탐지되지 않고 원장 항목을 변조하는 것은 불가능하다. 네트워크에 독립적이고 프로토콜을 지원하는 서버가 충분하다면, 원장은 변조를 방지할 수 있다.

블록체인은 예금주가 계좌 간 자금의 움직임에 대한 기록을 유지하는 것 외에도 프로그램의 상태에 대한 변경 사항을 기록할 수 있다. 블록체인 네트워크에서 호스팅 되는 프로그램을 스마트 계약 또는

분산 애플리케이션이라고 한다. Insights Network 는 블록체인 및 블록체인 기반 스마트 계약을 사용하여 작업을 기록하고, 보안 다중 공유의 출력을 취합하고, 계정 간에 자금을 전송한다.

4.1.1EOS 블록체인 플랫폼

우리는 곧 출시될 블록체인 운영 시스템인 EOS 를 개발할 예정이다. 비록 공개되지는 않았지만, 이 기술이 빠르게 발전하고 있으며, 이로써, 우리는 현재 지역 시험 노드를 구축하고 있으며, 동시에 에테륨을 기반으로 하여 개발을 하고 있다. 이 섹션에서는 EOS 를 선택한 이유에 대해 설명한다.

EOS 시점 이전에 EOS 를 설계한 Dan Larimer 는 두가지 성공적인 블록체인 프로젝트인 Steemit 와 BitShares 를 설계했다. Steemit 는 현실적인 작업 부하, 17,000 명의 일일 활성 사용자를 처리하는 유일한 블록체인 애플리케이션이다. BitShares 에 사용되는 블록체인인 Graphene 은 네트워크에서 초당 20,000 건의 트랜잭션을 처리할 수 있다는 것을 보여 주었다. EOS 는 출시되면 현재 존재하는 모든 블록체인 네트워크의 처리량이 가장 우수해 지며, 이는 Insights Network 에서 기대하는 작업 수준을 처리하는 데 필요하다.

또한 EOS 에는 Insights Network 와 같은 애플리케이션 운영에 적합한 여러 기능이 포함되어 있다.
1. EOS 는 트랜잭션 대역 폭과 같은 리소스를 각 계정에 할당하는 데 이는 해당 계정이 보유하고 있는 EOS 토큰 수에 따라 달라진다. 또한 앱이 사용자들의 사용에 대해 요금을 지불하게 하기 때문에, 사용자들이 Ethereum 과 같은 다른 블록체인 네트워크와 달리 앱을 사용할 때마다 요금을 지불할 필요가 없다.
2.스마트 계약과 분산 애플리케이션(dApps)은 새로운 기능을 도입하고 버그를 수정하기 위해 업그레이드될 수 있으며, 이를 통해 실제 사용 환경에 대응하여 통찰 네트워크를 빠르게 개선할 수 있다.
3. 우리 사용자들 중 많은 사람들이 평범한 사람들이고, 기기가 안전하다는 보장도 없다. 불가피하게, 그들의 일부 계정이 손상될 수밖에 없다. 다른 블록체인 네트워크와 달리 EOS 는 거래처들이 신원 확인서와 다중 요인 인증을 제공할 경우 거래처를 복구할 수 있게 해 준다.

우리 토큰 판매 수익금의 일부는 EOS 토큰을 인수하고 보유하는 데 사용될 예정이다. EOS 토큰 보유자는 EOS 블록체인에서 발생하는 다른 활동으로 인한 중단 없이 네트워크를 통해 보장된 트랜잭션 대역 폭을 제공 받을 수 있다. 예를 들어 ICO 나 서비스 거부 공격이 발생하는 경우에도 사용자는 여전히 트랜잭션 대역 폭의 자신의 몫을 사용할 수 있다. EOS 는 이를 "속도 제한"이라고 한다.

통찰 네트워크(Insights Network)에서 중요한 또 다른 고려 사항은 보안이다. 데이터 요청을 실행 중지하면 많은 수의 토큰을 지불해야 할 수 있다. 누군가 무단 데이터 요청을 한다면 원치 않는 거래가 발생할 수 있다. EOS 는 이러한 상황 및 기타 보안 위험이 있는 상황에 도움이 되는 몇가지 기능을 제공한다.
1. EOS 를 통해 사용자들은 일부 작업에 대해 여러 파티의 승인을 받도록 요구할 수 있다. 자료 요청의 경우에, 우리의 사용자들은 요구를 하는 것이 그들의 조직 내의 몇몇 사람들에 의해서 승인을 요구하는 것을 규정할 수 있다. EOS 백서에 따르면’다중 사용자 제어’라고 하는 이 기능은 보안에 가장 크게 기여하는 요소 중 하나이며 적절히 사용할 경우 해킹으로 인한 도난 위험을 크게 줄일 수 있다.

info@insights.network

2. EOS 를 사용하면 앱이 지연을 추가한 후에 민감한 작업이 블록체인(즉, 복구할 수 없게 되는 시점)에 기록된다. 대기 시간 동안 사용자는 작업이 발생하고 있다는 사실을 이메일이나 문자 메시지를 통해 통지 받으며, 권한을 부여 받지 못한 경우 작업을 중지할 수 있다. 데이터 요청이 있을 경우, 사용자는 무단으로 데이터를 요청할 수 있으며 이를 취소할 수 있다.

우리는 EOS 가 밝은 미래가 있다고 생각한다. 동사는 1 년간 1 억 8500 만불을 판매한 데 이어 5 일 만에 자금을 충분히 지원 받았으며 EOS 팀으로부터의 지원을 받고 있다. 이러한 점과 그 외에도 다른 고려 사항을 감안하여, 우리는 EOS 가 우리의 요구 사항에 가장 적합한 것으로 판단했다.

4.2 시큐어 멀티파티 계산(SMC)

시큐어 멀티파티 계산은 알려지지 않은 데이터에 대한 계산을 지원하는 최신 암호화 솔루션 클래스에 속한다. 처음에는 불가능한 것처럼 보일 수도 있지만 올바른 암호화를 사용하는 경우 그렇지 않다. SMC 과 더불어 이러한 솔루션 클래스에는 zkSNARKs 와 Homorphic 암호화와 같은 기술이 포함된다. SMC 은 계산을 분산 컴퓨팅으로 변환하여 이 목표를 달성한다. 이 경우에는 계산의 어느 참가자도 완전한 입력을 볼 수 없고 오히려 그 자체로 전체 입력에 대한 정보를 제공하지 않는 파생물로 볼 수 있다.

이 개념의 근본적인 측면은 샤미르(Shamir, 1979)로 시작됬으며, 1980 년대에 이 이론이 확립되었다 (Chaum 1988). SMC 이 1980 년대 중반에 일반적으로 적용되는 것으로 이론적으로 나타났지만, SMC 의 컴퓨팅 복잡성은 20 년 동안 실용적인 사용을 가로막았다. SMC 의 최초 대규모 상용화 및 상용화는 이중 경매에서 기존 경매인을 교체하기 위해 SMC 을 사용한 2008 년에 덴마크 기반 회사인 Partisia 에서 수행했다.

2008 년부터 이 기술은 SMC 프로토콜의 특성 뿐만 아니라 계산 속도 측면에서도 발전했다. 계산 오버헤드가 약 100 만으로 줄었습니다. SMC 의 개발은 다음 문서를 읽어 추적할 수 있다: 핀카스와 연구팀(2009), 세랏과 셴(2011), 슨과 연구팀(2012 년), 프레 데릭센과 닐슨(2013), 프레 데릭센과 닐슨(2014 년), 린델과 리바 (2015), 닐슨과 연구팀(2017 년).

1 www.sepior.com
2 www.tora.com

4.2.1 사용자 정의 SMC 시스템

SMC 은 다양한 응용 프로그램 집합에 적용할 수 있다. 이는 단일 프로토콜이 아니라 각각 다른 특성을 지닌 솔루션의 성장하는 클래스이다. 여러 SMC 시스템은 키 관리 및 재무 주문 매칭과 같은 다양한 응용 프로그램의 특정 요구를 충족하기 위해 고안되었다.

모든 SMC 솔루션에 공통적으로 포함되는 역할은 다음과 같으며, 각 개인 또는 조직에는 다음 중 하나 이상이 포함된다.

1.**컴퓨팅 작업의 파티**인 당사자들은 분산 컴퓨팅을 수행할 책임이 있다.

2.**입력 파티**는 그들이 비밀로 하고 싶은 계산을 위한 입력을 가지고 있다. 이를 위해, 비밀 공유라 불리는 기술을 사용하여 각 입력을 다른 컴퓨터 정당에 전달되는 부분으로 분해한다. 어떤 계산 파티도 한 입력에 대해 두개 이상의 부품을 가지고 있지 않으며, 어떤 부품도 원래의 입력을 유도하기에 충분한 정보를 제공하지 않는다.

3.**결과 파티**들은 컴퓨터 파티들이 그들의 결과를 보내는 파티들이다. 결과 파티들은 그들이 컴퓨터 당사자들로부터 얻은 데이터를 전체적인 계산의 결과로 조합한다.

결정적으로, 입력 파티 외에 어떤 파티도 원래의 입력을 보지 못한다.

사용자 정의 SMC 시스템은 다음 매개 변수에 따라 다를 수 있다.

- **기본적인 작업.** 이것들은 계산을 정의하는 데 사용되는 작업이다. SMC 시스템에는 산술 연산 또는 부울 연산 기능이 있다.
  - **산술 연산**을 사용하면 통계 분석을 표현할 때 더 편리하다.
  - **부울 연산**은 패턴 매칭 시 더 효율적이다.
- **암호화 우선 순위.** SMC 시스템은 다음 암호화 작업 중 하나, 하나 이상을 사용한다.
  - **비밀 공유**:1 개의 데이터를 원래의 데이터에 대한 정보를 제공하지 않는 부분으로 분할하는 기술. 비밀 공유는 SMC 시스템에서 매우 일반적으로 사용된다.
  - **명확한 이전**: 보내는 사람이 여러 데이터 중 하나를 보내지만 어떤 데이터인지 모르는 데이터 전송을 위한 프로토콜의 클래스.
  - 동질적인 암호화: 암호문을 만들기 위한 일종의 계획.
- **신뢰 모델**
  - **자기 신뢰**: 파티는 자신만 믿을 수 있다고 가정한다.
  - **정직한 대다수**: 파티는 다수의 파티들이 정직하다는 것이라고 믿어야 한다.

이러한 파라미터를 서로 다르게 조합하면 다음과 같은 다양한 속성이 생성된다.

- **결함 허용**: 신뢰 환경에서, 모든 파티가 계산을 진행하는 데 필요하며, 파티 중 한 파티도 참여할 수 없거나 참여하고 싶어 하지 않는다면 시스템이 실패할 것이다. 반면에 시스템이 단지 과반수

이상의 정직한 존재에만 의존한다면, 어떤 파티들이 그들의 의무를 수행하는데 실패하더라도 그 시스템은 완성으로 이어질 수 있다.

- **보안**
  - **패시브 보안**: 모든 컴퓨터 관련 파티들이 프로토콜을 따르는 한, 파티들은 컴퓨터 출력 외에는 아무것도 배우지 못한다. 세미 호스트 보안이라고도 한다.
  - **에크티브 보안**: 의도적으로 의정서에서 이탈하려고 하는 악의적인 파티들이 있는 경우에도, 파티들 중 어느 누구도 계산의 결과 외에는 아무것도 배우지 못한다.
  - **코베르 보안**: 그 시스템은 정당이 악의적인 행동을 할 확률이 50%라는 것을 알아낼 수 있고--의심할 만큼 높은--처벌 조치를 취할 수 있다.
- **실적**. 에크티브 보안은 패시브 보안보다 훨씬 덜 성능이 뛰어난 경우가 많다. 코베르는 에크티브과 유사한 보증을 제공하지만 훨씬 더 성능이 뛰어나다.

기술의 특성 때문에, 맞춤형 시스템은 허용 가능한 수준의 성능을 달성하기 위해 필요하다. Partisia 는 2008 년부터 사용자 정의 SMC 시스템을 개발하고 있으며, 필요한 보안 및 성능을 보장하는 사용자 정의 SMC 시스템의 설계 및 구현과 관련하여 통찰 네트워크를 지원한다. 특히, 이 시스템은 최초로 블록체인과 접촉한 SMC 시스템 중 하나가 될 것이다.

4.2.2 통찰 네트워크의 SMC 솔루션

SMC 은 Insights Network(통찰력 네트워크) 솔루션에서 다음과 같은 기술적 문제를 해결하는 데 사용된다. SMC 기반 인증과 SMC 기반 인증을 기반으로 하는 프로필 일치 및 데이터 지점 검증. 우수한 성능을 위해 이러한 각 사용 사례에 맞는 맞춤형 프로토콜을 설계했다.

이 SMC 기반 인증에서는 컴퓨팅이 정품의 디지털 검증(Digital Proof of Authenticity)을 생성한다. 이는 인증서로 간주할 수 있으며 공급 업체, 통찰 네트워크 및 검증 파트너가 수행한다. 이 인증서는 제공자의 EOS 계정 이름, 기본적인 인구 통계 세부 정보를 포함하며, Insights Network 에 의해 서명된다. 더 확실한 것은 제공자의 진실성이다. 즉, 파트너가 더 높은 품질의 검증을 제공할 수록, 공급 업체가 제공하는 기본적인 인구 통계적 세부 사항을 더 많이 제공할 수록 더 많은 비용을 지불하게 된다.

SMC 은 다음과 같은 입력을 수신하며, 이는 원래 소유자 이외의 모든 계산 참가자가 알 수 없는 정보이다.

- Insights 는 정품의 디지털 증명에 서명하는 데 사용되는 개인 키를 제공한다.
- 공급자는 자신의 EOS 계정 이름을 제공한다. 이 이름은 디지털 정품 인증 센터에 포함될 예정이다. 인증서에 포함하고 싶어 하는 인구 통계학적 세부 사항도 포함되어 있다.
- 각각의 검증 파트너는 제공 업체의 EOS 계정 이름으로 제공되며 기본적인 인구 통계적 세부 정보를 제공한다.

계산을 하는 동안, 제공자의 신원이 확인되고 기본적인 인구 통계학적 세부 사항이 비교 검토된다. 성공한다면, 요청자는 향후 거래에서 자신의 진실성을 입증하는 데 사용할 수 있는 인증서를 얻게 된다.

SMC 기반 프로필 일치 및 데이터 지점 검증의 경우, 요청자와 공급자 간에 비밀 보안이 적용되는 두 그룹의 SMC 프로토콜을 사용한다. 코베르 보안이란 파티 사기를 칠 확률이 50%라는 것을 입증할

수 있는, 에트티브 보안의 편안한 버전을 말한다. 부정 행위는 그 블록체인에게 부정 행위의 증거를 출판함으로써 처벌 받고 단념할 수 있다. 완전한 에크티브 보안이 아닌 코베르 보안 기능을 사용하면 악의적인 행동을 방지하는 동시에 사용자 환경을 개선하는 데 중요한 훨씬 더 강력한 솔루션을 제공할 수 있다.

우리가 고려해야 할 점은 Insights 공급자 클라이언트가 네트워크 연결 및 컴퓨팅 성능이 제한된 노트북이나 핸드폰에서 실행되고 있을 수 있다는 점이다. 우리가 설계한 SMC 프로토콜은 다음과 같은 속성을 사용하여 이러한 제한 사항을 해결한다.
●최소 여행: 요청자와 공급자 간의 커뮤니케이션은 2 번만 이루어지므로 네트워크 지연 시간과 연결 불량이 최소화된다.
●비대칭 계산: 요청자는 해당 공급 업체의 컴퓨터나 모바일 기기가 과부하 되지 않도록 대부분의 작업을 수행한다.

마지막으로, 표준 암호화 방식을 사용하면 나중에 향상된 처리 능력을 활용하여 폭력을 사용하여 블록체인에 저장된 암호화된 데이터를 크래킹 할 수도 있다. 반면, 우리의 시스템은 정보-이론적으로 보안이 되는 암호화를 사용하는데, 이는 공격자가 시간과 컴퓨팅 자원을 무제한으로 가지고 있어도 해결할 수 없는 것이다. 따라서, 우리의 시스템에서는, 현재와 미래에 오직 요청자가 구매하는 데이터를 해독할 수 있다.

4.3 기술적 문제 해결

4.3.1 진실성 증명

공급자들은 통찰 네트워크에 참여하는 동안 그들의 익명성을 유지한다. 그러나 요청자는 익명이지만 자신의 데이터 요청을 이행하는 제공자가 진실한 대답을 기대하고 있는 실제 사람이라는 사실을 알아야 한다. 이것은 제공자가 이러한 확신을 제공하는 과정이다.

우리의 시스템은 한 제공자의 신원을 확인하기 위해서 여러 파티들의 정보를 사용한다. 예를 들어, 한 파티가 공급자의 고용주일 수 있다. 다른 파티는 제공자의 국가가 제공한 신원 확인 문서를 가져가서 이를 검증할 수 있다.

우리는 이 파티들을 검증 파트너라고 부른다. 공급자가 검증을 통과하면 시스템은 Insights Network 에서 서명한 신뢰성 디지털 검증 자료를 발행하여 요청하는 사람이 액세스 할 수 있는 블록체인에 게시한다. 신뢰성에 대한 디지털 증거는 요구자와 제공자가 통신하는 ‘피어 투 피어’ 프로토콜에서 엔드 식별자로 사용되는. 공급자의 블록체인 계정 이름을 포함하는 디지털 문서이다. 이는 TLS 인증서와 기능이 비슷하다. 우리의 시스템은 SMC 을 사용하여 각 파티가 다른 파티에게 정보를 공개하지 않고 검증 프로세스에 대한 입력으로 보유한 정보를 제공할 수 있도록 설계되었다.

신원 확인과 관련하여, 입력 사항은 검증 파트너가 보유하고 있는 비밀 정보이며, 수행할 계산은 그 정보를 검증하고 진실성의 디지털 증거를 생성하는 것이다. SMC 컴퓨팅 파티가 하위 컴퓨팅 작업을 마치면 중간 결과를 Insights Network 가 서명한 디지털 신뢰성 입증 자료로 결합한 후공급자에게 보낸다.

Insights Network 는 서브 컴퓨팅에 할당되어 있지 않지만, 신뢰성이 입증된 디지털 서명을 생성하는 데 사용되는 입력으로 전용 키를 제공한다.

info@insights.network

4.3.2 데이터 요청 제출

소액의 비용으로 요청자는 Insights 스마트 계약에 데이터 요청을 보낼 수 있다. 이 요청서에는 제공자들이 작성하기 위한 조사, 대상 모집단을 설명하는 형식 및 유효 데이터 점에 대한 비용이 포함될 것이다. 또한 이 요청서에는 유효한 데이터 포인트를 제출한 유자격 공급자에게 지불하는 스마트 계약을 위해 제 3 자에 의해 제 3 자에게 예탁되는 토큰이 포함된다. 보안을 강화하기 위해, 많은 토큰이 포함될 수 있기 때문에 요청자는 블록체인 운영 체제의 사용 권한 시스템을 사용하여 조직의 여러 파티가 각 요청을 승인하도록 규정할 수 있다. 요청자가 자신이 받은 데이터 포인트에 만족하면, 요청자는 데이터 요청을 종료할. 수 있으며, 제 3 자 예탁에 남아 있는 토큰은 요청자의 계정으로 반환된다.

4.3.3 데이터 요청 이행

공급자에서 정기적으로 사용하는 Insights Network 클라이언트는 Insights Network 스마트 계약을 확인하여 열려 있는 데이터 요청이 있는지 확인한다. 이들을 로컬로 다운로드하고 제공자의 프로필을 사용하여 제공자에게 표시할 것을 선택한다. 이 섹션에서는 공급자가 데이터 요청에 대한 데이터 지점을 제출하는 프로세스를 설명한다.

제공자는 데이터 요청을 선택하고 해당하는 설문 조사를 작성하여 데이터 지점을 생성한다. 그리고 나서 데이터 포인트를 제출하는데 관심이 있다는 것을 나타내기 위해 데이터 요청 ID 와 함께, 인증서를 요청자에게 보낸다. 요청자는 Insights Network 의 공용 키를 사용하여 인증서가 유효한지 확인하고 제공자 이름이 인증서의 계정 이름과 일치하는지 확인한다. 이러한 체크 아웃하면 요청자가 나중에 데이터 포인트를 암호화하고(암호 해독과 함께)공급자를 사용하여 시큐어 멀티파티 계산 기능을 시작할 수 있는 비밀 키를 생성한다.

양쪽 파티는 계산에 입력 정보를 제공하며, 이는 프로토콜이 상대방에게 노출되지 못하게 한다. 제공자는 자신의 프로필과 자신이 만든 데이터 포인트를 제공한다. 요청자는 이 특정 제출 자료를 위해 생성하고 나중에 사용하기 위해 저장하는 프로파일 패턴, 데이터 형식 및 비밀 키를 제공한다.

양쪽 파티가 공동으로 수행하는 계산은 데이터 점이 데이터 형식에 맞는지 확인하고 비밀 키를 사용하여 데이터 점을 암호화하는 작업으로 구성된다. 서브 컴퓨팅 이 계산에서 도출되며, 이를 수행하고 결과를 최종 결과로 조립하기 위한 스마트 계약에 전송하는 두 파티에게 할당된다. 최종 결과가 빈 값이 아닌 암호화된 데이터 포인트인 경우에는

데이터 요청 조건에 따라 스마트 계약이 제공자에게 권한을 부여 받은 토큰을 전송한다. 그렇지 않으면 데이터 지점이 유효하지 않게 되고, 등급이 낮아진다.

특히, 우리 시스템에 사용되는 암호화 방식은 정보화에 있어 매우 안전하다. 즉, 공격자가 무제한적인 컴퓨팅 성능과 시간을 가졌더라도, 그는 데이터 포인트를 차단할 수 없을 것이다. 이는 곧 누군가가 10 년 후에 자원이 개선되어 순수한 암호화 방식으로 취약해 질 것을 우려할 필요 없이 블록체인에 암호화된 데이터 포인트를 저장할 수 있다는 것이다.

4.3.4 프로필 일치

제공자의 프로필이 요청자가 제공하는 패턴과 일치하는 경우에만 데이터 포인트를 제출할 수 있다. 이것이 이행될 수 있는 한가지 방법은 제공자가 자신의 프로필을 베팅 하기 위해 요청자에게 보내는 것이다. 그러나 이는 프라이버시 침해가 될 수 있는데, 이는 프로파일에 제공자가 공개를 꺼리는

정보가 포함될 수 있기 때문이다. 어쨌든, 요청자들이 프로파일이 무엇인지 알아야 하는 범위는 그들이 찾고 있는 패턴과 일치하는지 여부이다. 그들은 실제로 프로파일의 정확한 내용을 알 필요가 없다. 예를 들어 요청자는 해당 제공자의 나이가 25 세가 아니라 21 세에서 30 세라는 사실만 알아야 할 수 있다.

4.3.3 섹션에서 설명하는 것처럼, 시스템에서 프로파일 매칭 (일치)는 시큐어 멀티파티 계산에서 수행된다. 제공자는 SMC 에 대한 입력 정보로 프로필을 제공하며, 이러한 정보는 프로토콜을 통해 요청자에게 절대 노출되지 않는다.

4.3.5 검증된 데이터의 안전한 교환

요청자와 제공자를 고려한다. 요청자는 해당 데이터가 특정 요구 사항을 충족하는 경우 제공 업체로부터 데이터를 구매할 용의가 있다. 그러나 제공자는 지불을 받기 전에 요청자가 데이터를 보도록 하지 않는다. 요청자가 데이터를 소유하는 경우에는 비용을 지불하지 않고 데이터를 가질 수 있기 때문이다. 동시에 요청자가 패턴 매칭으로 정의하는 " 좋은 "데이터임을 알지 못하는 한, 요청자는 해당 공급자의 데이터에 대해 비용을 지불하지 않는다.

우리 시스템에서는 데이터 지점이 멀티파티 계산 내에서 검증 및 암호화된다. 제공자와 요청자는 서브-컴퓨팅을 수행하지만, 최종 결과로 함께 분류하는 것이 스마트 계약이다. 유효성이 확인되고 암호화된 데이터 포인트를 요청자에게 제공하는 블록체인에 저장하고, 한번의 트랜잭션으로 제공 업체에 지급을 전송하는 것은 완전히 실패하거나 완전히 성공한다는 이점이 있다.
즉, 유효한 데이터 점이 요청자에게 제공되고 토큰이 제공자에게 전송되지 않거나 둘 다 발생하지 않는다.

4.3.6 보관

Insights Network 를 통과하는 주요 데이터 카테고리는 제공자의 프로필, 제공자의 데이터 포인트 및 제공자의 ID 확인 프로세스 동안 사용되는 정보이다. 프로필은 공급자의 로컬 장치에 저장된다. 데이터 포인트는 원장에 기록되는 Insights Network 스마트 계약 상태에서 암호화된 형식으로 저장된다. 프로필은 사용자 대상 지정에 사용되지만 개인 프로필을 유지한다.

4.3.7 제공자의 인구 통계

공급자들은 그들의 통찰 네트워크 클라이언트에 인구 통계학적 정보를 포함하는 프로필을 보관한다. 프로필의 일부 필드는 성별 및 생년월일과 같이 고정된다. 가정 관계 상태와 같이 변경할 수 있는 것도 있다.

공급자들은 변경할 수 있는 필드를 변경할 수도 있지만, 각 변경 사항은 블록체인에 기록된다. 요청자는 사기를 방지하기 위해 이 정보를 사용할 수 있다. 예를 들어, 요청자는 지난 3 년 동안 가정 관계 3 번 이상 변경한 요청자를 피해야 한다. 또한 요청자가 의심스러운 활동을 발견하는 경우에는 수수료를 지불하고 우리의 양쪽 평가 시스템에 해당 공급자에 플래그를 지정할 수 있다.

5 토큰 경제학

5.1 양측 시장

Insights Network 는 요청자와 제공자 (공급자)라는 두개의 서로 다른 그룹 간에 트랜잭션을 원활하게 처리하는 플랫폼이다. 요청자는 공급자의 정보를 필요로 하며 이를 얻기 위해 기꺼이 비용을 지불할 용의가 있다. 이러한 역동성은 양측 시장으로 알려져 있다.

양측 시장은 시작하기 어렵기로 악명 높다. 요청자가 Insights Network 에 요청을 하는 주된 이유는 이를 이행할 제공자가 있기 때문이다. 이와 동시에, 제공 업체들이 Insights Network 에 참여하는 주된 이유는 돈을 벌기 위한 충분한 요청이 있기 때문이다. 처음에 플랫폼에는 다른 그룹을 끌어들일 만큼 한 그룹이 충분하지 않았다.

시장 개척을 돕기 위해, 우리는 INSTAR 라는 새로운 ERC-20 토큰을 사용하고 있다. INSTAR 토큰의 보유자는 데이터 요청을 저장하거나 이를 원하는 사람에게 판매할 수 있을 것이다.

공급자들은 미래의 요청자들에게 지불하는 토큰을 판매하고, 보상 스토어에서 항공사 마일이나 브랜드 기프트 카드와 같은 용도로 현금화하여 다른 사용자에게 보낼 수 있게 된다. 공급자들이 통찰 네트워크에 참여함에 따라, 더 많은 요청자들이 참여하고 데이터 요청을 하게 될 것이며, 이는 더 많은 공급 업체들을 끌어들일 것이다. 이는 네트워크 효과로 알려져 있으며, 이로 인해 네트워크가 매우 커질 수 있다.

5.2 토큰 분포

토큰은 다음과 같은 방법으로 배포된다. INSTARTokens 의 총 공급량: 300MM
●토큰의 5%는 사전 판매 방식으로 토큰 판매에 따라 할인된 가격으로 판매된다.
●토큰의 35%가 토큰 판매를 통해 판매된다.
●토큰의 30%는 에코 시스템에 사용된다.
● 토큰의 30%는 회사에 의해 팀, 고문, 운영, 미래의 엔지니어링 직원, R&D 를 위해 예약될 것이다.

초기 사용자들이 그들의 프로필을 작성하기 위한 지불로 사용될 환경에 사용될 9 천만개의 토큰이 발행될 예정이고 Insights Network 와 초기 파트너들에 의해 수행되는 시장 조사에 참여하게 된다. 에코 시스템 분야의 핵심 기술을 얼리 어답터들에게 제시함으로써, 우리는 수억개의 데이터 포인트를 만들어 내고 있으며, 이를 통해 요청자가 활용할 수 있는 실용적인 데이터 네트워크를 구축하게 된다. 예를 들어, 각 얼리 어답터가 10 개의 검증된 데이터를 클라이언트로 가져오는 토큰을 받는다면, 이러한 9 천만개의 토큰은 통찰력 네트워크를 위한 9 억개의 데이터 포인트를 생성한다.

설립자, 직원 및 자문을 포함한 Insights Network 팀이 이 회사를 보상금으로 사용하도록 하여, 이들 팀이 시장에서 제공하는 통찰력 서비스에 대한 수요를 증가시킨다.

참고로, Insights Network Desktop Client 의 베타 테스트 중에 EOS 플랫폼이 완전히 작동하고 공개적으로 사용될 때까지 Insights ERC-20 토큰이 사용되며, 이 시점에서 해당하는 INSTAR 토큰 소유자가 스왑 하기 위한 1 회 마이그레이션 토큰이 제공된다.

토큰 판매 캡 - 25,000 ETH.

info@insights.network

5.3 자금 사용

개발 - 50%
운영 - 25%
마케팅 - 15%
합법 - 10%

6 팀

브라이언 갤러거 - W.P. 캐리 경영 대학원 , Y-조합원
다윈 로우 - 스탠포드 컴퓨터 과학, Y-조합원
브란단 자우차- W.P. 캐리 경영 대학원 , Y-조합원
딜란 허먼 - 일리노이 대학교, 엔지니어링
디노 아마랄 - Ph.D. 암호 법

빅 데이터에 대한 열정이 있고, 컴퓨터 과학자이며, 신생 기업을 사랑한다면 저희에게 연락 주시기 바란다: team@insights.network

6.1 어드바이저

커트 닐슨
제스퍼 부스 닐슨
피터 프란츠 프란슨
앤드루 로즈너
제이슨 햄린
데이비드 고보

6.2 파트너

파르티시아는 SMC 의 상용 구현 분야의 선구자이다. SMC 의 최초의 대규모 상업용 용도는 2008 년 파르티시아가 프로덕션 계약을 위해 기존 경매 방식의 경매인을 교체하면서 처음으로 사용한 것이다. 다른 주요한 성과로는, SMC 을 사용하여 ‘신뢰할 수 없는’키 관리를 위한 순수한 클라우드 솔루션을 제공하는 Sepior 라는 스핀 아웃과,

연결되지 않는 통계 자료를 제공하는 Secata 와 같은 스핀 아웃 분석이 있다.

7 로드맵 초안

통찰력:Q1-Q3 2017
- ●개념 증명
- ●통찰 네트워크 시작 웹 사이트
- ●EOS 테스트 네트워크에 대한 개발 작업 개시

통찰력: Q4 2017
- ●SMC 을 포함하도록 업데이트된 백서
- ●토큰 사전 판매
- ●INSTAR 월렛 통합 감베알 앱

통찰력: Q1 2018
- ●INSTAR 토큰 크라우드세일

통찰력: Q2 2018
- ●시큐어 멀티파티 계산
- ●INSTAR AppClient 베타 ERC-20 토큰을 클라이언트에서 반환 가능

통찰력: Q3 2018
- ●EOS 플랫폼 베타 공개

통찰력: Q4 2018
- ●INSTAR EOS 블록체인 소비자 클라이언트가 완벽하게 작동함

8 결론

데이터 브로커는 허가 없이 개인에 대한 개인 정보를 수집하여 지불 의사가 있는 기관, 심지어 대학, 병원 및 보험 회사를 포함한 생활에 상당한 영향을 끼치는 기관에 이 정보를 판매한다. 이것은 사생활 침해일 뿐만 아니라 감시이다. 소비자들 중에 수수의 사람들이 이런 일이 일어나고 있다는 것을 알고 있어도 이 관행을 멈추기 위해 할 수 있는 것은 거의 없다.

다행히도, 전 세계의 정부들이 데이터 브로커들을 단속하고 있다. 유럽 연합은 기관들이 이른바 '개인 데이터' 를 처리하는 방법을 규제하는 '일반 데이터 보호 법'을 제정했다. 브라질은 개인 식별 가능 정보를 포함한 데이터를 다른 파티에게 전송하는 것을 금지하고 있다. 미국에서 상원 의원 에드워드 마키(Senator Edward Markey)는 2017 년부터 데이터 브로커의 회계 감사 및 투명성에 관한 법률이라는 법안을 후원하고 있다.

우리는 민감한 개인 정보를 다루는 데 있어 더 높은 기준을 요구하는 규정을 촉진하기 위해 노력할 것이다. 하지만 규제가 없어도 당사의 솔루션은 기존 데이터 브로커에 비해 우수하며, 우수한 정보를 제공하고 소비자가 자신의 데이터를 제어할 수 있도록 함으로써 무료 시장 경쟁에서 이길 것이다.

info@insights.network

우리는 10 년에서 20 년 내에 분산된 기술의 성장으로 인해 매개체가 없을 것이라고 예측한다. 기업들은 소비자들의 데이터를 직접 처리하기 위해 우리의 플랫폼을 사용할 것이다. 현재 기업들은 이 데이터를 위해 매년 2 천억달러를 지불하고 있다. 포브스는 이 수치가 늘어날 것이라고 예측한다. 우리는 통찰 네트워크가 이러한 수요를 충족시키고 Acxiom 과 같은 중간 계층의 사람들로부터 데이터의 정당한 소유자인 소비자로 가는 제어와 이익을 전환하기 위해 성장할 것이라고 생각한다.

9 출처

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)
7. Bogetoft P, Christensen DL, Damgaard IB, Geisler M, Jakobsen T, Kroejgaard M, Nielsen JD, Nielsen, JB, Nielsen K, Pagter J, Schwartzbach MI and Toft T (2009) Secure multiparty computation goes live, Lecture Notes in Computer Science, vol 5628, pp. 325–343.
8. Chaum D, Crepeau C, and Damgaard IB. (1988) Multiparty unconditionally secure protocols (extended abstract). In 20th ACM STOC, Chicago, Illinois, USA,May 24, 1988, ACM Press, pp. 11–19.
9. Shamir A (1979) How to share a secret, in Communications of the ACM 22, 11, pp. 612–613.
10. Pinkas B, Schneider T, Smart NP and Williams SC (2009) Secure Two-Party Computation Is Practical. Asiacrypt 2009.
11. Shelat A and Shen C (2011) Two-output Secure Computation With Malicious Adversaries. EUROCRYPT 2011.

info@insights.network

12. Nielsen JB, Nordholt PS, Orlandi C and Burra SS (2012): A New Approach to Practical Active-Secure Two-Party Computation. CRYPTO 2012.
13. Frederiksen TK and Nielsen JB (2013) Fast and Maliciously Secure Two-Party Computation Using the GPU. ACNS 2013.
14. Frederiksen TK and Nielsen JB (2014) Faster Maliciously Secure Two-Party Computation Using the GPU. SCN 2014.
15. Lindell Y and Riva B (2015) Blazing Fast 2PC in the Offline/Online Setting with Security for Malicious Adversaries. CCS 2015.
16. Nielsen BN, Schneider T and Trifiletti R (2017) Constant Round Maliciously Secure 2PC with Function-independent Preprocessing using LEGO. NDSS 2017.