IoT Chain

IoT 보안 Lite 운영체제

White Paper

목차

1 장 프로젝트 배경

1. IoT 란 무엇인가?

IoT(사물 인터넷)란 인터넷,기존의 통신망,그리고 여타 다른 형태의 정보 전달 방식들을 기반으로 한 각자 독립적인 위치에 있는 각종 사물 간의 상호 접속을 가능하게 해주는 네트워크를 일컫는다.IoT 에게는 3 가지 주요 특징이 있는데 이는 일반적인 사물들의 균등화, 자동 관리 단말의 상호 연결,그리고 보편적인 서비스의 지성화이다.IoT 를 통해서 모든사물들은 정보 교환과 통신을 위해 인터넷에 연결될 수 있고 이는스마트 인식,위치 확인,추적,감시및 관리를 가능하게 한다.

IoT 에는 두 가지 함축된사실이 있다.첫째,인터넷은 여전히 IoT 의 중심이자 기반이며 IoT 는 기존의인터넷에서 더욱 확장해 나간 것이다.둘째, IoT 의 사용자측은 모든 사물들의 정보교환과 통신으로 확장해 나아갔으며 이는사물대 사물의 상호 연결성(thing to thing interconnectivity)이라 불린다. IoT 는 통신 지각 기술 수단으로 융합 통신망에널리 적용되어 있으며 예로 스마트 지각,인지,그리고 퍼베이시브 컴퓨팅(Pervasive Computing, 유비쿼터스와 비슷한 개념) 등이 있다.그러므로,IoT 는 컴퓨터와 인터넷을 잇는 세계 정보 산업 발전의 제 3 의물결이라고 불리고 있다.IoT 는 인터넷으로부터 확장되어 나온 개념이기에, 네트워크보다는 하나의 사업이나 응용물로 언급되어야 한다.따라서,여러 응용의 혁신은 IoT 개발의 핵심이며 사용자경험 중심의 창조물은 IoT 의 영혼에 해당한다고 볼 수 있다.

2. IoT 의 시장 규모

2009 년에 미국, 유럽,그리고 중국에 의해서 IoT 개발 정책들이 발표되고 난 이후로, IoT 는 빠른 속도로 개발되어 왔다.기존 기업들과 IT 거물들은 모두 IoT 의 물결에 참여하기 위해 노력했으며 이는 제조업,소매업,서비스업 과 공공 사업 등 많은 분야에 영향을 주었다.오늘날, IoT 는 더욱 거대한규모로 폭발적인 성장을 앞두고 있다. Wulian Zhongguo 의 2016 *China IoT's Market Scale and Development Trend*(2016 년 중국 IoT 시장 규모와 개발 트렌드)에 따르면 세계의 IoT 시장은 2016 년에 약 624 억 달러의 규모에 도달했으며, 이는 전년대비 29%의 성장인 것으로 나타난다.이 수치는 2018 년에 약 1036 억 달러에 도달할 것으로 보여진다. 2013 년부터 2018 년 까지의 연간성장률은 21%가 될 것이고 새롭게 늘어나는 IoT 기기의 수 또한 2015 년의 약 16.91 억개에서 2019 년에는 약 30.54 억개까지 늘어날 것으로 전망된다. (Figure1 참고)

Figure1: 2013-2018 세계 IoT 시장 규모와 성장률

더욱 많은 사물들과 기기들이 IoT 에 연결되고 있다. Gartner 에 따르면 전 세계의 인구가 75 억임에도 불구하고 전 세계의 IoT 기기의 수는 2016 년부터 2017 년까지 64 억개에서 84 억개로 무려 31%의 성장률로 늘어날 것이라고 한다.2018 년에는 IoT 기기의 수가 전체 PC, 태블릿 PC, 그리고 스마트폰의총합산된 수를 넘어설 것이며 2020 년에는 약 204 억 개에 도달 할

것이라고 전망한다. (Figure2 참고)

Figure 2: 2014-2016 세계 IoT 시장 규모와 성장률

IHS Markit 에 따르면 2025 년에는 대부분의 사물들이 지능화 될 것이라고 한다.미래에는 컵에서 집까지 모든 것들이 서로 연결되고 IoT 는 우리 삶의 모든 면면에 퍼질 것으로 예측되고있다. (Figure 3 참고)

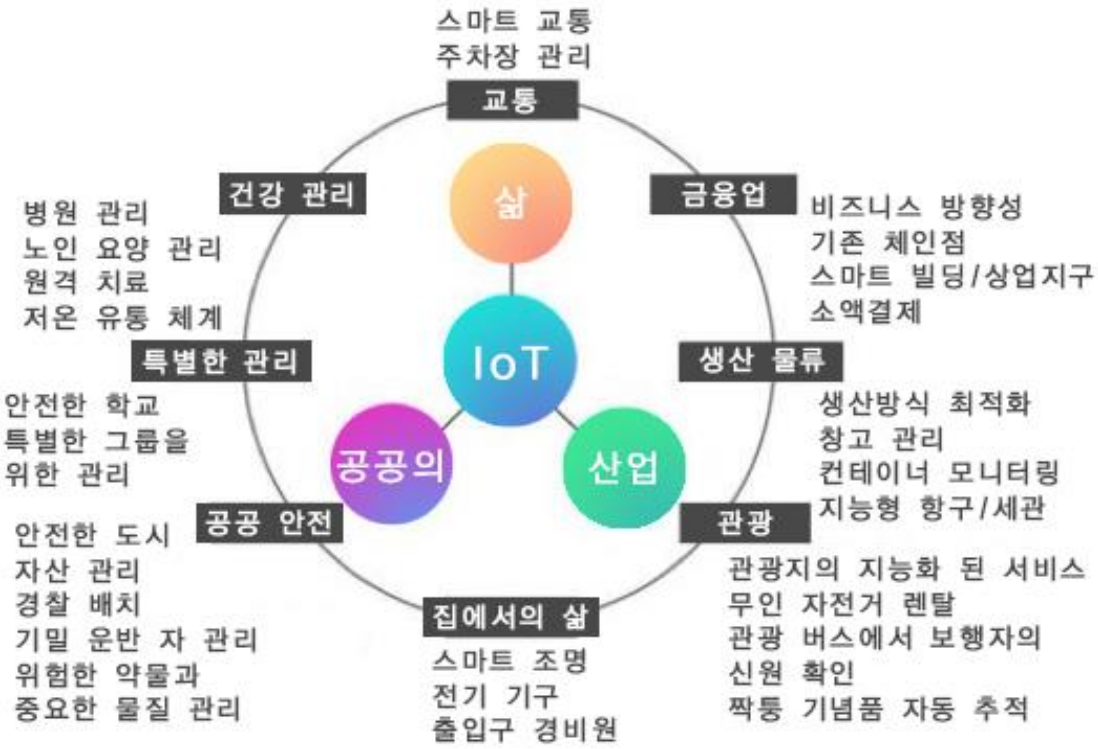

Figure 3: IoT 의 응용 분야

IoT 기술이 적용된 제품과 서비스에 대한 지출은 2016 년에 약 1200 억 달러에 도달했다. 이는 16%의 연간 성장률을 가지고 2021 년에는 약 2530 억 달러에 도달할 것이며,동시에순수 IoT 기술 서비스에 대한 지출은 연간 성장률 17%로 약 1430 억 달러에 이를 것이다.연간 성장률을 20%로 가정하고 보았을 때, 아시아는 세계에서 가장 빠른 성장세를 보일 것이며 2021 년에는 전 세계 IoT 지출의 약 35%를 차지하게 될 것으로 전망된다.

3. 문제점

문제점 1: 기존의공격방식으로도 충분히 IoT 기기들에 심각한 손상을 줄 수 있다.

[문제점]Mirai 에 의해 개발된 The Botnets of Things(사물의 봇넷)는 *MIT Technology Review* 에 의해서 2017 년의 10 가지 획기적인 기술 중 하나로 선정되었다. 통계에 따르면, The Botnets of Things 는 카메라 등의 2 백만개 이상의 IoT 기기들을 감염 시켰다.이를 통한 DDos(디도스)공격은 미국의 DNS 서버 제공자인 Dyn 을 다운 시켰으며, 사용자들의트위터나

페이팔과 같은 유명한 사이트들에 대한 접속이 잠시 제한되었다.이후에 더욱 많은 봇넷이 등장하였고 그 중에는 비트코인을 채굴하기 위해 IoT 기기들을 이용한 것도 있었으며, 더욱 큰 규모로 훨씬 더 활동성을띄는 http81 등이 있었다.

중앙집중식 관리 구조는 완벽하게 믿을 수 없고 개인적인 정보의 유출은 계속해서 빈번하게 일어나고있다.예를 들면, 2017 년 5 월에 People's Daily Online 은 청두 시의 카메라 중 266 개가 인터넷 방송을 위해 침범되어 강제로 사용된 적이 있다고 발표했다.

현재의 클로즈드 소스(Closed Source)를 바탕으로 한 보안 모델은 (흔히 "은닉을 통한 보안, security through obscurity"이라고 불린다)이미 잠재적인 보안 위험성을 노출 했기에 조만간 폐기되고 새로운 보안 모델인 "공개를 통한 보안, security through publicity"으로 대체 될 것으로 보인다.이를 실현하기 위해서는 현재의 모델을 오픈 소스(Open Source) 소프트웨어로 업그레이드 해야 한다.비록 현재의 오픈 소스 소프트웨어 시스템이사고에 취약하고 가용성도 낮을지라도,정부의 간섭과 다른 공격들을 받는 경향은 적다.그러므로,오픈 소스 시스템은 스마트 홈 시스템과차량및 기타 장치들의 네트워킹에 있어서 큰 역할을 할 것이다.

[해결방안]IoT Chain (ITC)은 비대칭 암호화를 도입하였기에 보안 키가 안전하게 보관되는 이상, 데이터가아무리 수집되더라도 해킹 당하지 않는다.동시에 ITC 의 모든 노드들은 동일하기 때문에 사용자들의 개인 정보를 안전하게 지켜준다.더 나아가,블록 체인은 조작이 불가능하다는 특성을 지니기에 제조사와 서비스 제공업체들은 사용자의 정보를 조작할 수 없게 된다.

문제점 2:중앙집중식 구조의 높은 비용

[문제점] IoT 의 매출액이 시장 기대치에 도달하기 이전에,여전히 IoT 의 비용은 매우 높다는 문제가 있다.대부분의 흥미로운 IoT 솔루션은 막대한 금액의 투자를 필요로 한다.서비스 중개자를 위한 수수료외에도 건물 임대료와 중앙집중식 클라우드와 대규모 서버를 위한 인프라 구축 및 유지 비용도 매우 비싸다.

안타깝게도,현재의 IoT 솔루션으로 제공되는 서비스는 소비자의 요구를 만족시키지 못한다.과거에는 IT 업계에서 생겨나는 비용과 이윤이 늘 일정했다.커다란 서버는 긴 수명을 지니고 제조사와 구매자가 신청 계약서를 작성하여 장기간의 서비스를 받을 수 있었다.개인 컴퓨터와 스마트폰에서는 비록 고수익의 지원 약정이 없지만 사용기간이 짧기에 크게 문제되지 않았다.

하지만 IoT 의 경우에는장비 제조업체에서 장비를 장기간으로 지원해주고 유지시켜 주기 위한 비용을 들일 만큼의 충분한 수익이 나지 않는다.그 와중에,수천억 개의 스마트 장비들을 유지하는 데에도 천문학적인 비용이 들고 소프트웨어를 배포하고 업데이트하는 중앙집중식 서버의 관리비 d 용만 해도 매우 높다.

6 억명이 사용하는 WeChat 의서버 운영비는 한달에 약 3 억 위안을 넘어섰다.현재 49 억개의 장치가 접속되어 있으며,서버의 연관리비용은 294 억 위안에서 매년 더욱크게 증가하고 있다.

[해결방안]미래의 ITC 는 수만개의 노드를 통해서 블록체인의 분산원장기술과 함께 IoT 의데이터 저장 요구를 완벽하게 충족시킬 수 있을 것이다.또한,블록체인의 비(非)중앙집중화 덕에컴퓨터에 과도한 무리가 가는 것을 걱정하지 않아도 된다.두 기술은 모두 전체적인 IoT 에서의 운영 및 유지 비용을 크게 감소 시켜주었다.

4. 해결방안

(1) 블록체인의 개념

블록체인은 비트코인과 함께 등장한 중요한 개념으로 분산형 데이터베이스라는 본질을 지니고 있다. 좁은 의미에서 보면, 블록체인은 체인-데이터 구조의 방식으로 데이터 블록들이 시간 순서에 따라서 연결되는 형태이다.또한,분산원장식 기술을 지니기에 암호작성술 방식의 보호 아래에서 변조되거나 위조되지 않는다.더욱 크게 보자면,블록체인 기술은 체인-데이터 구조를 통해서 데이터를 구분하거나 저장하고,분산 노드 합의 알고리즘을 통해서 데이터를 생성하고 갱신하며,암호작성술 방식을 사용하여 데이터 송수신과 접속의 안전성을 강조하고, 자동 스크립트 코드로 이루어진 스마트 컨트랙트를 사용해서 데이터를 프로그램하고 관리하는 새로운 분산 기반이자 컴퓨팅 패러다임인 것이다.

조금 더친숙한 방식으로 설명하자면,블록체인 기술은 참여원 모두를부기에 참여시키는 형식이라고 볼수 있다.모든 시스템의 뒤에는 데이터베이스가 존재하며 우리가 데이터베이스를 하나의 커다란장부라고 본다면,부기를 담당 하는 사람이 꽤 중요해진다.현재의 기술적 상황에서는, 시스템을 소유하는 사람을 부기 담당자라고볼 수 있다.예를 들자면, Tencent 는 Wechat 의 부기를 담당하며 Alibaba 는 Taobao 를 담당한다고 볼 수 있다.블록체인 시스템에서는모두가 부기 과정에 참여할 권한을 갖게 된다.일정 기간 동안데이터에 어떠한 변화가 생긴다면,시스템 내에 있는 모두가 부기에 참여할 수 있게 된다.시스템은 가장 빠르고 합당한 사용자를 선택해서 장부에 기록을 시키고 새롭게 갱신된 장부의 사본을 시스템 내의 다른 유저들에게 백업으로서 배분할 것이다.결국엔시스템 내의 모든 사람들이 완벽한 장부를 갖게 되는 것이다.이러한 부기 방식을 블록체인 기술이라고 한다.

(2) 블록체인 기술의 장점

모두가 부기를 담당한다는 아이디어는명확한 강점을 보여준다:

1. 높은 보안성:블록체인의 기본 구조는 기존의 인터넷 공격에 대한 면역을 지닌다.IoT 의 정보 암호화와 보안 통신의 특징은 '공개를 통한 보안'이고,이는 사용자들의 개인 정보를 보호해준다.신원 접속과 다수의 동의에 대한 관리는 오작동하는 노드에 대한 인지를 돕고 악의적인 노드가 네트워크를 파괴하는 것을 막는 것에 도움을 준다.체인 데이터를 기반으로 한 구조는증거로 사용되거나 추적할 수 있는 전자 증거를 만드는 데 도움을 줄 수 있다.

2. 낮은 비용:분산형 구조의 특성인 다수의 "중앙"과중앙집중화의 약화는 중앙집중방식 구조의 관리 비용을 줄여 줄 것이다.

(3) 블록체인 적용에 대한 장벽

객관적으로 말하자면,블록체인은 매우 뚜렷한 장점들을 지님에도 불구하고아직 몇 개의 장벽들이 존재하기에 널리 적용되지 못하고 있다.비트코인을 예시로 들어보자면:

1. 자원 소모량:비트코인의 POW(작업 증명)는 높은 자원 소비량을 지닌 합의 구성방식이다.하지만 부분의 IoT 장치들은 낮은 연산 능력과 네트워크 능력,그리고 짧은 배터리 수명을 문제로 지니고 있다.

2. 데이터 확장:블록체인의 성장에 맞춰서 IoT 장치들은 충분한 저장 공간을 제공할 수 있을까?현재 비트코인은 100 G 의 물리적 저장 공간을 필요로 하며 그 수치는 계속해서 증가하고 있다.만약 블록체인 기술이 더욱 널리 퍼지게 된다면, 그에 상응하는 거대한 저장 공간이 요구 될 것이다.

3. 성능 병목 현상:기존 비트코인 거래의 제한 속도는 초당 7 트랜잭션(tps)이며 블록체인을 읽어 들이고 합의를 확인 하는 데에한 시간 정도가 걸린다.이는 피드백과 경고의 지연으로 이어지고,지연에 민감한 산업 IoT 에서는 활용이 불가능하다.

4. 분할 내성:산업 IoT 에서는 노드가 "항상 온라인"이어야 한다는 점이 강조된다.하지만 일반적인 노드가 네트워크에 계속해서 접속실패 했다가 재 접속하는 행위를 반복하는 일은 늘 일어난다.이러한 현상은많은 네트워크 대역폭을 소모 해야하는 "네트워크 충격"을 주게되고, 심지어는 "네트워크 분할"까지 일어나게 된다.

위에 상술 된 모든 문제들은 블록체인을 소규모로 사용할 때에는 크게 문제되지 않지만, 대규모 적용에 있어서는 골치 아픈 문제가 된다.이러한 문제들을 어떻게 해결할 수 있을까?

2 장 프로젝트 설명

1. 간단한 소개

기존 IoT 구조의 중앙집중형 설계로 인해서 사용자의 행동 데이터는 판매업체가 관리하는 중앙 서버에 저장된다.따라서,사용자의 데이터는 노출되기 쉬운 환경에 있으며 사용자의 사생활 또한 심각한 위협에 직면하게 된다.

블록체인은 분산형 아이디어와 기술들을 제공하였으며 이는 IoT 산업[1]에서 기계들의 셀프 서비스,셀프 관리,셀프 거래와 상호 간의 공유를 위해서 적절하다.하지만 블록체인 기술을 IoT 에 적용시키기 위해서는 합의의 형성이나 빠른소액결제, 그리고 개인 정보의 보호와 같은 여전히 풀어야 할 숙제들이 있다.이러한 문제들을 위해서 IoT 는 자기만의 해결책들을 고안해냈는데 PBFT, SPV, DAG, CPS 클러스터 기술,빅데이터 분석 스마트 계약 ChainCode 등이 해당된다.

ITC 는 PBFT 합의를메인체인으로 채택하고, 높은 성능을 지원하는 DAG 네트워크를 사이드 체인으로 채택하였으며 다중 계층 구조를 사용해서 안전하고 분산형이며 높은 동시 접속률을 감당할 수 있는 IoT 운영체제를 설계하였다.

2. 기술적 구조

(1)PBFT

블록체인의 핵심 문제점 중 하나는 노드 간의 합의를 설정하는 데에 있다.여러 합의 알고리즘들은 각각 다른 성능을 보여준다.ITC 는 PBFT 합의 알고리즘을 적용하여 메인 체인 합의를 설정해 내었다(Figure 4 참고). 실용적 비잔틴 장애 허용(PBFT)은메세지 전달 일관성 기반의 상태 기계 복제 알고리즘이다.[2]. "준비 전","준비",그리고 "확인"의 세 가지 단계를 통해서 이 알고리즘은 활동성과 안전성에 대한 보장을 전제로 (N-1)/3 (N=전체 노드의 개수)의 장애허용도를 제공한다.

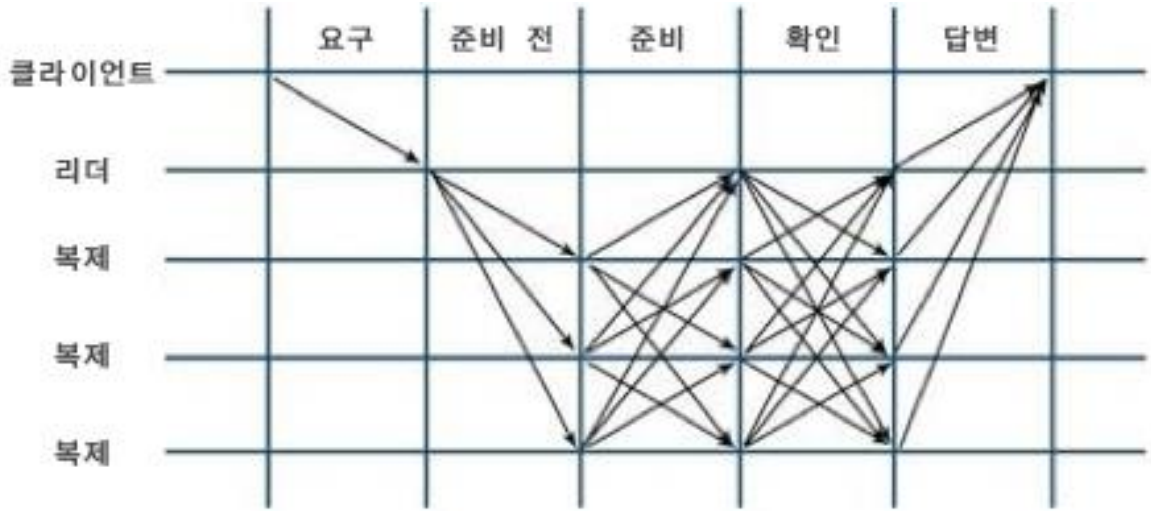

Figure 4: PBFT 알고리즘으로 합의를 찾는 과정

PBFT 알고리즘의 사용은 노드의 확장성에서 약간의 손실을 야기할 수 있지만,확장성과 성능 요구 사항은 가중치를 조정하여 조절할 수 있다.PBFT 합의 알고리즘을 바탕으로 한 블록체인 기술은 중국 중앙 은행의 가상 화폐와 Bumeng 블록체인,그리고 IBM 사의 Hyperledger 에 적용되었다.최근에 HoneyBadgerBFT 합의 프로토콜이 등장했는데, 이를 통해 비동기 BFT 프로토콜이 실현되었다고 한다.

PBFT 합의 알고리즘을 채택함으로, ITC 는 메인 체인 분산화에 대한 합의를 달성한다는 전제하에 메인 체인의 처리 성능을 크게 향상시켰다.

(2) DAG

최근에 비트코인은 SegWit 확장 방식으로 인해서 어려움을 겪었다.블록체인의 연결된 목록 데이터 구조로 인해서비트코인의 거래 성능은 더욱 저하됐고 거래 수수료 또한 점점 높아지고 있다. DAG 는 블록이 없는 분산된 구조이며 무겁게 연계된 블록체인 구조 대신 방향성 비순환 그래프구조를 적용한다[7] (Figure 5 참고). 비트 코인의 가장 긴 체인 합의와 달리, DAG 는 그 것을 가장 무거운 체인 합의 메커니즘(Heaviest-Chain Consensus Mechanism)으로 바꾸고 거래 가중치와 노드들 간의 부분 합의를 통해 새로운 거래를 만들며 각 거래 간의 작업증명을 능숙하게 묶어준다.이 것은 현재 비트코인 채굴이 지니는 중앙집중형 방식의 문제를 해소해줄 뿐만 아니라 거래비용을 낮추어 분산된 네트워크의 처리량도 대폭 향상시켜 주게 된다.이러한 분석을통해서, 우리는 DAG 가 다음 세대 블록체인의 기본 데이터 구조 방식이 될 것이라는 결론에 도달하였다.

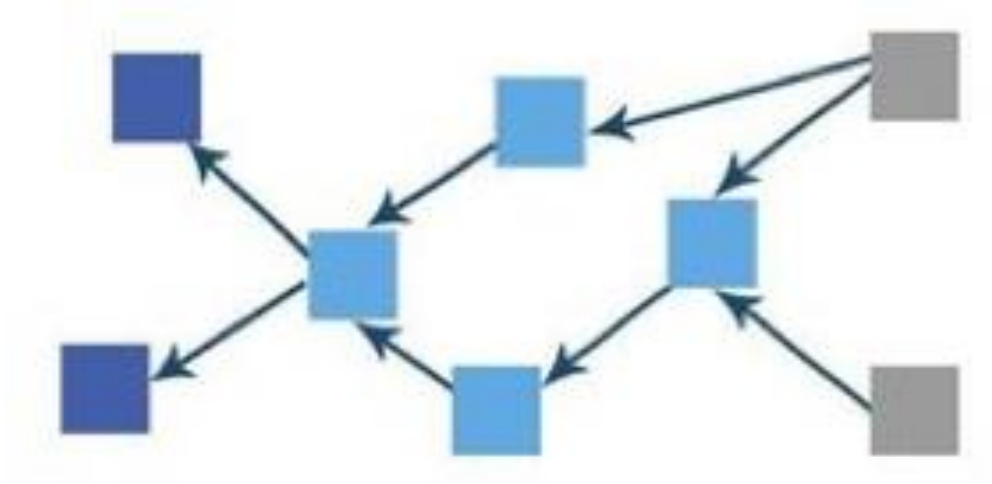

Figure 5: DAG 의위상학적 구조

DAG 네트워크에서 거래를 시작하기위해서는노드가 간단한 작업증명을 하고 여러 개의 증명되지 않은 거래들을 자체적으로 패키징 해야 한다.새로운하위 거래들이 상위 거래들을 증명하게 되면 부분적인 합의가 이루어지게 된다.더욱 많은 노드들이 상위 거래에 연관될수록거래가 증명되기 쉬워진다.이러한 노드들로부터 생성된 모든 거래는 방향성 비순환 그래프구조를 지닌다.새로운 거래의 증명은 이전 거래의 가중치에 의해서 정해진다.노드 선택 알고리즘을 최적화하고 거래 가중치를 설정함으로써 DAG 의 과다 분산과 불법 거래의 해시율 공격을 방지하여 높은 효율성과 체인의 거래 보안성을 보호할 수 있다.ITC 는 DAG 데이터 구조를 채택하여 성능 문제를 해결하였다.한편으로는 거래 성능을 개선할 수 있고 다른 한편으로는 ITC 는 양자 공격에 저항할 수 있다.

DAG 의 꼬여있는(Twisted) 구조는 IoT 의 자연스럽게 메시지 전달 모드에 적용되며 성능의 엄청난 향상과동시에 블록체인의 분산화와 안전성에 대한 요구를 만족시켜주었다.ITC 는 분산 POW 와 POS 아이디어 -서로 다른 IoT 장치의 노드가 요구사항에 따라서 서로 다른 보안 수준을 채택할 수 있다- 를 적용해서 IoT 생태계의 다양한 방면을 만족시켰다.

(3) SPV

SPV (간편 결제 검증)는 블록의 헤더들이 보존되는 한 완벽한 블록체인 정보가 유지되지 않아도 지불 확인을 수행해주는 기술이다.이 기술은 블록체인 결제 확인에 대한 비용을감소시킬 뿐만 아니라 사용자의 부담도 줄여준다. SPV 의 설계 원리는 나카모토의 Bitcoin: A Peer-to-Peer Electronic Cash System[5]에서 처음으로 소개되었다. 비트코인을 예시로 들자면,지불 확인은 노드들이 모든 블록의 헤더들을 보존 시킬 때 이루어진다.그렇지 않다면,결제 확인은 독자적으로

이루어지지 않고 다른 블록체인의 노드들로부터 필요한 결제 정보를 얻어서 거래를 완료하고 전체 블록체인 네트워크로부터 확인된 거래의 수량 정보를 얻어야 한다[6]. (Figure 6 참고)

ITC 의 노드들은 SPV 기술을 사용해서 주 네트워크와 DAG 의 데이터 확장 문제를 해결했다.결제 확인의 효율성을 높이는 것은 전체적인 네트워크의 성능을 보장하기 위한 핵심적인 방법이다.

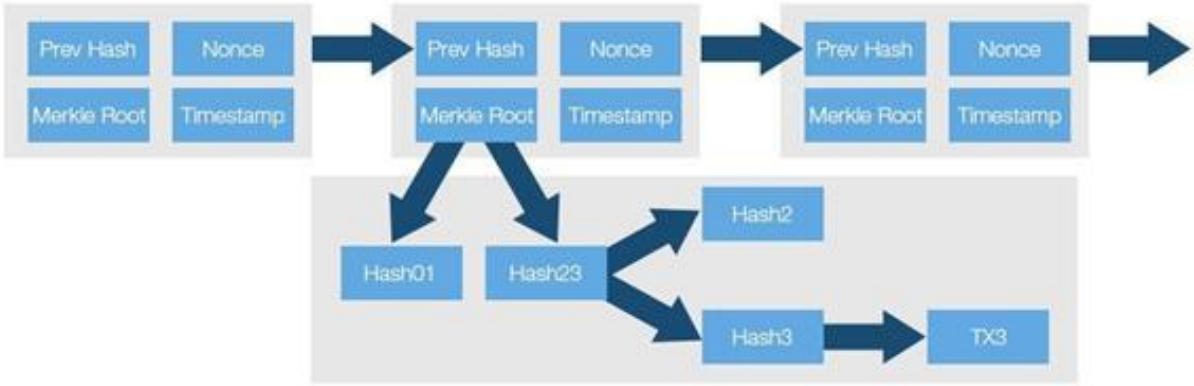

Figure 6: SPV 의 검증 원리

(4) **빅데이터 보안 스마트 분석—스마트 계약 ChainCode**

ITC 는 IoT 의 시대에서 가장 풍부한 데이터 생태계가 될 것이며 스마트폰과 사용자의 행동에 따른 엄청난 양의 데이터를 생산해 낼 것이다.현재,사용자들의 정보는 대기업들에 의해서 독점되고 사용자의 개인정보를 남용하는 기업들에 의해서 광고 제안이나 정보 재판매의 형태로 계속해서 침해당하고 있다.

ITC 에서 사용자의 정보는 그들 자신의 것이다.빅데이터 분석이나 광고 추천 형식의 알고리즘 모델 트레이닝을 시키려는 회사들은 모두 ITC 에게 체인코드를 제출해야 한다.하이퍼로그로그(HyperLogLog) 블룸필터(Bloom Filter)와 영 지식 증명(Zero-Knowledge Proof)과 같은 확률 알고리즘을 사용하여, 우리는 ChainCode 데이터 분석을 위해 필요한 인터페이스를 제공할 수 있다.이러한 인터페이스에 대한 제한과 설정을 통해서 ChainCode 에 제출된 계약들은 사용자의 기존 데이터를 훔치지 못하고 스마트 비즈니스 의사 결정(Smart Business Decision)을 위해 사용된 집계 데이터만을 얻을 수 있다.

ChaiCode 를 실행한 후에,회사들은 데이터를 제공하는 사용자들에게 그 데이터의 가치에 상응하는 ITC 토큰을 지불해야한다.이러한 방식을 통해서,ITC 는 사용자와 기업 모두가 이득을 보는 빅데이터 분석 생태계를 조성하게 된다.

(5) CPS²

만일 기존의 생산 시스템이 지적 물품을 생산하는 스마트 공장으로 바뀌게 된다면,빅데이터 가치 창출 시스템인 "ITC + 지능형 분석 플랫폼"이 필요하게 될 것이다.이러한 요구를 충족시키기 위해서 사이버 물리 시스템(Cyber Physical System)에 중심을 둔 스마트 시스템이 개발되었다.요컨대, CPS 는 빅데이터,네트워크,그리고 대량의 계산을 기반으로 하는 다차원 스마트 기술 시스템이다.지능형 센싱부터분석,채굴,평가,예측,최적화,그리고 협력까지 다양한 주요 기술들을 포함한 CPS 는 계산,통신 및 제어 기능을 통합하여 개체의 메커니즘,환경 및 커뮤니티를 포함한 물리적 공간과 사이버 공간 간의 긴밀한 통합을 실현할 수 있다[8].

ITC 의 구조는 CPS 클러스터를 참고하여 CPS 기술 시스템 구조를 연결,변환,사이버,인식 및 구성으로 이루어진 5 개의 네트워크 단계위에 구축하였다.이러한 시스템 구조에서 네트워크 통신, 데이터 분석및 가치 전송의 플러그형(Pluggable) 독립 블록은 ITC 에서 IoT 의생태계의 안정성을 높이고 이를 더욱 지능적으로 만들어 준다(Figure 7 참고).

Figure 7: CPS 기술 시스템의 대화식 네트워크

결론적으로,노드들에 SPV 기술을 적용시키고,PBFT 합의 알고리즘을 메인 체인에 사용하며, CPS 의 단계별 구조와 DAG 기술과 메인 체인의 독창적인 조합을 생성함으로써 ITC 는 안전성과 분산화라는 전제하에 IoT 의 높은 동시 접속률과 폭발적인 사용 시나리오를 충족시키며 지능형 데이터 분석 API 를 제공하고 사용자와 소비자 모두가 이득을 보는 빅데이터 분석 생태계를 구현해 냈다.

기존의 블록체인과 비교하여서 ITC 는 시스템 구성 및 거래 성능에 있어서 확실한 이점을 보인다 (Chart 1 참고).

	기존의 블록체인	ITC
CPU	Core Duo Quad 2.3 GHz	0.08 GHz
RAM	8 GB	0.002 GB
Hard Disk	1 TB	0.012 GB
거래 확인 속도	비트코인 10 분 이더리움 10 초	밀리초급 (Figure 8,9)

차트 1 ITC 성능 비교 분석

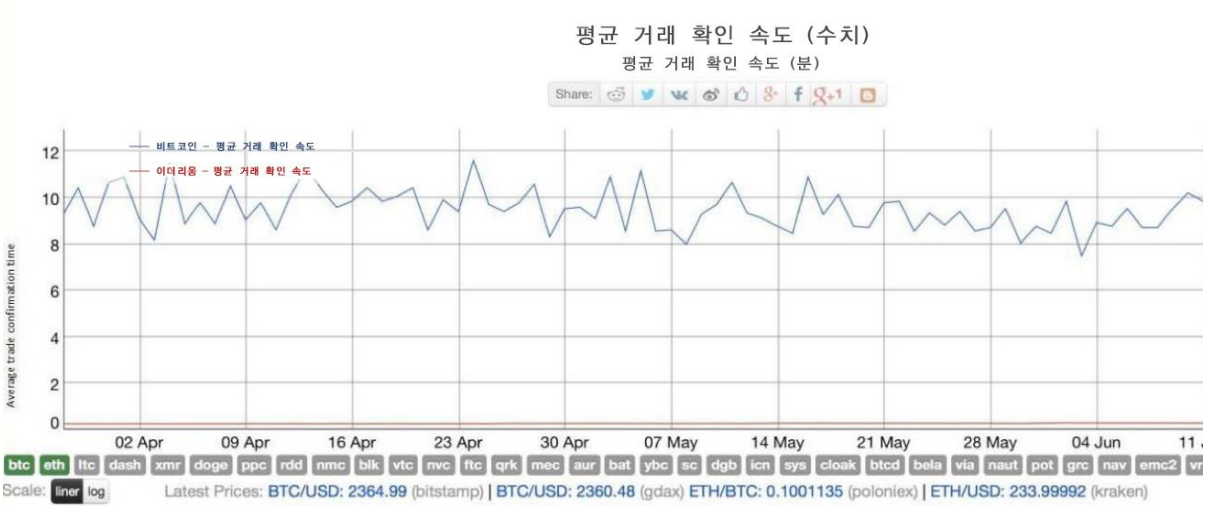

Figure 8: 다양한 기술들 간의 거래 확인 속도 비교

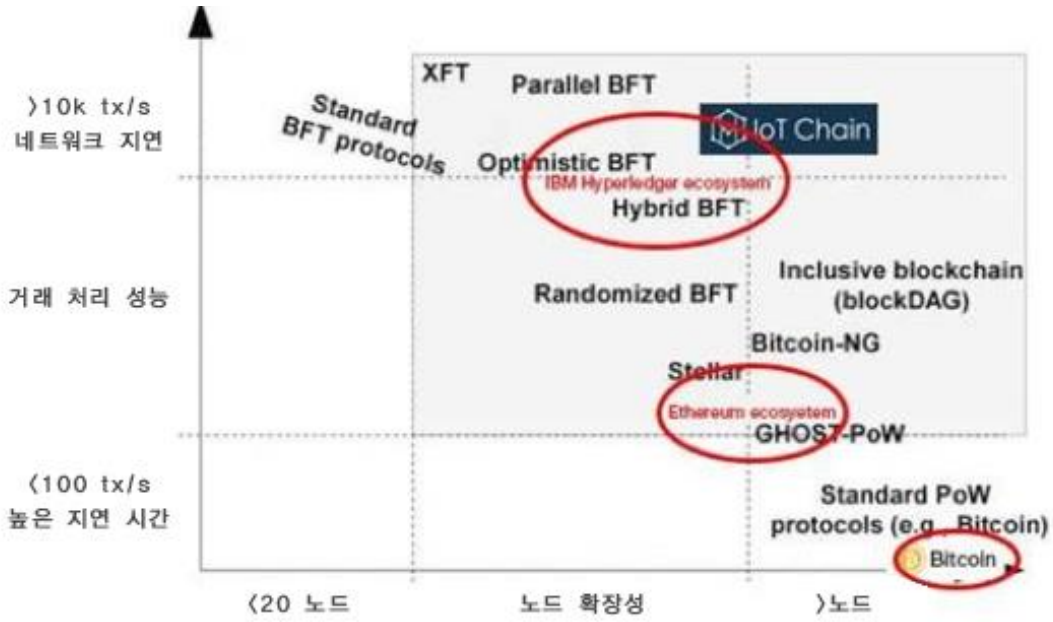

Figure 9: ITC 의 실행 효율에 대한 성능 분석

ITC 는 다음의 플랫폼 구조로 설계되어 있다.(Figure 10 참고)

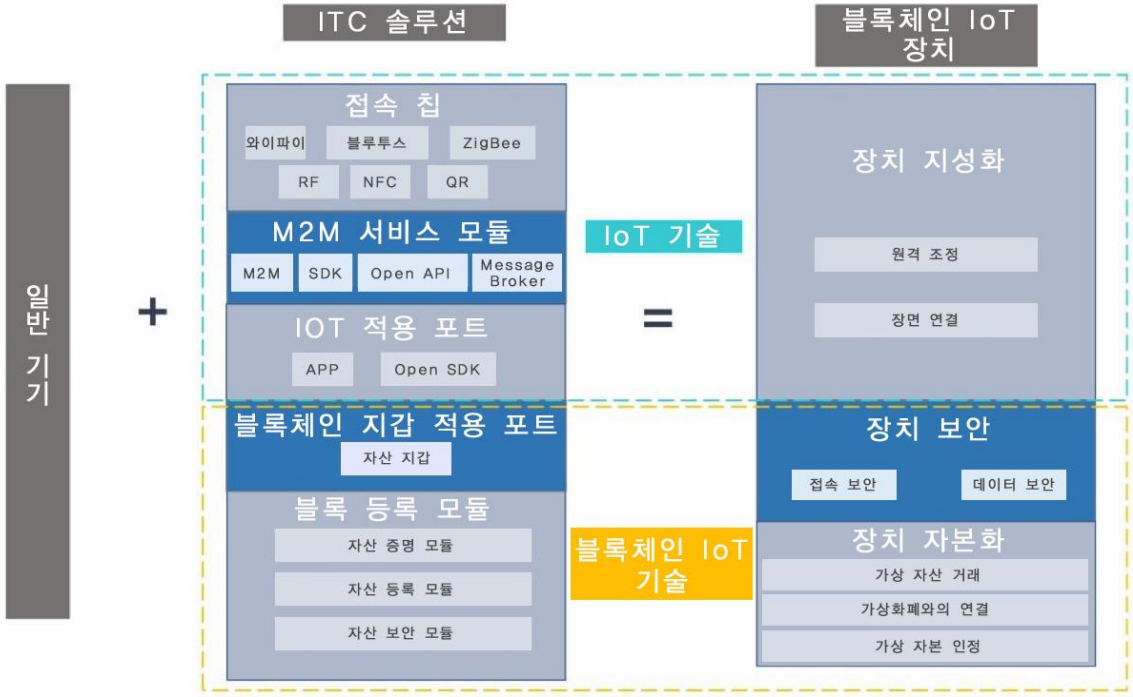

Figure 10: ITC 플랫폼의 구조

이 구조를 통해서 프로젝트 플랫폼의 안전 및 사용 편의성이 크게 개선되었다. (Figure 11 참고)

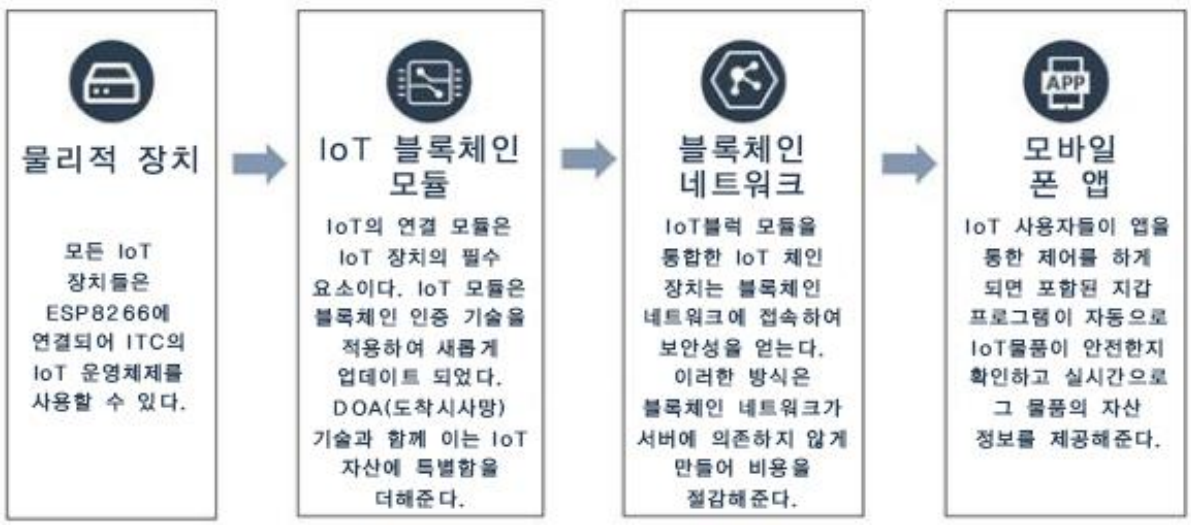

Figure 11: 사용자 시나리오

3. 우리의 구조

IoT 의 가장 큰 기본 구조는 전세계에 퍼져 있는 스마트 조명 장치와 그들의 노드들이다.세계에서 두 번째로 큰 시장 조사와 컨설팅 회사인 Marketsand Markets 의 최근 연구 보고서에 따르면, 2020 년에는 스마트 조명 시장의 규모가 81.4 억 달러의 규모에 이르고 2015 년부터 2020 년까지 연평균 성장률이 22.07%가 될 것이라고 한다.

Ericsson 의 예측에 따르면, 전 세계의 IoT 의연결 규모는 2020 년에 500 억 위안까지 증가할 것이라고 한다.스마트 가구는 건축 IoT 에 있어서 가장 실현가능한 중심점이 될 것이며 일반 사용자들에게도 퍼질 것이다.가장 일반적이고 기본적인스마트 가구로써,스마트 조명은 5G 의 개발에서 가장 큰 이윤을 얻을 수 있을 것이다.

Shanghai Zhuonian Software Research and Development Co., Ltd.는 전세계의 스마트 조명 회사들에게 IoT 기술을 제공하는 주요 전문 공급업체로써 단단한 기반과 방대한 자원을 바탕으로 ITC 프로젝트를 운영하고 있다.다른 비슷한 프로젝트들과 비교하였을 때,우리의 프로젝트는 놀라운 기술적 우수성을 지니기에 프로젝트의 성공을 보장할 수 있다 (Chart 2 참고)

	IoT Chain	IOTA	SLOCK.IT	IBM-ADEPT	중국 프로젝트
기반	일반 단일 칩 마이크로 컴퓨터	소비자가 자가 개발	이더리움에 특화된 컴퓨터	사용자의 요구에 따라서 주문 제작	RFID 라벨 붙이기
온 체인 전에 변형될 가능성	없다	없다	없다	없다	높음
서비스 모듈	비-인식 업데이트	소비자가 IOTA 적용 프로토콜을 직접 개발	소비자에게 이더리움 컴퓨터를 제공	사용자의 요구에 따라서 주문 제작	알려지지 않음ㄴ
소비자들이 직접 개발해야 하는가?	아니다	맞다	맞다	맞다	맞다
해결된 문제	IoT 중앙집중화/IoT 보안/물리적 자산 디지털화/장비 공유	M2M 소액 결제 효율성/수수료 없는 소액결제	물리적 장치 공유	사용자의 요구에 따라서 주문 제작	물리적 자산 디지털화
기본 블록체인 기술	PBFT 를 기반으로 한 분산된 메인 체인 DAG 서브넷과 조합한 합의 프로토콜	DAG 기반의 TANGLE	이더리움	Hyperledger	모름
타겟 적용 분야	스마트 조명/보안/전자기기/산업 IoT	스마트 전자기기/산업 IoT	스마트 잠금 장치	몇 개의 산업 IoT 분야	번호판 교체/자산 가상화 거래
확인된 적용 분야	스마트 조명은 정착했고 스마트 홈과 보안에서 발전 중	정식 회사가 통신 결제 서비스를 홍보해줌	이더리움 잠금 장치를 개발	모름	모름

Chart 2 여타프로젝트들과의 비교

4. 상품 계획

현재의 IoT 시스템은 중앙집중형 지능형 장치 시스템을 가지고 ITC 는 본질적으로 P2P 노드 네트워크이다.전체적인 네트워크의 안정성을 유지하기 위해서는 충분한 양의 노드들이 필수적으로 필요하다.노드들은 정상과 비정상 유형으로 나뉜다.정상 유형의 노드들은 열린 채로 있어도 작동 능력이 사용되지 않는 기기들을 의미한다.반대로 비정상 유형들은 한번 열리게 되면 바로 작동을 시작하게 된다.POW 에 따른 전력 낭비를 막기위해서 우리는 더욱 안정된 정상형 노드들을 찾아야한다.

조명을 예시로 들자면,지구의 자전은 우리에게 낮과 밤을 주고 우리는 밤에 조명을 필요로 하게 된다.현대 사회에서 빛은 조명 기구에서 나오는데, 이는 거대한 양의 정상 유형의 장치이며 ITC 의 안정성을 유지하기 위해 사용될 수 있다.예를 들면, Zhuonian 조명 클라우드

장치를 사용할 때,사용자는 APP 에 로그인해서 조명을 조절해야 하며 중앙 서버가 사용자와 장치 모두에게 권한을 부여하지 않는 이상 사용자는 조명장치를 사용할 수 없다.

우리의 기술 계획은 기존의 스마트 조명 장치를 업데이트하고 백엔드 검증 네트워크와 소유권을 활용하며 시스템이 ITC 의 블록체인 기술을 사용하여 검증하는 것을 보장하고자 하는 것이다.이를 통해,우리는 우리의 스마트 조명 시스템이 이전보다 더욱 안전하고,빠르며 안정적일 것이라고 보장 할 수 있다.

Figure 12: Zhounian 블록체인의 IoT 조명 구조

Figure 13: 블록체인 IoT 조명의 적용

좀더 구체적으로, 우리 프로젝트의 연구 개발 및 제품 개발 일정은 다음과 같다. (Figure 14 참고)

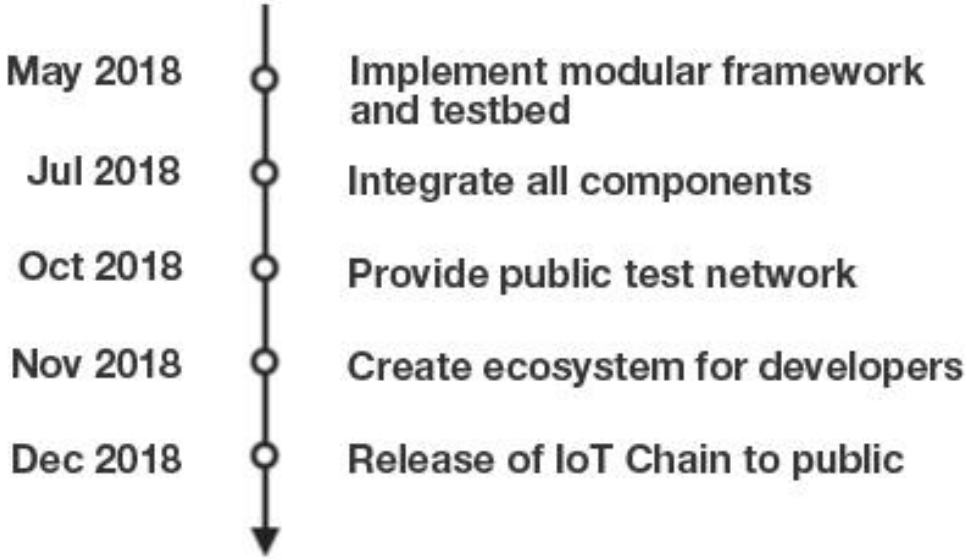

Figure 14: 기술 연구 개발 일정 및 제품 개발 전략

5. 상품 계획

ITC 만물인터넷 솔루션의 발전 전망에 대한 긍정적인 평가와, 향후 공동으로 블록체인 기술에 기반한 ITC 만물인터넷의 제품개발에 참여하는데에 대해 아래와 같은 업체들이 ITC 만물인터넷 팀과 기본협정을 체결하였다.

【Lierda Kesi Science & Technology Group Co.,Ltd】는 사물인터넷 매입형 기술 솔루션을 제공하는 국가급 하이테크 기업으로 주요하게 매입식 마이크로 컨트롤러 기술, 사물인터넷 무선 RFID 기술을 연구하고 있다. 회사는 수년간 고부가가치 및 하이테크 제품들을 출시했으며 솔선하여 중국 국내 매입식 마이크로 컨트롤 기술과 사물인터넷 기술을 위주로 한 신형 산업구조를 구축하였다. 그외 다수 핵심기술과 자주적 지식소유권을 보유하고 있다.

【Gizwits IoT Technology Co., Ltd】산하 브랜드 Gizwits 은 세계에서 가장 큰 사물인터넷 개발(PaaS) 및 (SaaS)클라우드 서비스 플랫폼, 종합 사물인터넷 플랫폼 서비스 선두자, 기술 인큐베이팅 플랫폼, 국가급 하이테크 업체다. 2016 년 년말에 이르러 5 만명이 넘는 스마트 하드웨어 개발자들이 Gizwits 을 기반으로 한 개발작업을 진행하고 있었으며 Gizwits 에는 700 만개 이상의 스마트 단말기가 액세스되었으며 Gizwits 은 6000 여개 기업에 서비스를 제공하여 시장점유율 1 위를 차지하고 있다.

【Shanghai Ximo Communication Technology Co., Ltd】는 연구개발, 생산, 판매를 일체화한 하이테크 기업이다. Ximo 는 글로벌 선두에 서고 있는 인터넷 관리 및 최적화에 전념하고 있는

장비 제조업체이며 스마트 홈 제품 및 솔루션, 스마트 라우터, 스마트 DNS 등 제품을 생산하는 업체이다.

【Comen Eletronics Technology CO., Ltd】는 연구개발, 생산을 일체화한 하이테크 스마트 홈 관련 제품 생산업체다. 2002 년에 설립된 회사는 부지면적 23000 평방미터, 임직원 300 여명을 거느리고 있다. Comen 는 스마트 홈과 사무용품 개발에 전념하고 있으며, 주로 파워 디스트리뷰터, 무선 스위치, 서지어레스트, 멀리 소켓, USB 충전기, 계량기와 에너지 절약 관련 제품들을 생산하고 있다.

【Wuxi Balas Lighting Electronics Co., Ltd. 】는 2000 년에 설립된 회사로서 종합적인 실력을 두루 갖추었으며 발전 잠재력을 지니고 있는 회사다. 전원으로부터 시작하여 조명제품의 설계과 개발 및 생산에 이르기까지 모두 자체적으로 완성하고 있다. Balas 의 LED 조명제품은 선두적인 기술력과 안전성으로 유명하다.

【Norra Technologies Co., Ltd. 】는 전문적으로 무선 온습도계 및 클라우드 시스템의 연구개발 및 생산과 판매를 하고 있는 기업로서 GPRS 무선 온습도계, 클라우드 센터, 스마트 데이터분석, 핸드폰 APP 를 일체화한 중국 국내에서 맨 처음으로 경량화 센서 데이터 채집 시스템 연구개발에 종사한 기업이다.

3 장 팀 구성

우리 프로젝트의 팀 멤버들은 모두 스마트 하드웨어와 알고리즘 분야에 있어서 노련한 전문가이며 비즈니스를 시작하는 데에 있어서 풍부한 경험을 지니고 있다.또한,우리는 업계의 엘리트들을 프로젝트 컨설턴트로서 고용했다.멤버들은 다음과 같다.

[코어 팀]

CEO: Xie Zhuopeng

Xie Zhuopeng 은 IT 분야의 수석 기업가이자 전문가이다.그는 스마트 하드웨어 분야에서 4 년간 종사했으며 3 년 간 블록체인에 대하여 깊이 연구해왔다. Xie 는 스마트 하드웨어에 대한 깊은 통찰을 지니고 있으며많은 스마트 하드웨어 관련 회담에서 연사로 초청 받아왔다.그는 국내외 여러 조명 회사들을 위한 스마트 조명 구조 설계에 참여하였으며그 외에도 여러 스마트 하드웨어 구조 설계에 참여하였다.

CTO: Ding Yin

Ding Yin 은 칩의 펌웨어 개발을 위해서 12 년간 일하였으며 디지털 이미지와, 3D 모델 검색, 음성 및 영상의압축 알고리즘 처리,그리고 은행 카드의 금융 소프트웨어 등에서 경험이 있다.Ding 은 칩의 하드웨어와 내장된 소프트웨어 구조,그리고 암호화 알고리즘에 대해 깊게 이해하고 있다.

CFO: Zhao Tan

Zhao Tan 은 MIT 출신의 경영학 석사이며 중국,싱가폴, 그리고 영국의 공인 회계사이다.그는 한때 Kerry 의 아시아 태평양 지부 CFO 였으며 몇 억달러의 외국 외환 손실 방지,국경간 자본 이동을 위한 전략적 계획,현금 흐름 관리그리고 은행 경영 시스템을 짜는 일을 담당했다 (J.P. Morgan).그는 한때중국의 IPO 와 싱가폴의 KPMG 의 감사팀에서 일하기도 했다. Zhao 는 금융 관리, 자금 조달 그리고 IPO 에 풍부한 경험이 있고 금융 기술 혁신에 큰 흥미가 있다.

메인 개발자: Liao Dongnian

Liao 는 스마트 하드웨어 분야에서 4 년간 종사해왔으며 세계 최고의 조명회사에서 스마트 조명 구조 설계를 이끌어왔다.그는 블록체인 기술을 3 년간 공부 했으며 java, C++, ruby, mqtt 그리고 블록체인을 완전하게 익혔다.

메인 개발자: Hu Yasheng

Hu 는 스마트 하드웨어분야에서 4 년간 종사해왔으며 2013 년부터 블록체인 IoT 기술에 관해서 연구해왔다.그는 한때 국제적으로 유명한 브랜드를 위한 IoT 구조 설계의 개발과 연구를 도왔다. 또한,그는 Tongcheng TourismPetty Loan 의 할부 사업부서에서 기술 매니저로 일했었다.

[자문 팀]

Liang Ran: 블록체인 분야의 전문가로서, Liang 은 주로 블록체인 자산의 문제와 거래에 대해서 연구했다. 그는 ChinaLedger Whitepaper 와 China Blockchain Technology, 그리고 MIIT 에 의해서 발행된 Application Development Whitepaper 를 공동 편집했으며 MIIT 의 첫 번째 중국 블록체인 개발 콘테스트를 심사했다.또한,그는 RippleFox 의 공동 창시자이다. (RippleFox 는 중국 최대 규모의 Ripple 과 Stellar 게이트웨이이며 Ripple 과 Stellar 의중국 커뮤니티를 이끌고 있기도 하다)

Zhou Shuoji : Zhou 는 FBGCapital 의 창립 파트너중 한명으로,디지털 화폐 거래의 전문가이자,블록체인영역의 활발한 투자가이기도 하다.중국의 블록체인 기술 선구자 이자 업계 핵심 인사로서, Zhou 는 현재 두개의 디지털 화폐 사모 펀드를 운영하고 있다.

Ma Zhiwei : Ma 는 Opple Lighting Co., Ltd (603515)의 부사장이다. Opple 은 공기업으로 바뀐 뒤 3 천만위안이 넘는 시장 가치를 기록하며 세계 최대의조명회사가 되었다.

Ji Xinhua: 상해 교통 대학의 총장이며 상해 과학 기술 발전대회에서 1 등 상을 받았다.Ji 는 Unionpay 신용 카드의 암호화 칩과 중앙 은행의 디지털 통화를 위한 표준을 구축하는데 일조했다.

Sheng Wenjun: Telink 의 창시자이다. 그는 칭화 대학교에서 학사, 석사 그리고 박사 학위를 얻었다.Telink 는 인텔의 전략적 지원을 받고 있으며 IoT 와 협력 관계이다.

Qiu Haiyi: High-Flying 의 창립자이자 총 지배인이다. High-Flying 은 AI 칩을 배포하는 회사이며 Baidu 의 지원을 받은 유일한 기업이다. High-Flying 의 연매출액은 1 억 5 천만위안이다.

4 ITC 토큰 모델

ITC 는 IoT onchain Token 의 약칭으로, 탈중앙화 사물인터넷 운영체제의 작동을 위한 '연료'이다.ITC 는 만물인터넷 생태계내 가치 유통의 척도 이며, 모든 스마트 기기의 사용권과 소유권 및 스마트 기기간 컨텐츠 생태계에서의 가치 유통 시에는 전부 ITC 로 결산하게 된다.

아래의 두가지 점은 생태계내 ITC 에 대한 수요가 부단히 늘어나는 것을 보장하게 된다.

1. 만물 인터넷 생태계에 접속된 모든 스마트 장비는 반드시 일정한 양의 ITC 를 가지고 있어야 한다. 따라서 더욱더 많은 스마트기기가 만물인터넷에 접속됨에 따라 ITC 에 대한 수요도 부단히 높아지게 된다.
2. 2.만물인터넷에서 데이터의 주권은 유저에게 귀속된다. 빅데이터 시대에는 빅데이터 분석 수요가 끊이질 않을 것이며, 빅데이터 분석 수요가 생길 때마다 (기업은) 각각의 유저가 기여한 데이터의 가치에 따라 ITC 를 지불하게 된다. 만물인터넷 데이터 생태의 건전한 성장에 따라 ITC 에 대한 수요 또한 끊임없이 늘어나게 된다.

참고 문헌

[1] Bahga A, Madisetti V K. Blockchain platform for industrial Internet of Things [J].J. Softw. Eng. Appl, 2016, 9(10): 533. Castro M, Liskov B. Practical Byzantinefault tolerance[C]//OSDI. 1999, 99: 173-186.

[2] Castro M, Liskov B. Practical Byzantine fault tolerance[C]//OSDI. 1999, 99:173-186.

[3] Cachin C. Architecture of the Hyperledger blockchain fabric[C]//Workshop onDistributed Cryptocurrencies and Consensus Ledgers. 2016.

[4] Miller A, Xia Y, Croman K, et al. The Honey Badger of BFT Protocols[C]//ACM Sigsac Conference on Computer and Communications Security. ACM,2016:31-42.

[5] Nakamoto S. Bitcoin: A peer-to-peer electronic cash system [J]. 2008.

[6] Jia Chang, Feng Han. Blockchain: from digital currency to credit society [J].2016. Beijing, CITIC Publishing House

[7] People on nxtforum.org (2014) DAG, a generalized blockchain.https://nxtforum.org/proof-of-stake-algorithm/dag-a-generalized-blockchain/(registration at nxtforum.org required).

[8] Lee J, Bagheri B, Kao H A. A cyber-physical systems architecture for industry4.0-based manufacturing systems [J]. Manufacturing Letters, 2015, 3: 18-23.