**데이터 거래용 코인 개발**

2012102901 유동관

2013104098 이상원

2013104118 조정현

**1. 개 요**

기존의 중앙 집중화 데이터 거래 시스템에 블록 체인과 결합시켜 프로젝트를 진행 하려한다. 블록 체인은 신뢰된 기관, 즉 제 3자가 관여하지 않고 사람과 사람(P2P)간의 데이터를 블록 형태로 저장함으로써 데이터 분산 네트워크를 기반으로 한다. 기존의 중앙 집중화 데이터 거래 시스템의 장점인 대용량의 데이터를 쉽게 저장 및 다운로드가 용이하다는 점과 블록 체인의 장점인 데이터의 무결성을 보장해준다는 점을 합쳐 대용량의 데이터를 기존의 중앙 서버의 데이터베이스에 저장하고 그 데이터의 해시 값을 블록 체인에 저장하므로 기존 데이터 거래 시스템의 장점과 블록체인의 장점을 합친 데이터 거래 시스템을 만드는 것을 목표로 하고있다.

**~~2. 서 론~~**

**~~2.1연구 배경~~**

블록체인 기술이 새롭게 도입됨에 따라 데이터의 위, 변조가 불가능에 가깝게 하는 기술들이 구현할 수 있게 되었다. 이런 블록체인의 기술은 일정 시간마다 만들어지는 검증된 거래 데이터를 ‘블록’의 단위로 나누고, 이 블록들을 ‘사슬(체인)’처럼 연결, 완전한 하나의 데이터를 구성하고자 한다. 이로 인해 거래 데이터가 훼손되거나 조작될 위험성을 제거할 수 있다. 거래 정보를 특정 기관의 중앙 서버가 관리하는 것이 아니라 개인 대 개인의 네트워크로 분산하여 특별한 장부 책임자가 존재하는 것이 아닌 사용자가 공동으로 기록하고 관리하는 거래 장부를 만든다는 이야기이다. 중앙 거래 방식의 장부를 쓰지 않고 사용자 모두가 장부를 관리한다고 볼 수 있다. 각각의 블록이 일정 단위의 시간마다 수시로 업데이트되며 동등한 정보를 유지하기 때문에, 이를 해커가 임의로 변경하기 위해서는 거래 장부를 보유한 사용자를 동시에 공격해 50% 이상의 내용을 해커가 원하는 정보로 바꾸어야 한다. 블록체인 분야는 장차 해당 이해당사자가 많고, 신뢰성이 요구되는 분야에서는 특별히 그 효용성이 클 것으로 예측된다. 따라서 캡스톤 디자인에서 블록체인 기술을 연구하고 데모 시스템을 직접 개발해보는 경험을 하고자 연구 주제를 선정하게 되었다.



[그림1] 출처 :h[ttp://news.joins.com/article/15322626](http://news.joins.com/article/15322626)

세계 최대 전자상거래 업체인 중국의 알리바바 그룹이 쉽고 빠른 결제 방식을 앞세워 국내의 전자결제 시장에 진출하였다. ‘알리페이’라고 불리는 이 시스템은 한국의 공인인증서 문제를 말끔하게 해결해 주었다. 액티브 x와 공인인증서에 막혀있어 새로운 결제 플랫폼 구축에 뒤처진 한국에 비해 중국은 빠르고 쉽게 거래할 수 있도록 도와주었다. 알리페이는 판매자와 소비자가 서로 다른 통화를 사용하더라도 알리페이가 중국 위완화와 달러의 환율을 반영하여 알아서 정산시켜준다는 장점도 있다. 이러한 환경을 극복하기 위하여 우리

도 빠르고 쉽게 데이터 거래를 위한 플랫폼을 구축하고자 하는 목표가 생겼다.

**~~3. 연구 목표~~**

데이터 거래용 코인을 개발한다.

기존 서버방식의 문제점을 블록체인을 적용하여 해결하고자 한다.

메인 서버가 해킹으로 인해 위변조 되는 것을 블록체인 기술을 적용하여 해결하고자 한다.

블록체인과 서버방식을 적절하게 조합한 방식의 새로운 시스템을 개발한다.

1. **~~기존 연구~~**

**~~3.1~~ 중앙 집중 시스템을 이용한 데이터 거래에 대한 연구**

중앙 집중 시스템을 이용한 데이터 거래는 한대의 서버를 중앙에 두고 데이터를 중앙에 저장하며 다운로드하는 구조다. 이 구조의 문제점으로 한대의 서버에 부하가 집중된다는 현상이 있는데 이것을 해결하기 위한 연구들이 이루어 지고있다. 그 대표적인 연구로 데이터 거래를 분산 처리 시스템으로 구축하는 것이다. 데이터 거래를 분산 처리 시스템으로 구축하여 컴퓨팅 자원의 제약이 없어지며 부하를 분산 시킬 수 있다. 또한 여러 시스템 중 하나의 시스템에 오류가 발생하더라도 다른 시스템은 계속 일을 처리하므로 신뢰도가 향상되는 효과도 얻을 수 있다. 하지만 설계가 복잡하고 운영 비용이 증가하는 단점이 있고 데이터의 갱신이 빈번히 발생되어 정합성 유지가 어려운 경우가 있음으로 이에 대한 해결방안이 연구 중이다.

**~~3.2~~ 블록 체인을 이용한 데이터 거래에 관한 연구**

블록 체인은 신뢰된 기관, 즉 제 3자가 관여하지 않고 사람과 사람(P2P)간의 데이터를 블록 형태로 저장함으로써 데이터 분산 네트워크를 기반으로 한다. 블록 형태로 데이터를 저장하는 일련의 작업을 여러 분산된 컴퓨터들에게 부여하고 그 보상을 암호 화폐의 형태로 지급하게 된다. 이는 방대한 블록 체인 속에서 우리는 물리적 환경에 관계없이 방대한 양의 데이터를 관리 할 수 있게 된다. 이에 대한 연구로 Datum은 블록 체인 장부를 기반으로 한 탈중앙화, 분산된 사용자 데이터 거래 장터이다. 사용자가 데이터를 제출하고, 스토리지 노드 마이너들이 데이터를 저장을 한다. 스토리지 노드는 그 대가로 DAT 토큰을 받는다. 그 후 구매자가 적용된 조건에 따라 데이터를 제공 받는 방식이다.



[그림2]출처: https://datum.org/

**3.3 블록 선택 알고리즘에 관한 연구**

블록을 보유해야 그에 대한 보상(코인)을 얻기 때문에 많은 사람들이 블록을 얻기 위해 블록 체인에 들어가려고 한다. 때문에, 타당하게 블록이 분배되는 것을 고려해야 했고, 악의적인 해커도 걸러내야 하는 보안상 문제도 대두되었다. 따라서, 몇가지 블록체인 알고리즘이 고안되었다.

먼저, 블록체인의 블록을 분배하는데 있어서 제일 먼저 고안된 POW (Proof-Of-Work)는 많은 양의 해시를 보유한 사람, 즉, 알고리즘을 풀어내는 작업을 많이 한 사람이 블록을 얻는 경쟁 방식의 블록체인 메커니즘으로 연구되었다. 이는 블록체인의 바탕은 분산된 형태의 데이터를 공유하는 블록 형성이 주가 되기 때문에 이 작업에 도움이 되는 즉, 많은 양의 해시를 보유하고 있는 사람이 블록을 얻고 코인을 얻는 타당성을 고려하였다.

또, POW는 보안성면에서도 탁월하다. 기본적으로 1개 CPU당 1개의 투표권을 가진다. 따라서, 공격자가 악의를 가지고 블록체인상의 거래내역을 조작하려 한다면 51%의 지분을 확보해야 하며, 이를 51% Attack이라고 한다. POW기반의 블록 체인을 공격자가 조작하려 한다면 공격자는 51%이상의 컴퓨팅 파워를 확보해야 한다. 하지만, 51%의 CPU를 확보하려 한다면 최소 수천억 이상의 돈이 들기 때문에 공격자가 수천억의 비용을 들여 블록 체인을 조작한다 해도 그 이익은 미비하다. 하지만, POW 방식은 많은 양의 일을 하기 위해 높은 전력과 여러가지 높은 비용의 하드웨어가 필요하게 되었기에 이를 보완하기 위한 다른 블록 분배 알고리즘인 POS(Proof-Of-Stake)가 고안되었다.

POS는 기존의 POW방식과는 달리 블록의 분배가 '해시'의 양이 아닌 '코인'의 양이 기준이 된다. 따라서, 많은 양의 코인을 가진 사람이 굳이 좋은 하드웨어 작업 환경(CPU, GPU 등) 없이 블록을 얻을 수 있다. 이는 많은 컴퓨팅 파워를 소비하지 않는 것을 의미하며, 환경 친화적이다. 두번째로 악의를 가진 공격자가 51% Attack을 시도할 경우 POW에 비해 POS의 경우 공격자가 훨씬 큰 비용을 지불해야 하기 때문에 보안성면에서도 POW에 뒤지지 않는다.

**~~3.4 기존 연구의 문제점~~**

**3.4.1 중앙 집중 시스템을 이용한 데이터 거래에 대한 연구의 문제점**

중앙 집중 시스템을 이용한 데이터 거래의 경우 데이터의 위/변조에 취약하다. 중앙 집중 시스템의 경우 하나의 중앙 서버만 존재하기 때문에 하나의 중앙 서버가 해커로부터 공격을 받으면 서비스가 마비되거나 데이터의 위/변조가 되게 된다. 서비스의 마비의 경우 분산 처리 시스템을 적용하면 해결이 되지만 데이터의 위/변조의 경우 해결이 어렵다. 이 부분의 경우 보안을 강화 하는 방법으로 해결하고 있지만 이 방법도 확실히 막는 것이 아니기 때문에 데이터 위/변조에 취약한 문제점이 있다.

**3.4.2 블록 체인을 이용한 데이터 거래에 관한 연구**

**3.4.2.1 데이터 크기에 대한 문제**

블록 체인을 이용한 데이터 거래의 경우 대부분의 연구가 데이터를 담을 수 있는 크기를 제한하여서 용량이 큰 데이터의 경우 거래가 어렵다. 또한 제한을 걸어놓지 않은 연구의 경우 데이터 크기에 따라 코인이나 이더리움의 경우 gas, Datum의 경우 DAT 토큰을 지불하기 때문에 실질적으로 대용량의 데이터를 거래하는 경우가 어렵다. 또한 블록의 바디에 대용량의 데이터를 넣을 경우 블록 해시를 구하는 시간이 길어져 블록 생성 시간이 늦어지는 문제점이 있다.

**3.4.2.2 합의 알고리즘에 대한 문제**

기본적으로 POW 방식은 해시 값을 찾아내야 하고, 그 작업을 위해 불필요한 리소스들이 대거 투입되어 무의미한 에너지 소비가 증가한다. 또 특정 연산 능력만 강요되다 보니, 연산 능력이 집약된 별도 칩들이 등장하게 된다.

POS는 지분이 많을 수록 더 유리해지는 방식이므로, 각 노드들이 토큰을 수집하기만 하고 사용하지 않으려는 경향이 나타날 수 있다. 그리고 블록 체인의 첫 번째 블록에 해당하는 제네시스 블록 시점에서 지분이 100%에 달하기 때문에 시스템을 개시한 사람은 몇 번이고 전체 블록을 다시 만들어낼 수 있다는 치명적인 문제가 있다. 그 외의 각 노드들도 지분만 갖고 있으면 그 시점부터 다시 시작하는 것이 가능하기 때문에 POS만으로는 위/변조를 막을 수 없는 단점이 있다. 블록을 생성하는 코스트가 너무 낮기 때문에 이전 블록들로 거슬러 올라가서 현재까지의 모든 체인을 위/변조할 수 있는 가능성이 존재한다.

1. **~~프로젝트~~**

**~~4.1 기존~~ 연구와의 ~~차이점 및 해결방안~~**

기존의 중앙화 시스템을 사용하는 데이터 거래소의 경우 중앙에 있는 메인 서버가 해커로부터 공격을 받거나, 혹은 천재지변으로 인한 서버에 손상이 올 경우를 대비하여 백업을 해놓거나 서버를 분산시키는 방향으로 연구를 하였다.

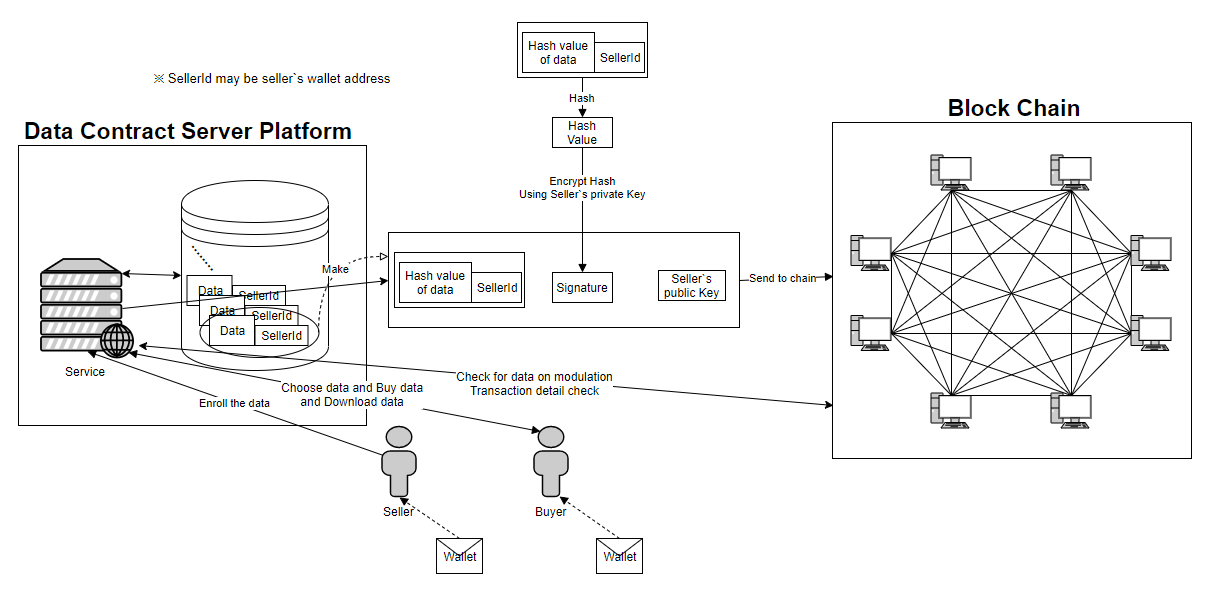
기존의 블록 체인을 이용한 데이터 거래소의 경우, 데이터 전체를 블록 바디에 담아 블록 자체의 크기가 커지므로 블록 해시를 찾는 시간이 증가하고 블록 체인의 크기가 커지므로 일부의 노드들은 채굴에 참여를 못하는 경우를 막기 위해 알고리즘을 개선하는 방향 혹은 데이터를 담을 수 있는 크기를 정해놓는 방향으로 연구를 하였다.

위 연구의 경우, 두 기존 연구의 문제점을 각 연구의 장점인 ‘데이터의 크기를 정하지 않고 용량이 큰 데이터도 문제없이 저장할 수 있는 점’과 ‘데이터의 위/변조를 막을 수 있다는 점’을 결합하여 해결을 하려고 한다. 데이터 자체를 중앙시스템에 저장하고 그 데이터의 해시 값을 블록 체인에 저장함으로 위/변조를 막을 수 있고, 블록 해시를 찾는 시간을 감소시킬 수 있고, 블록체인의 크기가 커짐을 막아 일부 노드들은 채굴에 참여하지 못하는 현상을 막으려고 한다.

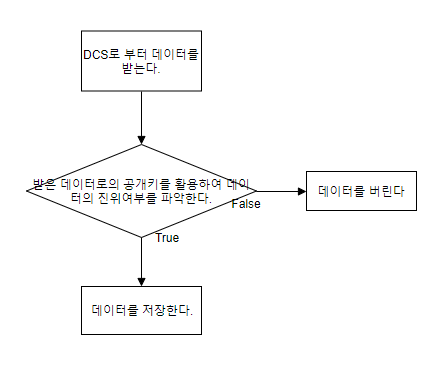
|  |  |  |
| --- | --- | --- |
|  | 문제점 | 개선 사항 |
| 보안 | 기존 서버방식 적용시 거점이 해커에게 공격받는다면 데이터 위,변조가 가능하다. | 데이터 해시값을 블록체인에 저장하여 위,변조를 막는다. |
| 블록체인 크기 | 블록체인에 데이터를 전부 담을 시 블록 체인 용량 자체가 커진다. | 데이터 자체는 서버에 저장하고, 해시값을 블록체인에 등록하여 데이터 크기 자체는 줄인다. |

**~~4.2프로젝트 내용~~**

~~기존의 중앙시스템의 장점과 블록체인의 장점을 결합하여 데이터 거래 코인 및 데이터 거래 시스템을 만든다~~**~~.~~**

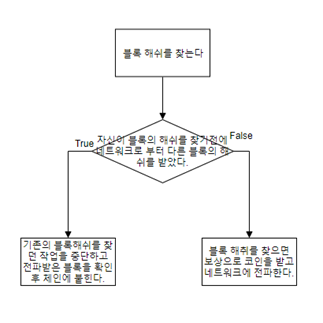
[그림 3] 전체 시스템 구조

판매자가 판매할 데이터를 서버(Data Contract Server, 이하 DCS)에 등록을 하게 되면 판매자가 등록한 데이터와 판매자의 지갑 주소가 같이 DCS의 데이터베이스에 등록된다. 그 뒤 판매자가 등록한 데이터와 판매자 지갑 주소를 합쳐 해시한다. 그리고DCS에서 앞선 해시 값, 그 해시 값을 판매자의 개인 키로 암호화한 값, 판매자의 공개 키를 담아 블록 체인 네트워크로 보낸다. 그 후 보내진 값들을 받은 채굴자 노드의 작업은 다음과 같다.



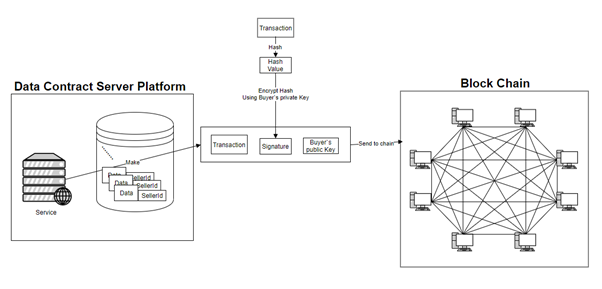
[그림 4] 채굴 작업1

채굴자는 저장한 데이터를 특정 기준(미정)에 따라가 블록 바디에 넣는다. 그 후

작업은 아래의 순서도와 같다.

[그림 4.1] 채굴작업2

이 과정이 일어난 후, 판매자가 등록한 데이터의 해시 값은 블록 체인에 기록됨으로, DCS에서 블록 체인으로부터 해시 값들을 가져옴으로 데이터의 위/변조를 확인 할 수 있다. 구매자의 경우 구매 시 DCS의 웹 서버에서 구매를 하여 자신의 지갑에서 판매자 지갑으로 코인이 전송 되며 DCS는 블록체인으로부터 구매자가 구매하려는 데이터의 위/변조를 확인한 뒤 구매자가 다운로드를 받을 수 있게 해준다. 그 후 구매자가 판매자에게 얼마의 코인을 보냈는지, 구매자가 어떤 데이터를 다운로드를 받았는지는 블록 체인에 데이터로 보내 기록하게 된다.

 [그림 5] 거래내역 및 구매 내역 저장

**~~5. 진행 일정~~**

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **월** | **3** | | | | **4** | | | | **5** | | | | **6** | | | |
| **주** | **1** | **2** | **3** | **4** | **1** | **2** | **3** | **4** | **1** | **2** | **3** | **4** | **1** | **2** | **3** | **4** |
| **데이터 코인의 개념 이해 및 체계 파악** |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| **논문작성** |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| **개발** |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| **디버깅 및 테스트** |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| **최종 보고서 및 발표준비** |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |

~~[표2] 진행 일정~~

**~~6. 결론~~**

기존 중앙 집중화 데이터 거래 시스템은 대용량의 데이터를 쉽게 저장할 수 있고 다운로드가 용이하다는 장점이 있다. 기존 블록체인의 장점은 신뢰기관인 제 3기관이 관여하지 않고 사람과 사람간의 데이터를 블록 형태로 저장함으로써 데이터 분산 네트워크가 형성되고, 데이터가 전부 공유되기 때문에 무결성을 보장해준다는 장점이 있다. 이러한 장점만을 합친 새로운 형태의 데이터 거래시스템은 물류 계약서 시스템 등 다수의 사용자, 이해관계자들에게 신뢰성 있는 데이터를 쉽고 빠르게 공유할 것으로 기대된다. 또한 기존 블록체인의 데이터 확장성 한계를 서버 시스템의 장점을 활용하여 해결할 것으로 기대된다.

**참고 문헌**

[1] Seo-Gu Kang, Hyung-Joon Bae, Seong-Hyeon Lim, Young-Sook Lee. (2017). A Study on the Vulnerability and Countermeasures of Bitcoin. Proceedings of the Korean Society of Computer Information Conference , 25(2), 124-127.

[2] Sungmin Rue. (2017). Industry Forecast – IoT Service based on Blockchain. Korea Institute of Information Technology Magazine, 15(1), 15-20.

[3] Kwang-Hun Kim, Heung-Youl Youm. (2017). File Exchange Model Using Ethereum. Proceedings of Symposium of the Korean Institute of communications and Information Sciences, , 1498-1499.

[4] JiYeon Yang, SoHee Kim, YoonJeong Kim. (2015). Bitcoin Vulnerability and Limitation Analysis of Current Countermeasure. 한국정보과학회 학술발표논문집, , 1013-1015.

[5] Satoshi Nakamoto.(2008) . Bitcoin: A Peer-to-Peer Electronic Cash System