블록체인 기반의 가상화폐 wallet 개발
- 이더리움 블록체인 기술 기반으로 -

안윤주[1], 박수영[2], 윤규희[3], 장예원[4]
동덕여자대학교 컴퓨터학과
yoonjoo30@gmail.com[1], sally0197971@naver.com[2], ojinga0519@naver.com[3],
rainsimple@naver.com[4]

Virtual money wallet development using Blockchain technology
- Based on Ethereum Blockchain technology -

Yoonjoo Ahn[1], Sooyoung Park[2], Kyuhee Yun[3], Yaewon Jang[4]
Dept of Computer Science, Dongduk Women's University

요 약

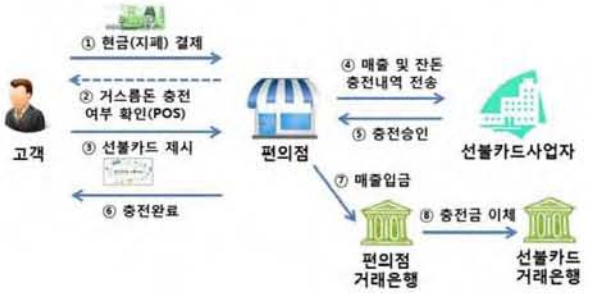
블록체인 기반의 가상 지갑을 만들어 그 가상 지갑 안에 현금 지폐를 쓰고 남은 거스름돈을 적립해 주는 사업 방식을 제시한다. 블록체인을 활용하여 기존의 선불카드를 이용한 거스름돈 적립의 복잡함을 없애고 간단한 알고리즘의 가상지갑에 거스름돈을 적립할 수 있다.

1. 연구의 배경 및 목적

2016년에 실시한 대국민 설문조사[1]에 따르면 지급수단으로 현금을 사용하는 비중이 점차 감소(2014년 37.7% → 2016년 26.0%)하고, 현금 이외의 지급수단에 의한 결제금액(총 9경 8,452조원)은 일평균 376.1조원으로 전년 대비 8.1% 증가했다. 이미 최근 다양한 국가의 중앙은행은 현금 없는 사회를 위해 디지털 화폐의 도입을 빠르게 시도하고 있다. 하지만 소액 거래 시에는 여전히 현금이 이용되고 있다. 그런데 현금 거래 시 거스름돈으로 받게 되는 동전은 그 발행과 관리에 많은 비용과 불편이 수반된다. 동전이 제대로 재사용되지 않아 매년 500억원정도가 동전을 발행하는 데에 소요되고 있다. 또한 은행 등 금융기관과 마트·편의점, 운수업체 등 동전을 많이 사용하는 업체들은 동전의 관리, 지급, 회수 등에 많은 인력과 비용을 투입하고 있다. 아울러 현금으로 거래할 때 발생하는 동전의 경우 사용하지 않는다는 응답이 46.9%였으며, 그 이유로 동전 소지가 불편하다는 응답은 62.7%였다[2]. 이를 통해 소비자들 역시 동전 사용에 많은 불편을 겪고 있다는 것을 알 수 있다.

한국은행은 이러한 동전 사용에 따른 불편을 해소하고 동전의 발행 및 유통에 드는 사회적 비용을 절감하기 위하여 「동전 없는 사회」 시범사업을 추진하고 있다. 한국은행의 잔돈적립서비스의 원리는 다음[그림 1]과 같다. 먼저 시범사업 매장에서 사용가능한 적립수단(선불전자지급수단)을 보유한 뒤 매장에서 현금으로 물건을 구입한 후 거스름돈을 돌려받는 대신 동일금액을 해당 적립수단에 충전한다.

그러나, 한국은행의 잔돈적립서비스 방식은 적립수단으로 충전하는 방식의 가장 큰 단점은 "적립 포인트 환급" 또는 "충전 포인트 환급"방식으로 인해 환급성이 제약이 발생된다는 점과 기존 중앙집중형 금융기관이 유지되고 있다는 점이다.



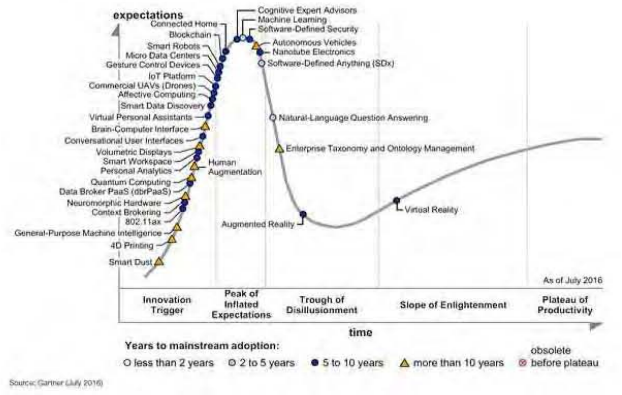
[그림 1] 한국은행의 잔돈적립서비스 방식

따라서, 본 연구에서는 편의점의 거래 은행, 선불카드의 거래 은행, 선불카드 사업자, 편의점, 그리고 고객을 묶는 방법으로 '이더리움 블록체인 기반의 가상화폐 wallet 개발'를 통해 P2P기반의 금융거래 생태계 형성이 가능한 기술적 방식을 제시하고자 한다.

2. 블록체인 기술의 배경과 Wallet 기술구조

2.1 블록체인의 설명 및 전망

2016년 초 세계경제포럼(WEF, World Economic Forum)에서 제 4차 산업혁명 시대를 이끌 핵심기술 중 하나로 블록체인이 선정되며 블록체인을 인식하고 활용하려고 많은 시도가 이루어지고 있다. 이미 IBM, Goldman Sachs, JP Morgan등에서는 블록체인의 혁신성을 인식하고, 2016 가트너(Gartner) Hype cycle(그림 2)을 통해서도 블록체인이 현 시점에서 떠오르고 있는 기술인 것을 볼



[그림 2] 2016 가트너(Gartner) Hype cycle

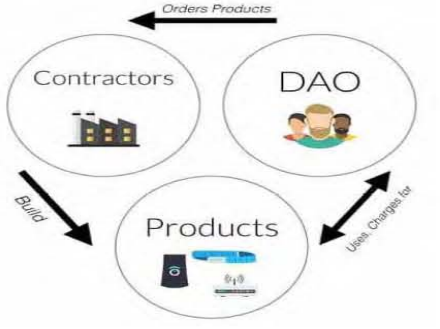
수 있다.

블록체인이란 분산된, 독립적인, 개방된 공통 장부(원장, ledger) 관리 기술이다. 이러한 블록체인은 Hashcash 아이디어를 공통 장부 관리에 응용하여 신뢰성 을 획득한 각 노드들이 P2P네트워크를 통해 일정 시간 동안 확정된 거래내역을 담는 방식으로 작동된다[3].

특히 블록체인 기술은 이론적으로 모든 종류의 자산의 등록, 보관과 거래에 적용 가능하므로 금융뿐만이 아니라 물류유통, 나아가서는 정부 공공행정 서비스에도 적용 가능할 것으로 전망된다. 이러한 블록체인이 적용 가능한 분야로는 디지털 자산의 거래, 디지털 인증, 디지털 지갑을 이용한 암호 화폐 등과 효율적인 계약을 자동화가 있다. 특히 블록체인을 기반으로 한 스마트 계약을 통해 계약할 경우 계약이 성립되기까지의 시간 단축과 시장의 규제 준수 비용을 절감하는 효과가 있다[4].

2.2 이더리움 기반의 블록체인 플랫폼

이더리움은 비탈릭 부테린(Vitalik Buterin)이 개발한 암호화폐로, '튜링완전언어'를 이용해 상상 가능한 모든 형태의 거래를 프로그래밍 할 수 있다. 튜링완전언어(Turing-Complete Language)는 계산 가능한 모든 수학 문제를 풀 수 있는 일반적인 알고리즘을 만들어낼 수 있는 컴퓨터언어이다. 이를 통해 본 연구에서는 이더리움 기반의 스마트컨트랙트[5]를 통해 자기 강제적 언어(Self-Enforcing Language)를 이용하여, 컴퓨터언어인 '실행코드'들로 작성한 조건들이 충족이 되면 자동으로 실행되어 계약이 이행되게 해주는 기술을 적용하고자 한다.



[그림 3] 이더리움 거래구조

2.3 블록체인 기반 가상 wallet 비즈니스 구조

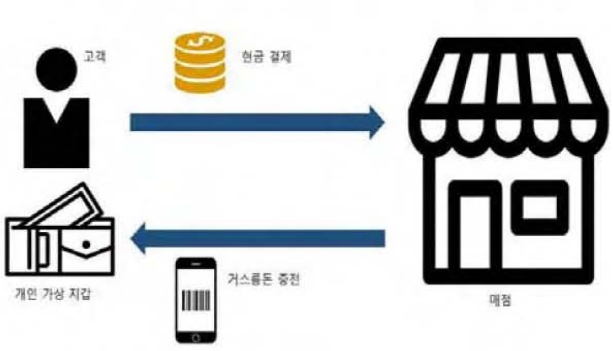
연구의 목표는 동전의 불편함과 비효율성을 없애기 위해 한국은행의 '동전 없는 사회' 사업에서의 선불카드 적립방식 대신에, 소액 및 단품 거래(대학 매점 같은)일 때 잔돈이 남으면 동전 대신 개인의 가상 지갑에 충전해주는 것이다.

현금으로 물건을 사고 거스름돈이 남을 경우, 동전을 주는 대신 개인의 가상 지갑에 적립하여 일정 금액이 되면 사용할 수 있도록 한다. 개인의 가상 지갑 별로 QR코드 등의 개인 아이디(바코드)를 부여하여 적립하는 시스템이다.

블록체인을 기반으로 하는 디지털 가상화폐로 물리적 형태가 없는 비트코인의 가장 큰 특징은 발행주체가 없는 것에 있다. 특정한 주체가 발행하는 화폐가 아니라 P2P방식으로 확보된다. 블록체인 기반인 '비트코인'의 계좌는 가상지갑이다. 우리의 연구는 현금으로 사고 남은 거스름돈을 이 가상지갑에 넣는 것이다.

잔돈 없는 사회는 몇 년 전부터 서서히 나오기 시작했다. 작년에 몇몇 편의점에서 잔돈이 남으면 동전을 선불카드에 적립하는 방식이 나오기 시작했다. 그렇지만 [그림 1]의 과정처럼 꽤나 복잡하다. 또한 선불카드 사업자를 통하기 때문에 수수료도 있을 것이다.

그래서 우리 연구는 블록체인을 이용하여 중개인(선불카드 업자)도 없고 수수료도 없이 동전 없는 사회를 만들 수 있다. 기존의 선불카드 방식에 비해 [그림 4]의 과정이 훨씬 간단한 것을 볼 수 있다. 블록체인을 통해 거래를 하면 거래하는 사람 모두 같은 거래 내역 정보를 가지게 된다. 이로 인해 해킹을 당하더라도 금방 대조하여 해킹 사실을 알 수 있고 중앙 서버가 없기 때문에 서버가 다운되어 일어나는 문제도 발생하지 않는다.



[그림 4] 중개인과 수수료가 발생되지 않는 구조

물론 '기존 화폐의 가치와 통용 될 수 있는가?'에 대한 의문이 제기될 수 있다. 비트코인의 가치는 유동적이라서 거스름돈의 현재 가치와 어떻게 비교하여 측정할 것인가가 어려운 문제다.

[그림 4]처럼 점차 많은 나라(한국, 미국, 일본, 영국, 유럽 연합회 등)들이 가상화폐를 법적으로 인정하고 있으면서 점차적으로 시장이 확대 되고 있다. 머지않아 이를 통

해 가상화폐를 점차 깊숙한 생활 속에서도 사용 할 수 있게 될 것이다. 결국 거스름돈의 현재 가치와 상응하게 될 것이다.

2.4 블록체인 기반 가상 wallet 설계 구조

본 연구에서는 기술적 구조를 Private기반으로 구현하기 때문에 Difficulty에 따라 선택된 Target 데이터 규격을 만족할 필요가 없다. 즉, 조건을 만족하기 위해서 블록체인 노드를 통해 Nonce라는 임의의 값을 계속 대입해야 하는데, 임의로 대입한 Nonce값이 Target 데이터 조건을 만족하면 블록이 생성하는 POW와 같은 거래방식이 발생되지 않는다. 이와 같은 기술적 구조로 적용하기 때문에 별도의 컴퓨팅자원이 필요가 없다.

그 대안으로 지분증명을 통해 컴퓨팅 파워 낭비가 아닌 자신이 가진 돈(stake)을 통해 블록을 생성을 시키고, 자신이 가지고 있는 지분(Stake)과 지분이 생성된 날짜에 의해 결정하여, 편의점의 거래 은행, 선불카드의 거래 은행, 선불카드 사업자, 편의점, 그리고 고객을 묶는 방법으로 '이더리움 블록체인 기반의 가상화폐 wallet 개발'를 통해 P2P기반의 금융거래 생태계 형성하고자 한다.

블록체인 기반 가상 wallet 기본 설계 목표는 1) 단순성으로 가급적 적은, 그리고 가급적 로우레벨 opcodes, 가급적 적은 데이터 타입을 제공하고, 2) 전체적인 확정성을 고려하여 모호한 부분을 제거한다. 3) 어셈블리는 가능한 컴팩트 해야 하여 20바이트 주소 처리, 32바이트 값을 가지는 암호화 처리 능력, 커스텀 암호화에 사용되는 모듈러 연산, 블록과 트랜잭션 데이터 읽기, 상태 정보 확인 등을 고려한다. 4) 최적화 용이성과 최적화를 적용하기 쉽게 하기 위해 설계를 한다.

블록체인 기반 가상 wallet Principles은 Sandwitch complexity model로 제시할 수 있다. 이더리움에서 제시되는 레벨별 아키텍처는 가장(mostly)로 정의할 수 있다. 가능한 단순하게 만들고, 가능한 인터페이스를 쉽게 만든다. 프레임웍에서 발생할 수 있는 복잡도가 최소한의 부분은 "미들 레이어"에 배치한다. 따라서 이 부분은 코어 컨센서스 영역은 아니지만 엔드유저에가 알 필요가 없는 부분이다. 컴파일러, 인자 직렬화, 데이터 스트럭처 모델(스토리지), leveldb 스토리지 인터페이스와 wire protocol로 구조를 제시한다. 블록체인 기반 가상 wallet Freedom은 사용자가 이더리움 프로토콜을 어떤 용도로 사용하던지 제약을 두지 않는다. 또한, 목적성에 별개로 이더리움 컨트랙트나 트랜잭션과 구분하여 구조화하지 않도록 한다. 블록체인 기반 가상 wallet Generalization 프로토콜 피처나 opcode는 최대한 로우레벨 컨셉들을 구현하고자 한다. 이를 통해 다양한 형태로 재구성과 활용될 수 있도록 구조화 한다. 프로토콜의 본질적인 기능은 컨트랙트 내부의 서브 프로토콜로 구조화한다.

Blockchain-level protocol은 비트코인은 UTXO기반이지만 본 연구에서는 이더리움 기반으로 프로토콜을 사용하기 때문에 Account를 사용한다. 본 연구의 가장 장점으로는 1) UTXO 모델에서 300바이트를 사용할 때 Account 모델은 30바이트만 사용하기 때문에 공간을 절약한다. 2) 특정 코인의 소스에 대한 블록체인 레벨의 개념이 없기 때문에 코인의 출처(사용자 소유권)에 따라 레드리스트나 블랙리스트를 적용하기 어렵다. 3) 스크립트를 작성하고 이해하기 쉽다는 단순성을 제공한다. 4) 경량 클라이언트 상태 트리를 읽음으로써 어느 순간에도 계정과 관계된 모든 정보를 읽을 수 있다는 경량 클라이언트를 제공한다.

이더리움의 Merkle Patricia Tree구조로 기본 데이터 구조. 어카운트 상태와 트랜잭션 등을 각각의 블록에 저장한다. 머클 트리와 패트리샤 트리를 결합한 것으로 구조를 생성한다. 즉, 루트 해시에 유일하게 매핑되는 기본적으로 키-밸류 쌍. 키-밸류 쌍의 추가, 수정, 삭제는 대수적인 (logarithmic) 시간 내에 처리되며, 최대 소요 시간이 일정한 한도 내에서 유지가 된다.

블록체인 기반 가상 wallet의 구현의 단순성을 위해서 바이트 단위의 확실한 일관성 확보를 하고자 한다. 많은 언어에서 키/밸류 맵은 순서(명시적)를 가지지 않는다. 이로 인해 동일한 데이터가 다른 인코딩으로 만들어지고 결과적으로 다른 해시를 가지게 될 가능성이 있다는 점이다.

블록체인 기반 가상 wallet Compression Algorithm은 와이어 프로토콜과 데이터베이스 모두 데이터를 저장할 수 있도록 커스텀 압축 알고리즘을 사용한다. 본 연구의 이더리움 블록체인의 각 블럭 헤더는 세 트리(Trie Usage)에 대한 포인터를 가진 것을 그대로 사용하고자 한다. 1) 블록 액세스 후의 전체 상태 표시(상태트리) 2) 인덱스를 키로 사용하는 블록의 모든 트랜잭션 표시(트랜잭션 트리: key 0: 첫번째 트랜잭션, key1: 그 다음 트랜잭션) 3) 트랜잭션을 처리한 후 상태 트리의 루트(medstate) 4) 트랜잭션 처리가 끝난 후 사용된 개스의 양(gas_used) 5) [address, [topic1, topic2 ..], data] 형태를 가지는 아이템 리스트로 트랜잭션의 실행중 LOG0 .. LOG4 opcode로 생성되는 로그 6) 컨트렉트의 주소. topic은 최대 4개까지의 32바이트 값이며, 데이터는 임의 길이의 바이트 배열인 address 7) 트랜잭션에 포함된 모든 로그의 주소와 토픽으로 구성된 블룸 필터(logbloom)을 제시한다.

블록체인 기반 가상 wallet 블록 시간 알고리즘에 대한 결정은 1) 네트워크 레이턴시보다는 충분히 크면서 가능한 빠른 시간(12초의 블록 시간) 2) 블록 히스토리를 일정 수의 블록이 지난 후에 "삭제"하기 위함(이전블록제한)이다. 3) 단순성 목표를 위한 설계(블록 자손 제한) 4) 빠른 업데이트 5) 낮은 변동성을 제시하는 난이도로 해시파워가 균등할 경우 급격히 바뀌지 않아야 한다. 6) 구현이 상대적으로 단순한 알고리즘을 제공한다. 7) 낮은 메모리 사용제공을 통해 메모리 변수를 제공한다. 8) Non-exploitability로 타임스탬프를 조작하거나 마이닝 풀이 수익 극대화를 위해 반복적으로 해시 파워를 추가하고

제거하는 일을 제거한다. 9) Gas and Fees는 프로그래밍 언어를 튜링 컴플리트하게 때문에 하나의 트랜잭션의 네트워크 대역, 스토리지, 연산 사용량은 달라질 수 있도록 구조화하고 무한 루프를 통한 DoS 공격을 막고자 한다.

2.5 블록체인 기반 가상 wallet 기술 구조

블록체인 기반 가상 wallet 주요 기술은 임시/영구 스토리지 구분을 구분하여 임시 스토리지와 영구 스토리지의 구분이 존재한다. 임시 스토리지에 저장된 값은 해당 인스턴스 안에서만 유효. 영구 스토리지는 해당 컨트랙트 전체에 유효하도록 구조화 한다. 이를 위해서 세 가지 유형의 computational state를 가지도록 하는데, 1) Stack 2) Memory 3) Storage로 구성한다.

블록체인 기반 가상 wallet 32바이트의 워드 크기를 통해 4바이트와 8바이트 워드 등은 너무 작아 비효율적으로 판단되며, 32바이트구현에서 사용되는 값들을 보관하기에 충분하다고 판단된다. 또한, 독자적인 VM을 개발을 하여 Java, Lisp dialect, Lua 등을 사용할 수도 있겠으나 독자적인 VM을 만들어 향후 연계 시 VM을 요구사항에 맞게 좀 더 특화시킬 수 있다고 판단된다. 따라서 dependency가 많아지면 설치가 매우 어려워지기 때문에 복잡한 외부 dependency를 없애도록 한다. 또한, 가변적인 메모리 크기인 스택 크기에 제한 없애며, 단순성을 위해 타입 형태를 제거한다. 다만, signed, unsigned에 대응하는 별도의 opcode 제공한다.(예: DIV, SDIV, MOD, SMOD)

3. 연구요약 및 제언

본 연구의 가장 큰 특징으로는 현재 사용하고 있는 화폐의 가치와 가상화폐의 가치를 동일화함으로써, 물건 구매 후 발생하는 잔돈과 동일한 가치의 가상화폐를 고객의 가상화폐 지갑에 적립을 시킬 수 있도록 한다는 것이다. 이는 혹시라도 사용자들이 가질 가상화폐의 가치에 대한 우려를 해소할 수 있다는 점을 구현했다는 점이다.

또한, 사용되지 못한 채 잠자고 있는 동전들이 회수되지 못 하는 것 아니냐는 우려가 있다. 하지만 이 프로젝트가 활성화 된다면 물건 구매 후 발생하는 잔돈이 가상화폐로 대신 지급되어 실제 사용되는 동전들의 양이 줄어들게끔 한다. 이에 더 나아가 동전들이 점차 줄고 있는 현상으로 인해 동전들의 가치가 사라질 것이라 걱정하는 사람들이 여태까지 회수되지 못하던 동전들을 사용함으로써 유통되지 못하던 동전들까지 유통되도록 해 사람들의 우려를 해소하고 동전의 유통과 관리에 소요되는 사회적 비용을 줄일 수 있다.

물론 위에서 언급한 블록체인 기반 가상 wallet 연구는 현재 시제품으로 이론과는 다른 양상의 결과를 초래할 수 있다. 그렇다 하더라도 현재 추세로 보아 해당 연구가 성공할 시에는 국내뿐만 아니라 한국을 찾은 외국인들이 쓰고 남은 동전들을 고국으로 가져가 국외에 남게 된 한국 동전들의 수를 줄여나갈 수 있을 것으로 보인다.

* 본 논문은 2017년 한이음 ICT멘토링 프로젝트의 결과물입니다.

참고문헌

[1] 한국은행 설문조사 결과, 2016
[2] 한국은행 보도자료 2016년 지급결제 동향, 2017
[3] 비트코인의 기반 기술 블록체인의 원리, 김석원(SPRI, Software Policy & Research Institute)
[4] 블럭체인 기술동향과 시사점, 이제영 (STEPI, 과학기술정책연구원)
[5] 이더리움 설계 근거
https://github.com/ethereum/wiki/wiki/Design-Rationale
https://andybclee.wordpress.com/