**1. 기존의 전자투표 시스템에 대한 문제점과 블록체인 기술을 도입하여 해당 문제점을 어떻게 해결할 수 있는지를 설명하시오**

기존 전자투표의 문제점을 확인하기 전에 기존 전자투표의 장점을 확인 해 보아야 한다.

전자투표의 장점으로는 1) 유권자의 투표 참여율 제고, 2) 다양한 투표 방식 지원, 3) 투개표의 안전성과 신뢰성이 보장을 들 수 있다.(표1 참조)

표 전자투표 특징

|  |  |
| --- | --- |
| 특징 | 내용 |
| 정확성 | 모든 정당한 유효투표는 투표결과에 정확인 집계됨 |
| 검증성 | 투표결과 위조방지를 위한 투표결과 검증수단이 필요 |
| 완전성 | 부정 투표자에 의한 방해 차단, 부정투표는 미집계 |
| 단일성 | 투표권이 없는 유권자의 투표참여 불가 |
| 합법성 | 정단한 투표자는 오직 1회만 참여 가능 |
| 기밀성 | 투표자와 투표결과의 비밀관계 보장 |
| 공정성 | 투표 중의 집계결과가 남은 투표에 영향을 주지 않음 |

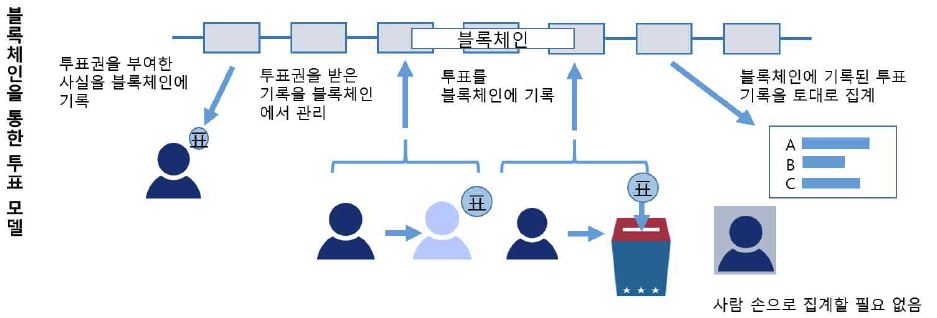
자료 : 케이보팅(K-Voting) 서비스 개요, <http://www.kvoting.go.kr>

이러한 장점을 가진 전자투표 시스템이 더 많은 분야에서 널리 활용되기 위해서는 기술적 안정성에 대한 신뢰와 전자투표의 유용성에 대한 공감대가 형성 되어야 할 것이다. 특히 전자투표 기술에 대한 “신뢰” 확보는 매우 중요하다. 기존의 전자투표 시스템이 가지는 보안성에 대한 문제점은 반드시 해결되어야 한다. 이를 위해서 “블록체인” 방식을 투표에 활용 하고자 하며 전자투표 시스템의 보안성 및 신뢰성, 투명성 향상을 위한 대안이다.

기존전자투표의 문제점으로는 크게 보안 문제 및 신뢰 확보의 문제(직접 선거 원칙의 위반)와 디지털 격차의 문제(선거의 평등원칙 위반)로 볼 수 있다.

중앙집중적 구조인 전자 투표 시스템은 해커나 바이러스 등의 사이버 공격에 취약할 뿐만 아니라 운영기구에 대한 불신이 있을 수 있는 1) 보안 문제 및 신뢰 확보의 문제(직접 선거 원칙의 위반), 원격(온라인)에서 진행되는 투표는 제3자에 의해 비밀 투표의 원칙을 훼손할 가능성이 존재 하며 조작의 어려움으로 인해 타인의 도움을 받는 과정 또한 비밀선거의 원칙에 어긋날 수도 있는 2) 투표의 비밀보장 문제(비밀 선거 원칙의 위반)와 같은 문제점이 있다.

기존 전자투표에 블록체인이 도입된다는 것은 기존의 전자 투표시스템의 기능보다 더 많은 기능을 블록체인 기반 전자 투표시스템이 해낼 수 있음을 의미한다. 블록체인은 기본적으로 공정성과 투명성, 확실성을 가지고 있다. 이에 더해 기존 전자 투표시스템의 한계점으로 지적되는 보안성 측면에 있어서 문제가 발생할 확률이 기존 시스템에 비해 매우 낮다.



블록체인은 모든 거래가 모든 사용자에게 기록되는 ‘분산거래장부’를 특징으로 한다. 이런 블록체인의 특성이 해킹과 그로인한 위/변조 위험에서 기존의 온라인투표시스템보다 자유로울 수 있다.

신뢰 대상의 변경도 블록체인 전자 투표시스템의 기능 중 하나다. 중앙서버의 관리자가 존재하고 그를 전적으로 신뢰 해야 했던 기존 온라인투표시스템에 반해 유권자 모두가 투표 과정과 결과를 스스로 검증할 수 있다. 투표의 위/변조가 불가능할 뿐만 아니라, 신뢰의 대상이 중앙서버의 관리자에서 시스템 그 자체로 옮겨간다.

전자 투표시스템에 블록체인을 적용할 경우 크게 2가지 형태로 적용 할 수가 있는데 private 구성과 public 구성이 있다. Public 구성의 경우 블록체인의 보안성이 사용자 수에 비례한다는 점을 통해 소수의 유권자가 참여하는 선거에 대해 안전하게 사용할 수 있다. private 구성은 참여 기준, 범위, 공개여부를 제한할 수 있어 유권자가 아닌 사람들의 참여나 열람을 막을 수 있다.

기존 전자투표의 장점을 포함하면서 블록체인 기반 기술을 활용하여 더 많은 기능을 활용하기 위해 블록체인이 가지고 있는 기본적인 특징도 기존 전자투표의 단점을 해결할 수 있지만 추가적으로 투표권의 행사를 위해 투표권자에게 각각 Account를 생성하고 SmartContract를 이용하여 투표권을 부여한 사실이 맞는지에 대한 권한체크, 사용자의 정보를 Hash화 하여 Account와 매핑을 한다면 익명성 또한 보장 할 수 있다.

참고자료

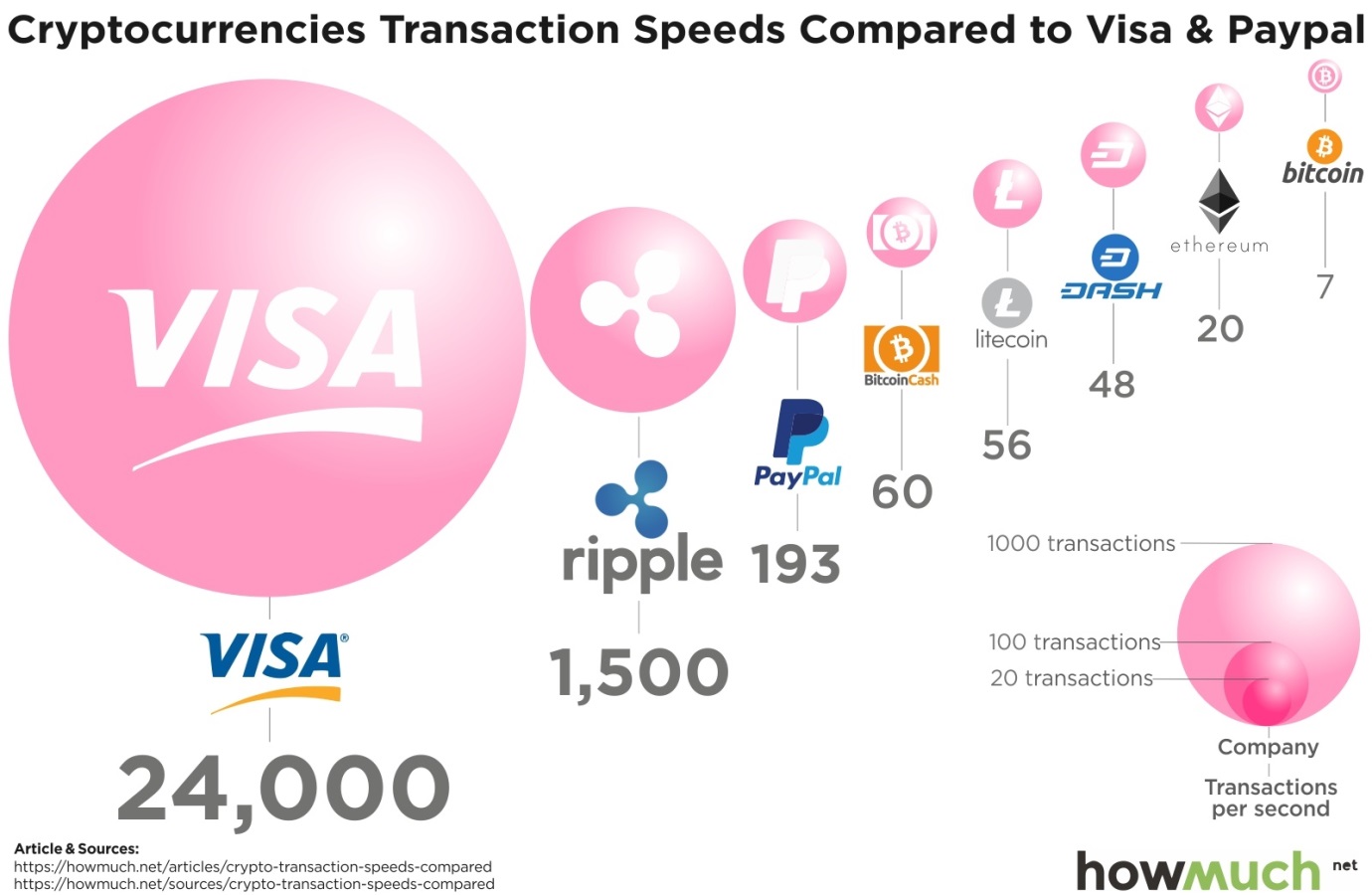
* 블록체인 방식을 활용한 온라인 투표시스템 적용 가능성 연구(http://www.electionstudy.kr/modules/bbs/index.php?code=research&mode=view&id=104&page=1&\_\_\_M\_ID=150&sfield=&sword=)

**2. 확장성을 고려한 구조를 설명하고 동작 방식에 대하여 설명하시오**

'확장성(Scalability)'은 블록체인 응용프로그램의 실현에 큰 문제가 되고 있다.

대부분의 블록체인 합의 프로토콜(Bitcoin, Ethereum, Ripple, Tendermint)에는 확장성의 한계가 존재한다. 이는 블록체인의 특징으로 부터 발생하며 네트워크에 참여하는 노드들은 모든 ‘트랜잭션(Transaction)’을 처리하여야 한다. 또한 하나의 노드가 전체 상태에 대한 복사본을 유지 해야 하는데 이러한 분산 합의 메커니즘은 강력한 보안과 중립성 및 신뢰성을 제공하지만 확장성을 보장하지는 못한다.

확장성이란 특정 자원이 투입된 양에 대해 얼마만큼의 성능이 향상될 수 있는지 나타내는 지표이다. 현재 비트코인의 트랜잭션 처리속도는 약 7 TPS 정도이다. TPS는 Transaction Per Second의 약자로, 초당 처리할 수 있는 트랜잭션의 수를 의미한다. VISA같은 서비스를 제공하려면 약 2000TPS 정도가 필요한데, public 블록체인 상에서 Dapp 제작에 막대한 영향을 준다.



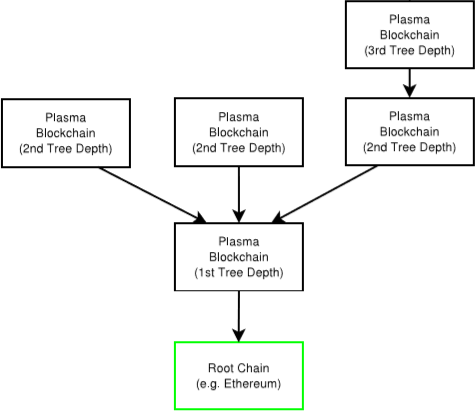
자료 : https://howmuch.net/

이를 해결하기 위해 다양한 확장성 솔루션들이 제시되어 왔고 캐스퍼, 샤딩, 라이덴 네트워크를 통해 설명 하고자 한다.(사실 왠만한 모든 블록체인들의 확정성을 고려하기 위한 방법들이 비슷하다고 생각한다.)

이런 다양한 확정상 솔루션들은 on/off-chain 으로 나눠지는데 대표적으로 off-chain에서는 플라즈마, on-chain에서는 샤딩으로 동작 방식을 예를 들어 설명 하고자 한다.

플라즈마

샤딩과 캐스퍼가 온체인(on-chain) 확장성 솔루션인 것과 달리, 플라즈마와 라이트닝 네트워크는 오프체인 확장성 솔루션이다. 기본적으로 플라즈마는 라이트닝 네트워크와 유사하다. 플라즈마의 전체적인 구조는 다음의 그림과 같다.



그림과 같이 플라즈마에서는 수많은 블록체인들이 트리 구조로 연결되며, 그 끝에는 루트 체인(이더리움 메인넷)이 위치해 있다. 여기서 A(화살표의 시작점) 체인이 B(화살표의 끝) 체인에 연결되어 있다는 것은 A 체인의 블록 정보가 B 체인에 담긴다는 것을 의미한다.

B 체인에 A 블록의 정보가 담길때 블록 헤더의 해시값만을 올리는 방법을 취한다. 위 그림을 예로 들면, Depth 3 체인의 여러 블록 헤더들이 Depth 2 체인의 트랜잭션 하나가 되고, 다시 Depth 2 체인의 여러 블록 헤더들이 Depth 1 체인의 트랜잭션 하나가 되는 식이다. 이러한 반복적인 과정의 결과, 루트 체인의 트랜잭션 하나에는 하위 체인의 수 많은 블록 정보들이 담길 수 있다. 플라즈마가 일차원적인 사이드 체인 구조가 아니라, 다차원의 트리 구조를 취하는 이유도 여기에 있다.

라이트닝 네트워크에서는 모든 트랜잭션을 메인 체인에 기록하지 않고 최종적인 결과만을 저장하여도 메인 체인에서 이를 신뢰할 수 있다.

이와 비슷하게 플라즈마에서도 차일드 체인의 모든 트랜잭션이 아닌 블록 헤더의 해시값만을 패런트 체인에 올리더라도, 루트 체인만 정상적으로 작동한다면 문제가 발생하지 않는다. 이것이 무엇을 의미하는지는 플라즈마의 동작 흐름을 통해 알 수 있다.

<플라즈마 동작 흐름>

체인 참여 시작(Deposit) → 플라즈마 체인 내부 프로세스(Transaction, Periodic Commitment) → 플라즈마 체인 참여 종료(Exit)

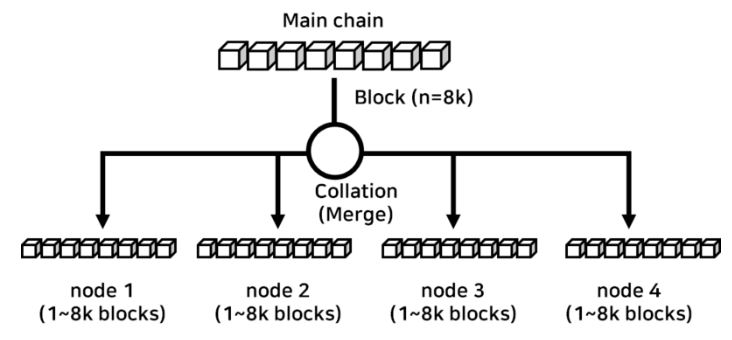
플라즈마의 동작 흐름은 플라즈마의 용어를 알아야 하므로 조금 복잡해 지지만 간단하게 예를 들자면 카지노를 연상하면 된다. 카지노에 입장해서 게임이나 기타 다른 것을 하기 위해 참여하기 위해서는 일정 금액의 현금을 카지노 화폐로 변경해야 하고 카지노를 빠져나오기 전에 돈을 잃거나 얻거나 하는 일련의 과정들은 중요하지 않고 빠져 나온후의 금액(현금)만이 결과값으로 저장한다는 개념으로 이해하면 쉽다.

샤딩

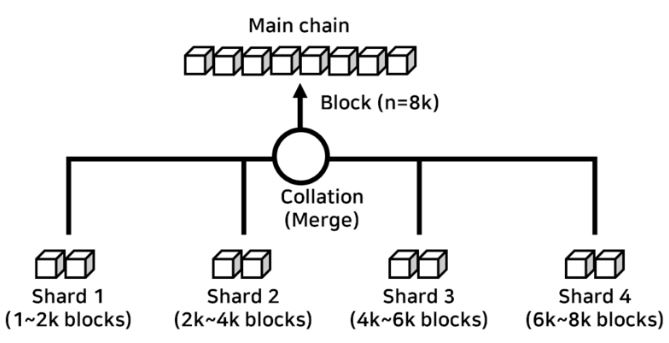
샤딩은 전체 네트워크를 분할한 뒤 트랜잭션을 영역별로 저장하고 이를 병렬적으로 처리하여 블록체인에 확장성을 부여하는 On-Chain 솔루션이다.

On-chain 솔루션이란 메인체인 자체의 프로토콜을 변경시켜서 메인체인의 성능을 향상시키는 방법을 말한다. 따라서, On-chain 솔루션을 적용하기 위해서는 메인 네트워크의 하드 포크가 필수적이다.

쉽게 설명하면 데이터를 샤드라는 단위로 나눠서 저장 및 처리하는 것이다. 샤딩 개념의 근원은 데이터베이스 샤딩에 있다. 데이터베이스 샤딩이란 대용량의 데이터를 처리하기 위해 테이블을 수평 분할하여 데이터를 분산 저장하고 처리하는 것이다.



이더리움 블록체인에서는 기존 n개의 블록을 바탕으로 새로운 블록의 유효성을 검사한다. 이 때 모든 노드에 기존의 블록들을 다 저장하게 하며 모든 노드들은 동일한 Transaction을 가지고 있게된다.



이더리움 샤딩에서는 메인체인이 처리해야할 블록을 쪼개어 샤드에 할당한다.

샤드에서는 주어진 조각블록에 대해 유효성 검사를 한다. 이후, 서로간의 연결을 통해 결과를 합치게 되고, 메인체인과 다시 연결을 하여 기존 블록체인에 온전한 블록을 연결한다. 메인체인에 집중된 계산량을 분배함으로써 트랜색션 초당 속도 처리에 이점을 얻을 수 있다. CPU가 하던 일을 GPU 를 통해 병렬 처리를 하여 속도의 이점을 얻는 것을 생각하면 간단하다.

참고자료

* https://howmuch.net/articles/crypto-transaction-speeds-compared
* https://brunch.co.kr/@curg/3
* https://medium.com/decipher-media/%EB%B8%94%EB%A1%9D%EC%B2%B4%EC%9D%B8-%ED%99%95%EC%9E%A5%EC%84%B1-%EC%86%94%EB%A3%A8%EC%85%98-%EC%8B%9C%EB%A6%AC%EC%A6%88-3-1-interchain-overview-8ed188d5b7d9
* https://medium.com/decipher-media/%EB%B8%94%EB%A1%9D%EC%B2%B4%EC%9D%B8-%ED%99%95%EC%9E%A5%EC%84%B1-%EC%86%94%EB%A3%A8%EC%85%98-%EC%8B%9C%EB%A6%AC%EC%A6%88-2-1-plasma-overview-7e6875f4c20d
* https://medium.com/decipher-media/%EB%B8%94%EB%A1%9D%EC%B2%B4%EC%9D%B8-%ED%99%95%EC%9E%A5%EC%84%B1-%EC%86%94%EB%A3%A8%EC%85%98-%EC%8B%9C%EB%A6%AC%EC%A6%88-4-1-sharding-%EC%83%A4%EB%94%A9-611a311c80e6