Blockchain

Blockchain's limitation

Prof. Byung Il Kwak

Outline

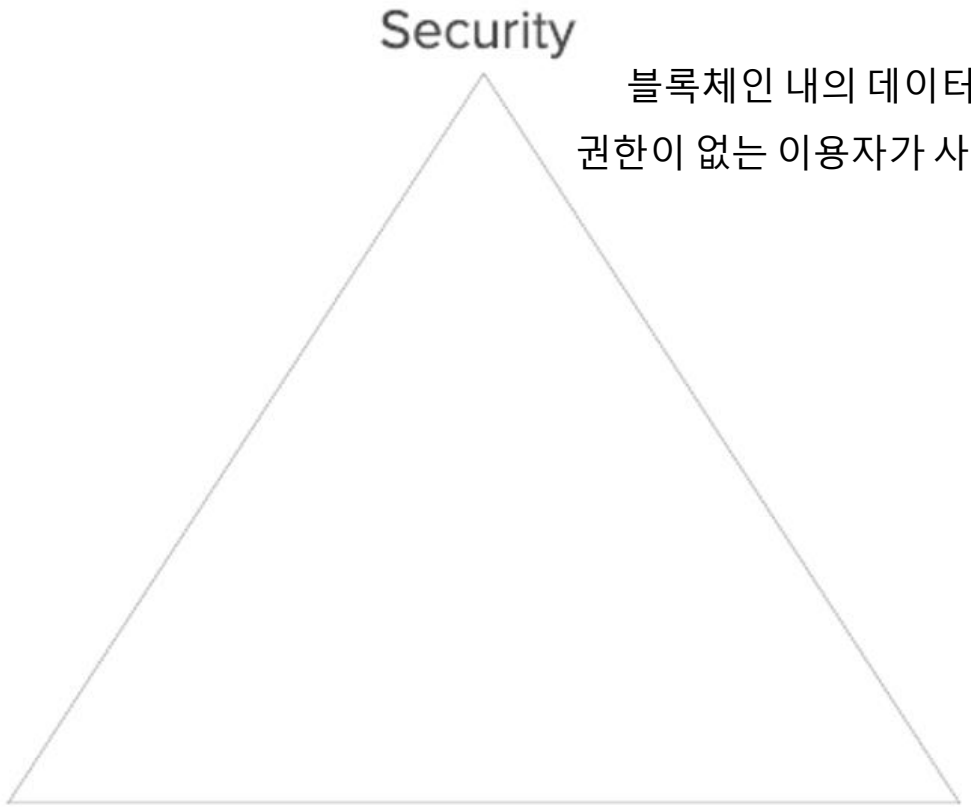
- Blockchain Trilemma
- PoW-based Blockchain's Scalability
- Sidechain
- Research Areas

Blockchain Trilemma

- 블록체인 확장성

Blockchain Trilemma

- 블록체인 확장성



블록체인 내의 데이터나 프로그램을
권한이 없는 이용자가 사용 할 수 없도록 함

중앙 집중화를 벗어나 분산된 소규모
단위로 자율적으로 운영

사용자 수의 증대 및 거래 증가에 따라
유연하게 대응할 수 있는 정도

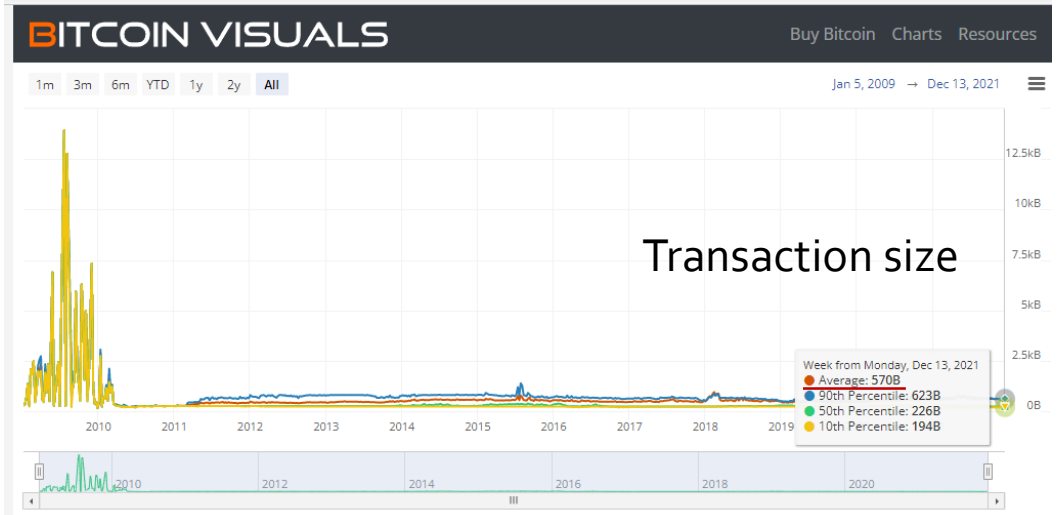
Blockchain Trilemma

- 비트코인 TPS (Transactions Per Second)
  - Transaction당 평균 570 byte 크기
  - 비트코인 1개 블록크기 is 1 MB
    - 1개 블록에 대한 트랜잭션 수

      = 1024 x 1024 / 570 = 1,839.6개
  - 평균 10분에 블록 1개 생성

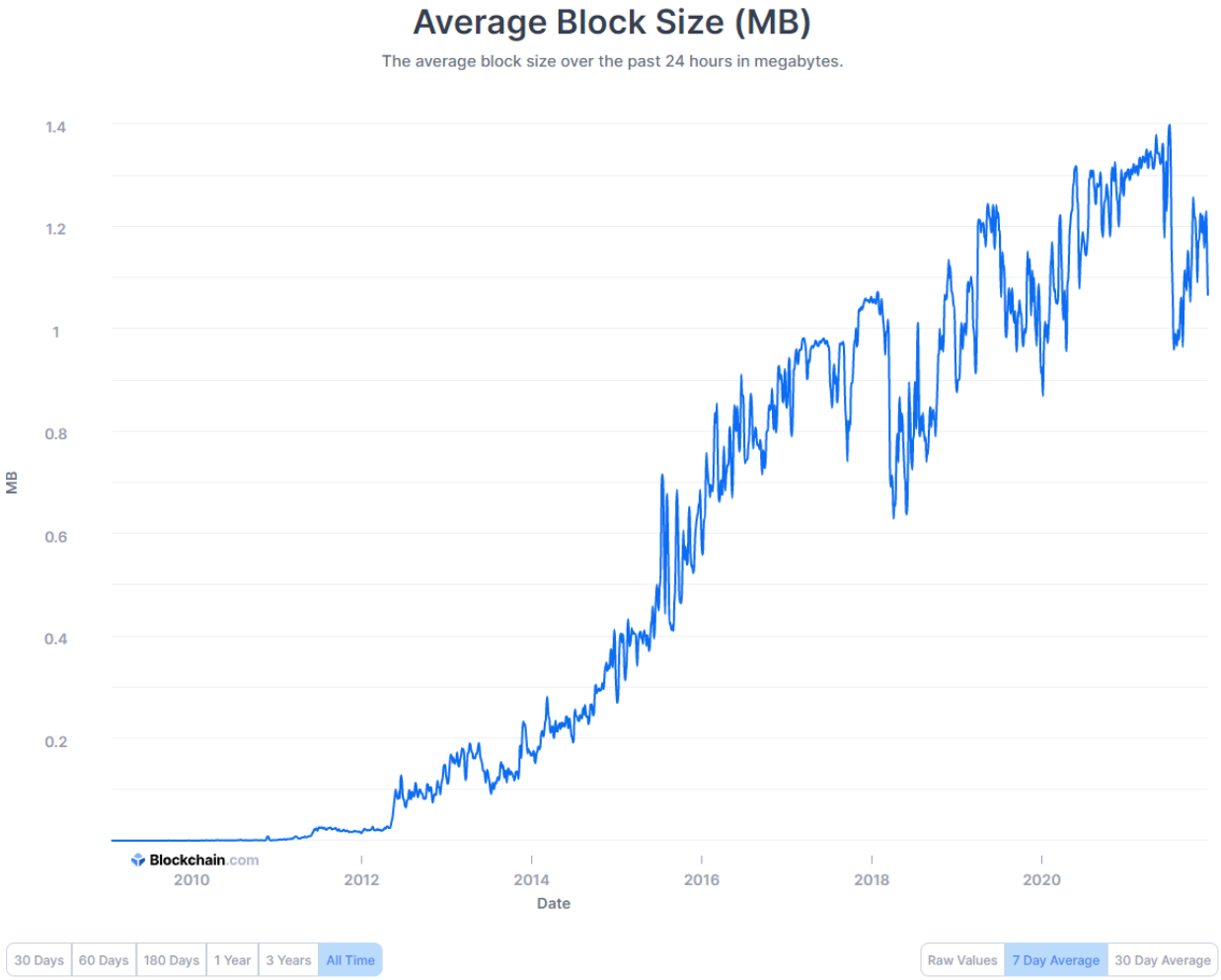
    600 초 : 1 블록에 대한 트랜잭션 수 = 1 초 : X TPS

    → ***3.066 TPS***



Blockchain Trilemma

- Bitcoin's average block size



https://www.blockchain.com/ko/charts/avg-block-size?timespan=all&daysAverageString=7

Blockchain Trilemma

- 다른 지불 시스템과의 비교

	Average	High Load / Maximum
Bitcoin	3 tps	3.2 tps
PayPal*,**	150 tps	450 tps
VISA***	2,000 tps	56,000 tps

Blockchain Trilemma

- 합의 알고리즘 변경에 따른 TPS 성능 향상
  - PoW: Bitcoin, Ethereum
  - PoS: Ethereum (after PoS update)
  - DPoS: EOS
  - PBFT: HyperLedger
  - FBA: Stellar
  - 하지만, 토큰, 기능, 사용자 수가 증가하게 되면 미래에 병목현상이 발생할 수 있음
    - 예) IPv4 주소 할당 => IPv6 주소 할당

PoW-based Blockchain's Scalability

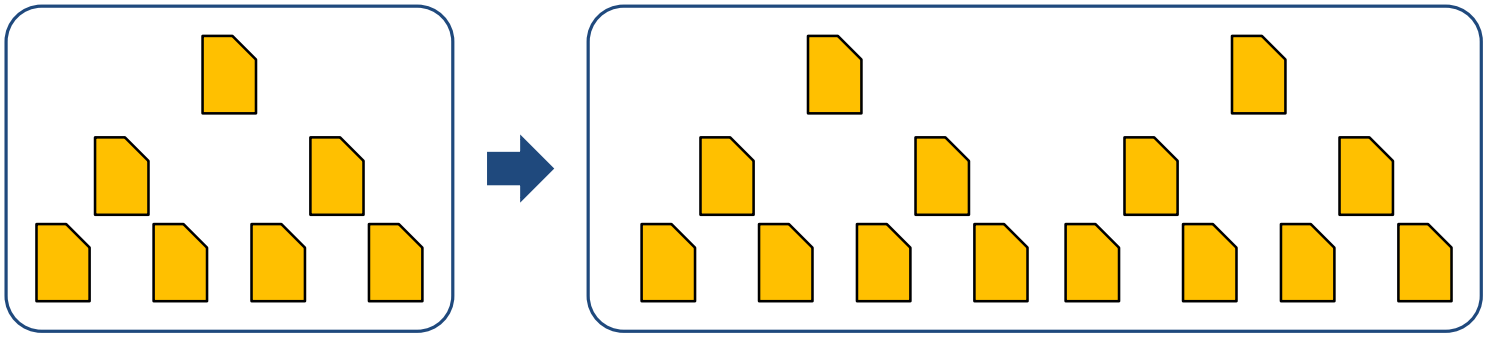
- Solutions - 1
  - PoW 난이도 조절을 통한 블록 생성 속도 향상

Time to broadcast block fixed while Block creation time decreases

- 발생 가능한 문제점: 생성 주기가 짧아지는 것으로 인해 전파시 문제가 발생할 수 있음
  - 이더리움에서는 GHOST 프로토콜을 사용하여 무효 블록(엉클)도 유효 체인을 결정하는데 포함시킴
    - 다만, 이더리움이 PoW에서 PoS로 전환하게 되면 무의미해질 수 있음 (채굴이 필요 없고, 즉각적으로 트랜잭션이 종결됨)

PoW-based Blockchain's Scalability

- Solutions - 2
  - 블록 크기 증가를 통한 더 많은 트랜잭션들을 포함



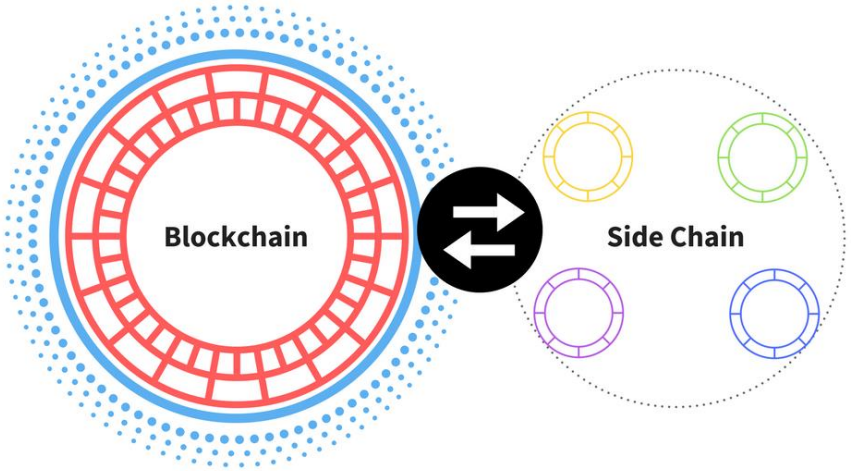
Block size 1MB

Block size 2MB

- 발생 가능 문제점
  - 하드 포크 (모든 채굴자가 동의해야 함) 필요
  - 스토리지 크기 증가
  - 블록 전파하는데 있어 시간이 오래 걸림

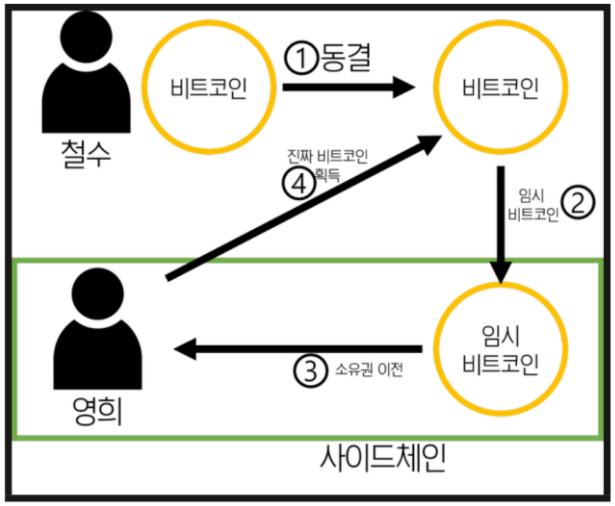
Sidechain

- 사이드체인은 메인 블록체인과 함께 다수의 사이드체인을 운영함으로써 간접적으로 확장성을 향상시킬 수 있는 방법



Sidechain

- 사이드체인 단계 구성
  - Part 1- sending.
    - 사용자는 자신의 코인을 **특정 주소로 전송**
  - Part 2 - waiting for confirmation.
    - **자산 보호**를 위해 확인 대기
  - Part 3 - using a new sidechain.
    - 확인이 되고 나면, 대기 중인 코인은 사이드체인에서 해제됨



Sidechain

- Advantages
  - 유연성
    - 사이드체인을 통해 거래 속도를 향상시킬 수 있으며, 다양한 암호화폐들을 거래할 수 있음
  - 실험 가능성
    - 핵심 소프트웨어 업데이트 또는 블록체인 관련 소프트웨어를 테스트하는데 사용할 수 있음
- Disadvantages
  - Security issues
    - 비트코인 블록체인과 마찬가지로 사이드체인은 공격으로부터 보안성을 유지하기 위해 채굴 작업이 요구될 수 있음
    - 충분한 힘이 없다면, 사이드체인 역시 공격에 취약할 수 있음
      - 다만, 사이드체인만 공격 당하게 될 경우, 메인 체인은 그대로 유지될 수 있는 장점을 가짐

Research Areas

- Consensus Algorithms
  - PoW, PoS, DPoS, PBFT, PoET, …
- Blockchain Security
  - 51% Attack, Mining Pool Attack, …
- Smart Contract Security
  - Code Formal Verification
  - Symbolic Execution
    - Oyente, Mythirl, …
- Scalability
- …

References

- EE817/IS893: Blockchain and Cryptocurrency @KAIST

Q & A