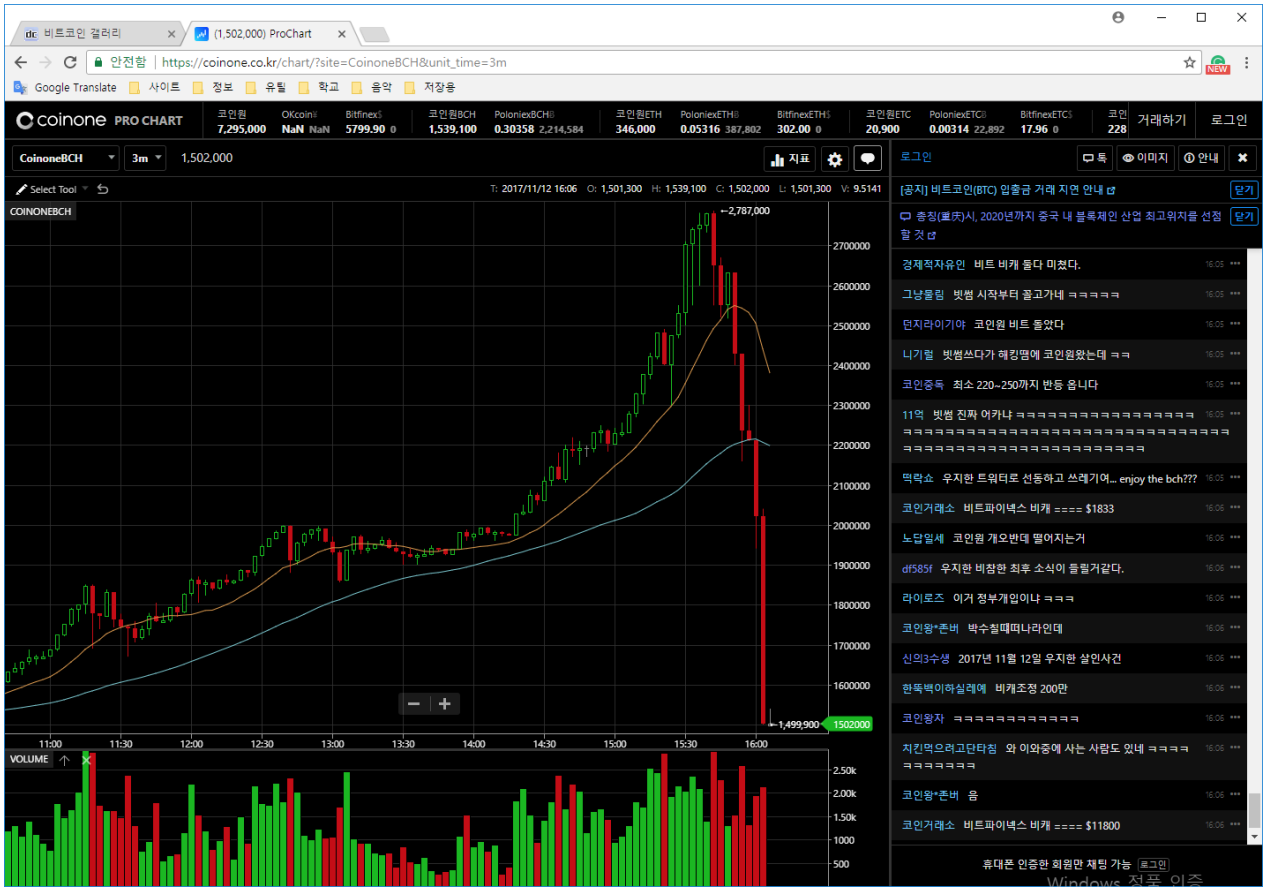
BTC와 BCH를 보며 느낀 탈 중앙화에 대한 단상

이번 글은 투자 목적도, 이윤 추구도 아닌 그냥 순수하게 제3자 입장에서 살펴본 **비트코인/비트코인캐시 vs 블록체인** 내용이다.



최근(17.11.12)에 있었던 BCH 폭등 후 정말 어느 한 순간에 있었던 폭락 그래프 ~~지옥으로 가는 불꽃열차~~ 이다. 사실 저 순간을 지켜보고 있었던 사람으로써 "진술"하자면, 285만원을 찍는 순간 뭔가 이상한 기운이 감지됐고, 그 짧은 순간(약 몇 초?)에 285만원이 180만원대가 되어 있었다. ~~ㅎㄷㄷㄷㄷ~~

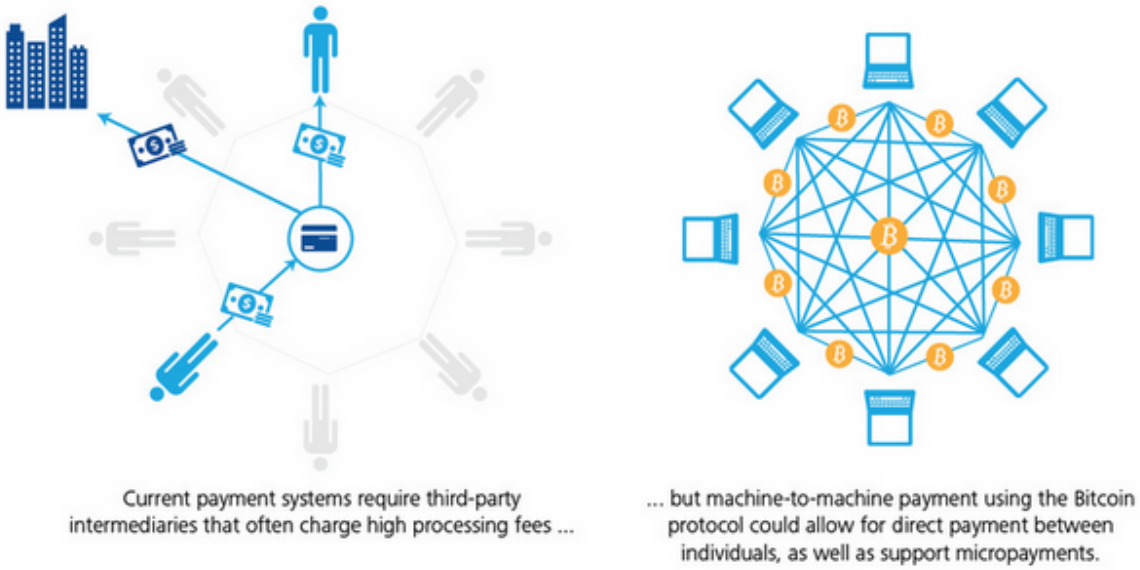
알고보니 빗썸 사이트가 순간적으로 터졌던 것이고, 이에 따라 대규모 폭락사태가 이루어졌던 것.. 관련기사 (사실 빗썸 폭파? 사건은 지난 8월에 있었던 BCH 대규모 펌핑 때와 너

무도 동일한 모습을 지니고 있다.. 관련기사)

사실 밖에서 투기 목적으로만 바라보면, 이 사태는 단순하다. 제동장치 없는 가상화폐 투기 시장에서 큰손들과 개미들의 싸움, 그리고 늘 그랬던 것처럼 개미들의 처절한 패배..

근데 이면에는 좀 독특한 성질이 있다.

블록체인



블록체인의 개념에 대해서야 워낙 요즘 핫한 시스템이기 때문에 대부분 알 것으로 생각하고.. 간단히 요약하자면 서버-클라이언트 구조가 아닌 P2P 환경에서의 공통 장부를 이야기한다.

깊이 들어가면 어려우니.. 그냥 모든 네트워크의 노드들이 동일한 영향력을 가지고 참여하는 분산 네트워크라고 보면 된다.

예를 들어 하나카드에 기록되고 처리되는 나의 신용카드 처리는 하나카드와 그에 딸려있는 VAN 사 등의 시스템에서만 처리/보관되지만 블록체인은 모든 사람들이 나의 이력과 처리에 대해서 관여하고 승인해줄 수 있다고 보면 된다.(물론 실제 기술적으로는 조금 다르지만..)

- 블록체인 - 위키피디아
- 사토시 나카모토 논문 -Bitcoin: A Peer-to-Peer Electronic Cash System

블록체인의 의미

기술에 대한 상세한 이해도 중요하지만 의미를 깨치는 게 더 중요한 법. 블록체인의 가장

큰 의미는 탈 중앙화라고 모두가 평가한다. 서버-클라이언트 구조는 사실 서버를 trusted boundary 라는 assumption을 대부분 전제로 삼고 있다.

설마 내 요금제를 맘대로 바꿨을까, 설마 내 이메일을 맘대로 삭제했을가, 설마 내 카드 청구대금을 맘대로 바꿨을까..

즉. 통신요금제/인터넷포털/카드/은행 등의 “서버들”은 믿을 수 밖에 없는 존재들이고 굉장히 폐쇄적인 모양새를 갖출 수 밖에 없는데, 블록체인은 이를 근본적으로 깨는 시스템이다. 그리고 이것은 **블록체인의 영향력을 극히 감소시키는 근본적인 원인** 이기도 하다. 양날의 검..

예를 들어, 삼성카드의 모든 transaction을 하나카드와 공유할 수 있을까? 절대 불가능하다. SK텔레콤이 그들의 통신망을 임대해서 사용하는 알뜰폰 사용자들에게 모든 데이터를 공유할 수 있을까? 절대 불가능하다.

즉, 기득권 및 카르텔을 갖춘 조직에서는 블록체인을 사용하는 것이 굉장히 불가능한 일이다. 정보의 불균형을 통해 권력을 유지하고 있는데 이를 “탈중앙화” / “분산화” 한다는 것은 불가능하며, 블록체인은 이 부분에 있어 역설적으로 각광을 받는 존재이유를 가지고 있다고 본다.

비트코인의 성장과 비트코인캐시의 탄생

비트코인이 지속적으로 가파르게 성장하면서 가장 큰 문제가 되었던 것은 블록사이즈이다. 블록 안에는 트랜잭션 (그냥 데이터라고 하자)들이 있는데 거래량이 폭증하면서 이를 처리하지 못하는 문제였다.

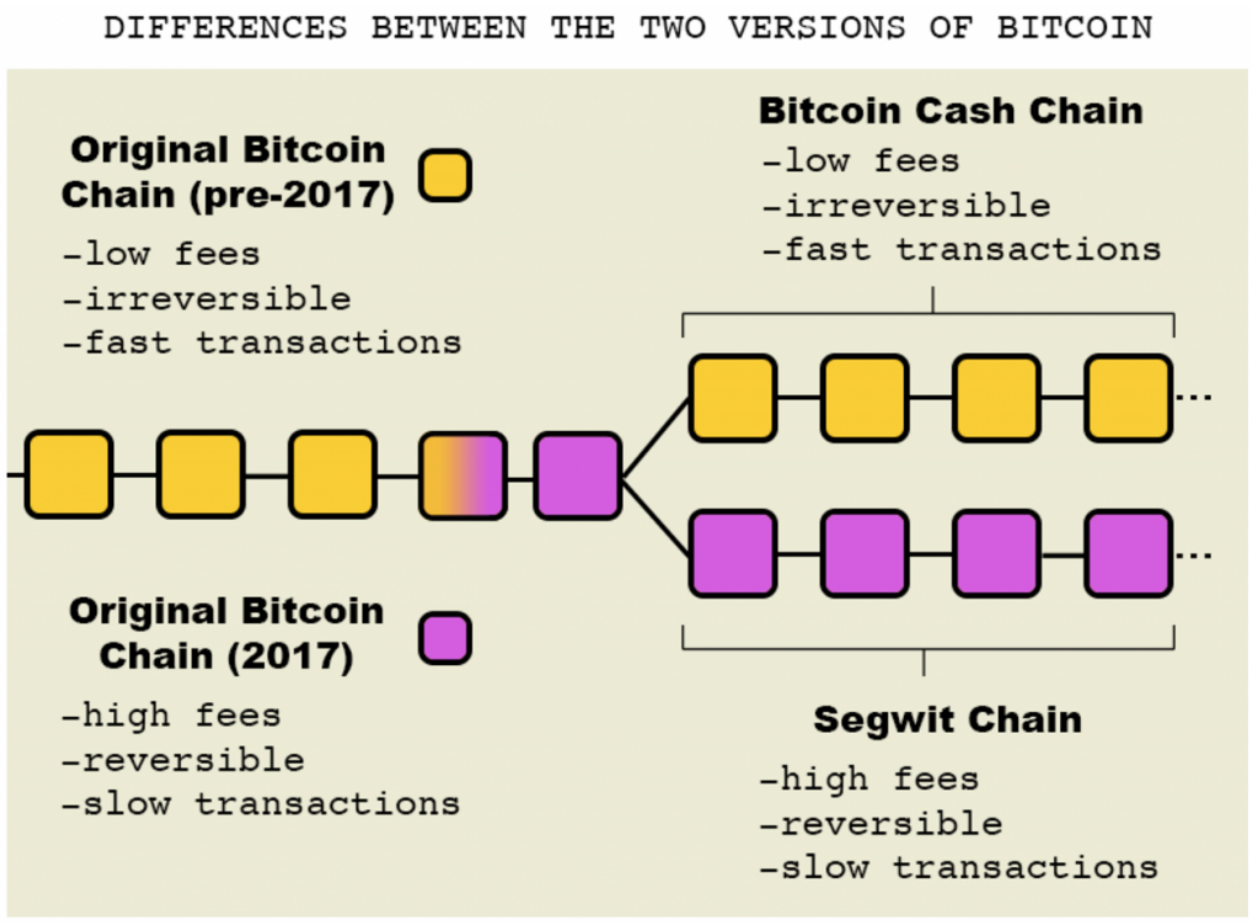
즉, 1MB의 블록 안에 보통 250byte 정도의 데이터가 담기니 대략 한번에 4000개 정도를 처리할 수 가 있는데 점점 데이터 량이 폭증하니 데이터가 처리되지 않고 큐에 쌓여있는 것이라고 보면 되겠다.

이는 블록체인 네트워크에 많은 악영향을 주는데, 우선 수수료가 올라간다. 비트코인은 수수료가 높은 애들을 먼저 처리해주기 때문에 수수료가 계속 상승을 할 뿐 아니라, 처리가 지연됨에 따라 비트코인의 확장성(결제 연동 등)에 심각한 악영향을 주는 것은 맞다.

그래서 총 2가지의 개선방안이 있었는데 하나는 블록사이즈를 임시적으로 늘릴 수 있는 segwit(seperated witness)와 블록사이즈를 2배로 늘리는 segwit2x 방안이 논의되었다. 결론적으로 **segwit은 default, 2X는 논의대상** 이었다고 보면 되겠다.

segwit은 쉽게 말해, 모든 데이터에 서명을 붙이는 기존 방식에 비해 서명값을 분리해서 따로 보관하는 방식을 이야기한다. (블록 안에 서명값이 포함되지 않으니 그 여유분으로 트랜잭션을 더 채우겠다는 거..)

길고 긴 논의 끝에 segwit 찬성파와 반대파의 갈등으로 인해 비트코인을 17년 8월 1일자로 쪼개기로 한다 - bitcoin hardfork. 이것이 비트코인 캐시의 시작이다.



비트코인캐시의 의미

이게 겉으로 보면 기술적인 논쟁 같지만.. 사실은 지극히 돈의 논리가 가득한 분쟁의 결론이다.

ASIC BOOST와 우지한

위 그림에서와 같이 segwit은 블록체인, 조금 더 구체적으로는 머클트리를 구성하는 방식 자체가 바뀐다. 기술적으로는 충분히 커버할 수 있는 문제이나, 반대 논리의 핵심에는 ASIC이라는 게 있다.

Application Specific Integrated Circuit, 즉 ASIC은 주문형 반도체로써 특정 연산을 굉장히 빠르게 할 수 있도록 해주는 반도체이다.

문제의 핵심은 여기서 잘 살펴볼 수 있다 - ELI5: Gregory Maxwell's Inhibition Proposal

상기 제안의 핵심은, ASIC을 사용하지 말도록 하자는 제안이다. 이게 왜 중요하냐면..

Bitcoin의 블록헤더 구성은 아래와 같다.

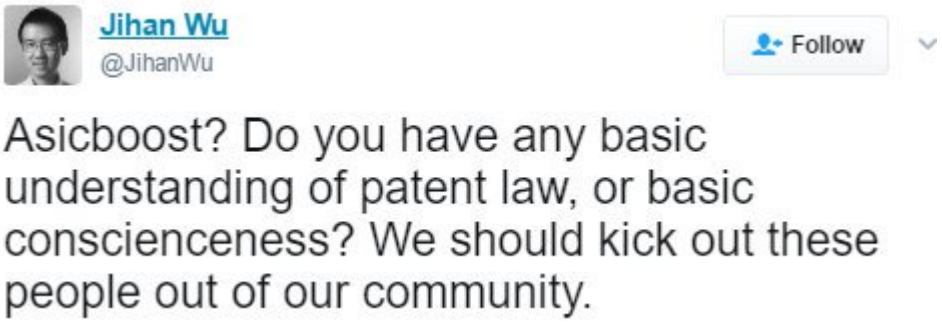
- Bitcoin block header(80 byte) = 64byte data + 16byte data
- 64byte data = 이전 블록해시(32byte)+ 트랜잭션 지문 version(4byte) + merkle root (32byte중 28byte)
- 16byte data = Merkle Root(4byte) + 타임스탬프 (4byte) + bits (4byte) + Nonce (4byte)

여기서 취약점이 발생하는데, 원칙대로 블록을 계산해서(해싱해서) 값을 도출하는 게 아니라.. 1) timestamp와 nonce는 그냥 임의로 정해두고 2) bits 값은 retargeting 하는 시점에 정해지면 남은 것은 머클루트 4 byte인데. 3) 이것을 미리 쭈루룩 계산해둔 뒤 값을 끼워맞추는 형식으로 올바른 해시값을 계산해낸다는 것이다.

이렇게 하면, 동일한 HW에서 계산하는 것보다 30% 이상 더 빠르게 블록값을 **채굴** 할 수 있다고 한다. 그리고, **segwit은 이러한 ASIC BOOST를 쓸 수 없다는 것** 이 가장 중요 포인트였다.

즉, 채굴자 진영에게 segwit은 굉장히 짜증나는 존재였으며, 이유는 블록채굴 성공시 25 BTC가 주어지는데.. 최근 1 BTC가 8백만원 정도임을 생각해보면… 어마어마한 금전적 손실을 가져오기 때문이다.

이 문제에 대해서 채굴자 진영의 대표, 중국의 우지한은 아래와 같이 응대했다. ~~찔리냐.. 말하는 꼬라지 하고는..~~



비트코인캐시의 성장과 전략

위에서 언급했던 것처럼, 블록사이즈 제한으로 인해 발생하는 문제를 해결하고자 하는 것이 비트코인캐시의 ~~명분상으로만 존재하는~~ 전략이다.

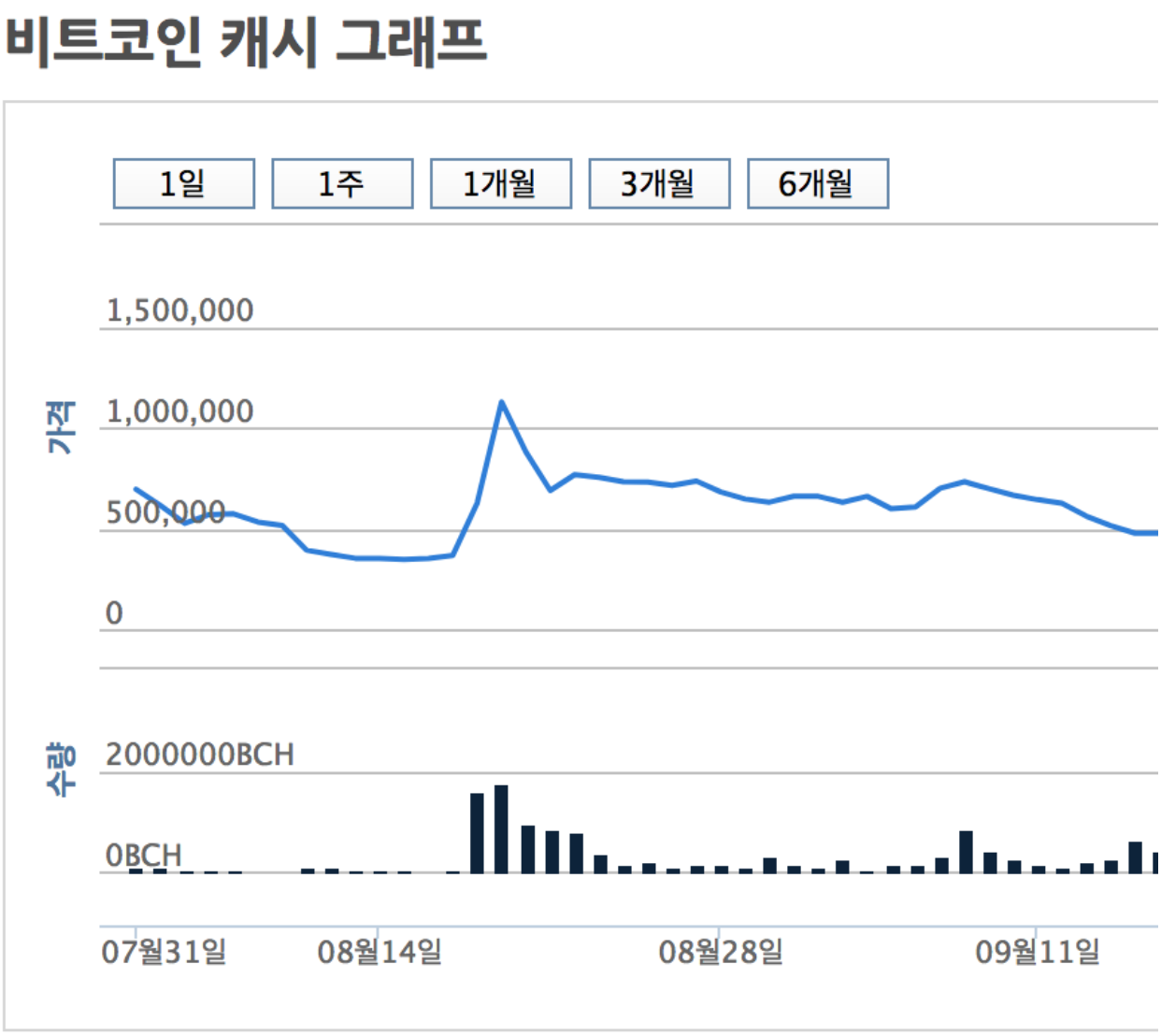
이를 통해 결제시스템에도 연동을 쉽게 할 수 있고 bitpay에서 bitcoin cash를 결제수단으로 제공 블록 사이즈도 8M로 늘려 처리 지연 등의 문제가 없다.

하지만.. 가장 중요한 점은 바로.. **ASIC을 그대로 쓸 수 있다** 는 점일 것이다.. 블록사이즈 증가 외에 로직 자체는 변경된 것이 전혀 없다는 것이며. 이 점이 bitcoin core 개발자들의 가장 큰 반발을 사는 지점이기도 하다.

별다른 차별점도 없이 그저 돈만 보고 비트코인에 묻어가려는 (그리고 네이밍도 bitcoin을 포함한) 블록체인 정신에 아주 어긋나는 crypto currency라는 주장이다.

참고로 비캐는 출시되고 나서 60만원대를 유지하다가 30만원 중반대를 유지 중.. 8월 중순

(17일쯤으로 기억하는데..) 2일 연속 100%의 역대급 펌핑을 보여주며 이목을 끌기 시작한다.



비트코인캐시 하드포크 - BEFORE

화려하게 등장한 이후, 비트코인캐시는 끝없는 추락에 추락을 거듭하게 된다. 이유는 단순하다. 특색이 없으니까..

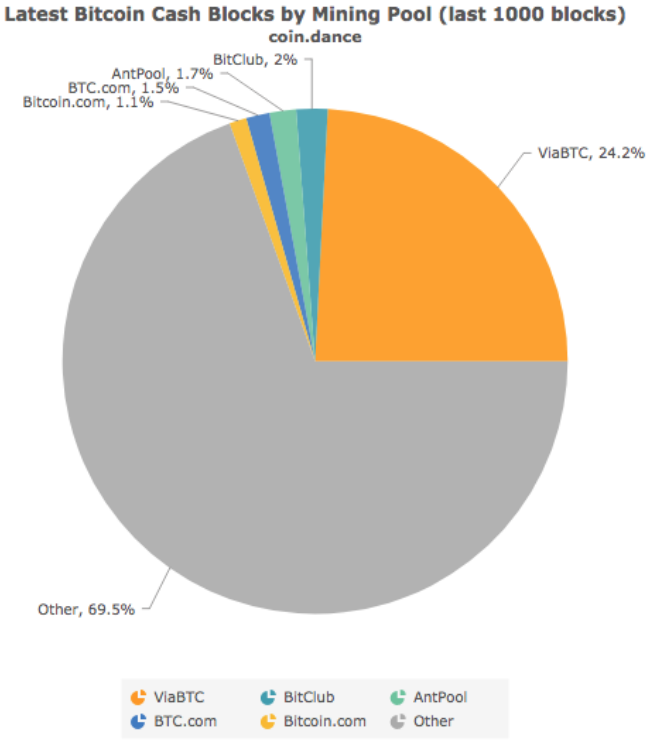
비트코인 위에 라이트닝 네트워크를 얹어서 결제를 빠르게 하겠다는 라이트코인이나 송금에 특화된 리플, 익명성이 강조된 대시 등 메이저 코인에 비해서 비트코인캐시가 내세울 수 있는 강점은 전혀 없었다. ~~그럼에도 난 계속 물려있었다.. 뭔가 돈이 될 거 같아~~

특히 가장 문제가 되었던 점은 들쭉날쭉한 해시파워와 그에 따른 안정성에 대한 문제였다. 그 근본적인 이유는 **비트코인 채굴 마이닝 풀과 비트코인캐시 채굴 마이닝풀은 다르지 않다** 는 점 때문이다.

즉, 채굴자집단에서는 돈 되는 애를 캘 뿐인 것이다.

예를 들어 채굴자 입장에서는 1) 비트코인의 채굴 난이도와 가격을 비교해보고, 2) 비트코인캐시의 채굴 난이도와 가격을 비교해본 후 더 돈 되는 애를 캐면 되는 것이다.

따라서 어느 정도 안정화(균형)가 된 비트코인과 다르게 비트코인캐시는 도대체 누가 캐는지도 모를만큼 문제가 많았고 (아래 사진은 17년 8월 21일자 채굴현황)



특히.. 1) 채굴을 한다 2) 난이도가 올라간다 3) 채굴이 힘들어지는데 가격은 싸다 4) 채굴 안한다 (비트코인으로 이동이동) 5) 난이도가 내려간다 6) 채굴이 쉬워져서 막 캐진다 (비트코인캐시로 이동이동)

이따위 짓들을 일부러 했기 때문에 비트코인캐시의 신뢰도는 땅으로 떨어져 있었다. 조금 더 기술적으로 설명하자면, 비트코인캐시는 EDA(Emergency Difficulty Adjustment)라는 난이도 조정 알고리즘을 추가해 **12시간 동안 6개 블록이상 채굴되지 않으면 채굴 난이도를 20% 낮추는 방식을 사용** 했었다. 즉, 블록이 오랜 시간 제대로 채굴되지 않으면 자동적으로 쉽게 블록이 채굴되도록 바뀌는 것이다.

그리고 하드포크는 이러한 EDA를 제거하고 새로운 난이도 조정 알고리즘을 적용하는 것이 주된 목적이었다. 뉴스 링크

~~디게 reasonable 해 보이지만, 굉장히 전략적인 돈에 대한 접근이라는 거..~~

비트코인캐시 하드포크 - AFTER

결국 새로운 DAA(Difficulty Adjustment Algorithm)이 11월 13일에 적용되는가 했는데.. ~~난 솔직히 이 타이밍을 기다리고 3개월을 졸버하고 있었다~~

그 전에 대규모의 펌핑이 시작되었다. 그게 바로 도입부에 보여줬던 그 지옥으로 가는 불꽃 열차의 시발점이었던 것이다. 이 코인판에서 전무후무할 펌핑이 필요했던 이유는 단순하다. 비트코인캐시의 채산성을 비트코인 수준 또는 그 이상으로 맞추기 위해서 (== 마이너들을 **안정적으로** 끌어오기 위해서)

비트코인캐시 펌핑 원인

아래 사이트를 보자

- https://fork.lol/

중요한 지표가 나오는데, DARI(Difficulty Adjusted Reward Index) 즉 채산성 지표는 아래와 같이 계산된다.

```
(block coinbase+fees in satoshis) / (block difficulty)
```

이걸 맞추기 위해서는 결국 난이도가 올라가더라도 `exchange rate in USD` 즉 가격이 올라가야 하는 이슈가 발생하는 것이다. 이걸 비트코인과 레벨을 맞추려면 최소한 110만원 (당시 70KRW/BCH) 정도가 필요했었다.

난이도가 올라가는 것은 네트워크의 안정성이 높아진다는 것(계산을 많이 해야 한다는 뜻이므로) 이고, **채굴자들을 끌어들인다는 것은 그만큼 돈이 되어야 한다** 는 것인데 이걸 둘 다 높이기 위해서는 대규모의 펌핑은 불가피했다.

그걸 누가? **우지한** 진영에서 진행한 것으로 보여진다.

중요한 것은 채굴진영의 대표자인 우지한 진영은 이러한 짓을 할 수 있는 거의 유일무이한 존재이다. **비트코인도 엄청나게 가지고 있으면서(자금력), 본인이 채굴업자이면서(비트코인 네트워크 최대 채굴진영), 비트코인캐시의 창시자이기도 한 사람** 은 전 세계에 우지한 한 명이라고 알려져 있다.

펌핑 과정과 이후, 그리고 의미

~~거의 막바지다. 조금만 쓰려고 했는데 글 디게 길어졌네~~

펌핑은 위에서도 얘기했던 것처럼 전무후무한 역대급 펌핑이었으며, 그 말로는 매우 비참했다. 그 시간에 1분 단위로 현황을 보고 있었던 현장 목격자로써 얘기하자면. 아 지옥에 아수라장이 있다면 이런 모습이겠구나 할 정도로 탐욕과 혼란의 그 자체였다. (물론 나도 ㅋㅋㅋㅋ ~~더 오르나! 더 오르나!~~)

비트코인캐시의 펌핑으로 인해 비트코인과 자리를 맞바꿀 것이라는 억측 BCH/BTC 비율이 0.5 이상 갈 것이라는 예측 등 꿈과 환상이 가득한 모험의 나라였다. 실제로 비트코인닷컴의 주인이자 비트코인의 예수?? 라고 불리는 로저 버가 25,000개의 비트코인을 이동시키면서 **비트코인 가격을 반토막 낼 것이다** 라는 억측도 많았다.

(8백만원 x 25,000개를 한번에 팔게 되면 2천억원의 물량이 한번에 나오는 것이므로…)

로저 버의 비트코인 지갑 이동

당연히 그런 일은 벌어지지도 않았고, 한걸음 떼서 보면 말도 안되는 주장이었지만 투자 게시판에는 난리가 나고 말도 안되는 선동이 난무했다.

가격을 떠나, 결국 하드포크는 무사히 완료가 되었다. 개인적으로 나는 이 하드포크의 의미를 DAA 조정이 아니라 **비트코인캐시가 비트코인 목에 개목걸이를 걸었다** 고 평하고 싶다.

즉, 정해진 마이닝 풀을 이용하여 **가격 정책에 맞게 비트코인에 붙었다가 비트코인캐시에 붙었다 왔다갔다를 기존과는 다르게 안정적으로 진행하겠다** ~~이돈도 저돈도 다 내꺼!!~~ 가 우지한에 의해 완성되었다고 평하고 싶다.

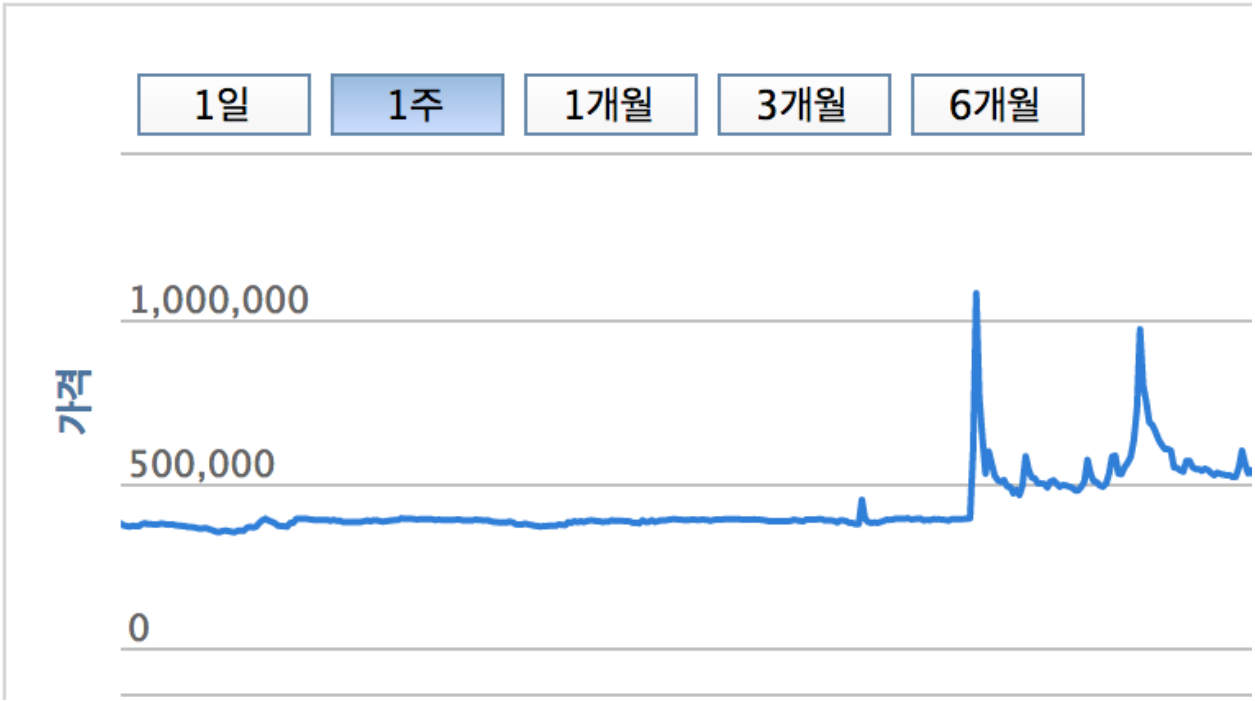
이러한 혼돈과 탐욕이 넘치는 곳에서 과연 블록체인이 이야기하는 탈중앙화, 탈집중화와 권력 분산이라는 것이 가능할까? 오히려 지금의 흐름은 가상화폐가 지녀야 할 가치보다는, 그리고 블록체인이 그려나가야 할 그림과 정 반대로 나아간 것이 아닌가 라는 체념만이 가득해져버렸다.

ASIC기반의 마이닝풀이 불가능한 equihash라는 것이 비트코인골드에 포함되었다고 한다. Equihash 참고링크 하지만 이것을 보면서도 그러면 메모리를 많이 가진 또다른 권력을 창출하지 않을까? **과연 탈중앙화라는 것이 근본적으로 가능한 문제인가?** 라는 물음을 가질 수 밖에 없다.

모네로, dash 폭등

아래는 비트코인캐시의 역대급 펌핑 이후의 dash 폭등 그래프이다. 30만원 정도 하던 놈이 갑자기 순간적으로 100만원을 넘어섰다.

대시 그래프



그리고 모네로, zcash까지 총 3개의 코인이 순식간에 폭등을 하는 기 현상을 보여줬다.

이에 대해서는 “추측상으로” 빗썸 서버 폭발?? 사태로 인한 기현상이라는 의견이 있다. 참고링크

나는 이것이 굉장히 일리있다고 보는데, 이유는 **세 코인 모두 익명성을 강조한 코인** 이다. 뭔가 숨기고 싶다는 뜻이다. (비트코인은 익명성이 보장된 거 아니냐고 할 수도 있지만, 그 부분은 차치하고…)

즉 뭔가 몰래 돈을 빼야 하는데, 그걸 걸리기 싫고 또 싼 값이 빼긴 싫으니 일단 엄청난 펌핑을 하고 손해를 보지 않는 선에서 큰 손들의 돈이 빠져나간 거 아닌가 하는 추측은 일리가 있어보인다. 실제로 그 이후에 대규모 펌핑은 없었고, 두 번째로 개인적으로 빗썸에 대해서 좀 의구심이 있었는데 (이런저런..ㅋㅋ) 저 펌핑은 모두 빗썸을 통해서만 이루어졌다.

~~그래서 나는 업비트로..~~

coin dance / fork.lol

글이 길었지만, 결론적으로 비코와 비캐는 뭔가 역학관계를 이번 하드포크를 통해서 기술적으로 달성했고, 그 목적은 돈에 있음은 두말할 나위가 없다.

그리고 그걸 행할 수 있는 자는 “알려진 바에 의하면” 우지한 한 명이고, 정해진 마이닝 풀을 이리저리 옮기면서 최적의 가격에 채굴한 비트코인 또는 비트코인캐시를 팔 것이다.

그리고 거기에 달라붙은 개미들은 혹시 1% 라도 먹기 위해 달려들 것이고…

- https://cash.coin.dance/blocks
- https://fork.lol/

위 두 사이트를 가보면(특히 첫 번째) 현재 마이닝 풀들이 어느 체인에 달라붙어 있고(채굴하고 있고), 또 상대적인 이득이 어느 정도 인지 한눈에 보인다.

이론적으로 난이도는 높은데(채굴이 어려운데), 안정적으로 마이닝풀들을 데리고 있으면 가격은 높게 책정이 되기 시작한다. 가치가 인정 받아지는 것이므로. 물론 실제 코인판에서는 이러한 이론과는 무관하게 세력과 큰 손들에 의해서 가격이 출렁이지만 이번 하드포크로 인해서 어느 정도 예측할 수 있는 기준점은 마련이 되었다고 본다.

문제는. 예를 들어 **비트코인을 캐는 게 유리한 시점이라고 한다면 가능한 시나리오는 늘 두 가지** 가 된다. **비캐 가격을 높이거나(이리로 붙거라!!), 비트코인 가격을 덤핑하거나(거기서 떨어져라!!).**

하지만 개목걸이의 효과로 인해, 중장기적 관점으로 보면 비트코인과 비트코인캐시는 함께 가치가 상승하지 않을까 싶다. 정보의 불변성을 기반으로 하는 비트코인이 금의 역할을, 낮은 수수료와 빠른 전송을 기반으로 하는 비트코인캐시가 USD의 역할을 가져가는 게 최종 목표일 것으로 보인다.

예측 상으로, 저렇게 계산을 해보면 현재 800만원 대의 비트코인 가격대비 비트코인캐시의 적정가격은 대략 110만원~130만원 정도 되지 않을까 싶은데 그건 순전히 그냥 추측.. ~~며느리도 몰라!!~~

결론

글이 좀 중구난방으로 길어졌지만, 결국 블록체인 기술 그 자체에 관심이 있었고 또 그것들이 이루고자 하는 이상향에 대해서 굉장히 민주적인 (실제로 IBM의 블록체인 기반 IoT 플랫폼인 ADEPT의 캐치프레이즈는 Device Democracy이다 - 링크) 방법으로 구현하고자 하는 접근방법은 나에게 큰 감명을 주었지만.

실제로 기술의 지향점과 다르게 “돈”과 인간의 욕망이 껴들게 되면서 모든 것들이 무너지고 있는 것 아닌가 싶다. Ripple도 일단 자기네들이 20%를 나눠먹고 시작을 하고 - 링크 pre-mining 이후에 ICO를 하는 코인들도 부지기수다. (물론 이것 자체가 나쁘다고 볼 수는 없지만.. IPO를 대체하는 개념으로 보면 자사주를 가지고 있는 것이므로..)

```
Of the 100 billion created, 20 billion XRP were
```

```
retained by the creators, who were also the
founders of Ripple Labs.
```

그나마 희망이 되는 것은, 저러한 비트코인캐시 진영에 맞서는 Bitcoin Core 개발자들이 나름의 사명감을 가지고 있다고 들었다. 코드 한 줄을 넣더라도 그것들이 미치는 영향에 대해서 수 개월을 토론했던 적도 있고 또 비트코인캐시의 막가파식 행동에 대하여 비판적인 자세를 견지하며 나름의 전략으로 대응하고 있다고 들었다.

또한 단순히 stakeholder 들 간의 겨루기가 아닌, 각국 정부 차원에서의 규제도 반드시 필요하다고 본다. 그 혼란과 탐욕의 끝판을 보고나니 반드시 어떤 boundary는 필요하지 않나 하는 확신이 들기 시작했다.

결국 헤겔의 정반합 이론처럼, 가상화폐가 뭔가 엄청난 희망과 미래기술처럼 인식되는 지금의 상황에 맞서, 의식을 가진 개발자들, 사업가들이 불꽃으로 가는 지옥열차를 막을 대안을 제시해주고 그것들이 사회적 합의를 통해 더 좋은 발전방향으로 가지 않을까 하는 희망을 갖고자 한다. 그것들이 지식인, 너무 거창하다면 개발자/사업가/기획자 등 그래도 일반인들보다 하나라도 더 알고 있는 사람들의 책무가 아닐까 한다.

가상화폐가 단순히 투기 목적이 아닌, 실제로 우리의 삶을 윤택하고 편리하게 해줄 수 있는 방법 그리고 대안으로 활용되길 바래본다.

~~그리고 업비트를 켜고 시세를 본다.. 한숨이 나온다.. 아효.. 말만 많으면 뭐해.. 수익은 하나도 못내는데..~~

Written on November 17, 2017