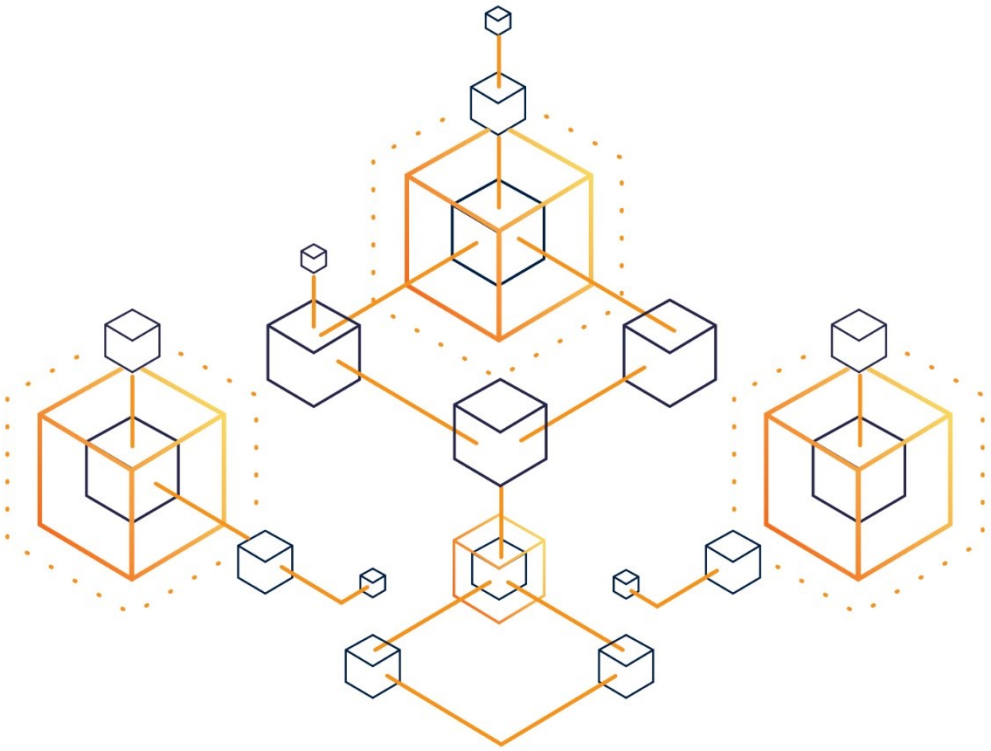
INVENTING BITCOIN

인벤팅 비트코인



가장 쉽게 따라가며 배우는
비트코인의 설계 원리

얀 프리츠커 Yan Pritzker 지음

허성필 옮김

인벤팅 비트코인(INVENTING BITCOIN)

가장 쉽게 따라가며 배우는 비트코인의 설계 원리

얀 프리츠커(YAN PRITZKER) 지음

허성필 옮김

inventingbitcoin.com 에서 본 저서의 업데이트 버전을 받으시기 바랍니다.

이 책을 구 소련 독재정권의 삼엄한 자본통제와 횡포로부터 우리 가족을 대피시킨 저의 부모님 Yury 와 Lana 에게 바칩니다.

또한, 비트코인에 대한 이야기를 한시도 멈추지 않고 늦은 시각까지 책을 마무리하기 위해 밤을 지새곤 했던 저를 견뎌준 아내 Jessica 에게 이 책을 바칩니다.

목차

서론 (INTRODUCTION)

비트코인에 대해 처음 접하는 순간, 많은 사람들이 비트코인을 이해하기 위한 별다른 노력없이 섣불리 판단을 내려버리곤 합니다. 시중에 잘못된 정보가 아주 많이 퍼져 있기 때문에 비트코인이 무엇인지, 어떻게 작동하는 건지 잘못된 판단을 내리기 쉽습니다. 세 달전까지 저도 마찬가지였습니다.

제가 왜 이 책을 쓰기로 마음먹었을까요? 저는 지난 20 년을 테크놀로지 스타트업을 만드는데 쏟았습니다. 매일 새로운 기술에 몰두해왔기 때문에, 이해력이 좋다고 자부합니다. 그럼에도 불구하고, 저 또한 비트코인에 대해 처음 들은 순간부터 제대로 집중해서 이해하기까지 5 년이 걸렸습니다. 세상을 바꿀 잠재력이 있는 이 혁신을 이해하는데 도움이 필요한 사람이 저 혼자는 아닐 것이라고 생각합니다.

저는 2011 년 slashdot.org 라는 인터넷 뉴스 사이트를 통해 비트코인을 처음 접했습니다. 당시 비트코인은 가격이 천정부지로 치솟으면서 거품의 최고가로 30 달러를 기록하던 때였습니다. 당시 제가 알고 있던 것은 인터넷에서 몇몇 사람들이 P2P 결제 시스템을 만들려고 한다는 것뿐이었습니다. 그게 무엇인지, 어떻게 작동하는지는 물론, 투자나 시장 사이클에 대해서도 모른 채로, 혹시 이 프로젝트가 성공해서 중요한 시스템이 될 경우를 대비해 조금 사두면 좋겠다고 생각했을 뿐입니다. 당시 저는 비트코인을 사기 위해 마운트 각스(Mt. Gox)라고 불리는 흉측한 인터페이스의 웹사이트를 통해야 하기도 했습니다. 이 달러-비트코인 거래소는 나중에 파산하게 됩니다.

저는 비트코인 가격이 30 달러에서 2 달러로 폭락하는 과정에서 제 투자금액이 서서히 줄어들어 아무것도 남지 않는 과정을 지켜보게 되었습니다. 이후 언젠가쯤 저는 이 모든 것에 대해 잊어버리고, 스타트업을 만드는 일상으로 돌아갔습니다. 당시 매입했던 코인이 어떻게 되었는지는 지금도 알 수 없습니다. 아마 어느 쓰레기 더미 속 낡은 노트북 하드드라이브에 해당 코인의 키(keys)가 보관되어 있지 않을까 추측할 뿐입니다.

2013 년에 저는 비트코인을 다시 접하게 됩니다. 이번에는 미디어에서 더 큰 화제가 되었을 뿐 아니라 비트코인을 사는 과정도 훨씬 수월하게 바뀌어 있었습니다. 코인베이스(Coinbase) 같은 아주 번듯한 앱들이 나와있었습니다. 이는 예전 마운트 각스 시기와 비교해서 비약적 발전이었습니다. 저는 비트코인이 정말로 성공하지 않을까 하고 생각하게 되었습니다.

저는 여전히 뭐가 뭔지 모르는 상태였지만 한편으로 혹시나 하는 생각에 당시 시장 최고가인 코인당 약 1,000 달러에 다시 한번 비트코인을 사게 되고, 이후 200 달러로 가격이 떨어지면서 투자금액이 산산조각 나는 과정을 지켜보게 됩니다. 이번에는 투자금액이 굳이 매도해서 회수할 정도의 금액도 아니라 판단한 저는 코인을 그대로 내버려두고 당시 한창 진행 중이던 저의 다음 스타트업인 reverb.com 을 준비하는데 전념하게 됩니다.

이후 4 년 동안 Reverb 는 빠르게 성장하여 뮤지션들이 가장 즐겨찾는 서비스가 되었습니다. 저는 세상을 바꾸는데 일조하면서 사람들에게 음악을 선사하고 있었습니다. 저는 신나고 빠르게 성장하는 테크 회사의 CTO 로써 제가 열정을 가진 일을 하고 있었고, 무슨 인터넷 머니(Internet money) 따위에 신경 쓸 겨를이 없었습니다.

제가 처음 안드레아스 안토노폴로스(Andreas Antonopoulos)의 영상을 접한 것은 부끄럽게도 2016 년에 와서야 일이었고, 이 영상들을 통해서 비로소 제대로 주의를 기울이기 됩니다. 저는 질문하기 시작했습니다. 비트코인은 어디에서 만들어 지는 것인가? 누가 통제하는가? 어떻게 작동하는가? 채굴은 무엇인가? 이 모든 것이 세계에 미칠 영향은 무엇일까? 저는 매일을 관련 내용을 닥치는 대로 읽고, 끊임없이 팟캐스트를 찾아 들으면서 일년 반을 보냅니다.

마침내, 비트코인이 2 만 달러의 신고가 기록한 직후인 2018 년 초, 저는 Reverb 를 떠나 어떤 방식으로든 비트코인을 세상에 퍼뜨리는데 기여하기로 결심합니다. 아주 성공적인 스타트업을 떠나 비트코인과 관련된 일을 하기로 결심한 이유는, 비트코인의 발명이 일생일대, 더 나아가 여러 세대에 한번 일어날까 말까 한 일이라고 믿기 때문입니다.

비트코인이 성공한다면, 이는 인쇄술의 발명(정보 생산의 분산화), 인터넷(컨텐츠와 커뮤니케이션의 분산화), 삼권분립 민주주의(정부의 분산화)만큼이나 중요한 사건이 될지 모릅니다. 저는 여러분이 비트코인의 원리를 이해함으로써 어떻게 비트코인이 세상에 이로운 영향을 미칠 수 있는지 이해하실 수 있기 바랍니다. 비트코인은 돈의 생산과 소비과정을 분산화시켜, 이제까지 상상할 수 없었던 인류적 규모의 협력이 가능하게 하는 다양한 가능성을 여는 열쇠가 될 것입니다.

여러분이 미디어를 통해 듣는 대부분은 비트코인의 가격에 대한 내용일 것입니다. 하루는 코인당 수십억까지 가격이 오를 것이라고 떠들다, 다음날이면 추락의 소용돌이에 휩쓸려 곧 제로가 될 것이라고 부산을 떠는 식입니다. 이도 저도 아니면 비트코인이 세상의 모든 에너지를 낭비해서 수년 내 지구의 환경을 파괴할 것이라는 내용일 수도 있습니다. 물론 이는 틀린 말이며, 여러분도 이 책을 통해 비트코인의 원리를 이해한 후 깨달으실 수 있기를

바랍니다. 또한 이 책을 통해 가격 등락보다 더 흥미로운 비트코인의 다른 많은 특성을 이해하게 될 것입니다.

비록 비트코인을 둘러싼 경제학적 원리나 건전화폐(sound money)의 관점을 간략히 다루기는 하나 이 책의 목표는 이 관점에서 비트코인을 분석하고자 하는 것이 아닙니다. 비트코인을 투자의 관점에서 살펴보거나, 모두가 조금씩 보유해야 한다고 설득하는 것은 이 책의 의도가 아닙니다. 사이프딘 아무스(Saifedean Ammous)의 책, *비트코인 스탠다드(비트코인 본위제, The Bitcoin Standard)*를 읽어보지 않으신 분은 제 책에 이어서 꼭 읽어보시길 권합니다.

또한, 이 책에서는 컴퓨터 코딩을 다루지 않기 때문에, 컴퓨터 공학에 배경지식이 없어도 무방합니다. 이 관점에서 비트코인을 공부하고 싶으시다면, 안드레아스 안토노폴로스(Andreas Antonopoulos)의 대작, *비트코인, 공개 블록체인 프로그래밍(Mastering Bitcoin)*이나 최근 출간된 송재준(Jimmy Song)의 *밑바닥부터 시작하는 비트코인(Programming Bitcoin)*을 추천합니다.

저에게 비트코인의 원리를 구성하는 여러가지 측면을 종합적으로 이해하는 것은 깊은 통찰의 순간이었습니다. 이 책을 통해 명료한 방식으로 그 깨달음을 나눌 수 있기를 바랍니다. 오늘 저의 목표는 여러분의 머리 속에 작은 자극을 주고, 비트코인을 우리 시대 가장 흥미롭고 심오한 발명으로 만드는 구성요소로써 컴퓨터 공학, 경제학, 게임 이론의 맛보기를 보여드리는 것입니다. 여러분이 비트코인의 원리를 이해함으로써, 제가 그랬던 것처럼, 처음 생각했던 것보다 비트코인이 가지는 의미가 훨씬 방대하고, 앞으로 여러 세대에 걸쳐 믿을 수 없을 영향을 끼칠 수 있음을 깨닫길 바랍니다.

이 책은 차례대로 단계적으로 진행됩니다. 고등학교 수준의 수학을 벗어나지 않는 수준에서 비트코인의 발명을 한걸음씩 되짚어볼 것입니다. 이 책이 여러분이 신비로운 비트코인의 세계에 들어가는 토끼굴로 빠져들어가는 출발점이 될 수 있길 기대합니다. 그럼, 같이 시작해 보겠습니다!

1. 비트코인이란? (WHAT IS BITCOIN?)

비트코인은 P2P(Peer-to-Peer) 전자현금으로서, 은행 같은 중개자를 신뢰할 필요 없이 사람이나 컴퓨터끼리 주고받을 수 있는 새로운 형태의 디지털 통화입니다. 이 비트코인의 발행은 어떤 단일 주체도 통제권을 가지고 있지 않습니다.

종이 지폐나 동전을 떠올려 보시기 바랍니다. 이 돈을 다른 사람에게 넘겨줄 때, 그 사람이 여러분이 어떤 사람인지 알아야할 필요는 없습니다. 단지 받은 돈이 위조지폐가 아니란 신뢰만 필요할 뿐입니다. 보통 이 신뢰를 얻는 데에는 눈과 손의 감각으로 간단히 검증해 보는 정도면 충분하며, 거래 금액이 크다면 특수한 기계를 활용하는 정도일 것입니다.

사회가 디지털화 되면서 이제 결제수단의 대부분은 중개자의 서비스를 통해 이루어지고 있습니다. 비자(Visa) 같은 신용카드사, 페이팔(PayPal)이나 애플페이(Apple Pay) 같은 디지털 결제서비스 사업자, 위챗(WeChat) 같은 온라인플랫폼 사업자가 그 예입니다.

디지털 결제수단의 확대는 거래를 승인 검증하는 중앙 기구에 대한 의존의 확대로 이어졌습니다. 이는 돈의 특성이 직접 가지고 다니고, 넘겨주고, 검증할 수 있는 물체에서 거래의 통제권을 쥔 제 3 자가 보관하고 검증하는 디지털 신호로 바뀌었기 때문입니다.

현금 대신 편리한 디지털 결제가 확대되면서, 특정 소수에게 사람들을 억압할 수 있는 막강한 권력이 집중된 시스템이 태어났습니다. 디지털 결제 플랫폼은 반체제 인사를 감시하고 불온한 시민의 경제력을 빼앗아 버리는 중국 정부의 사례 같이 디스토피아적 권위주의 사회의 기반이 되어 버렸습니다.

비트코인은 다른 사람을 통할 필요 없는 현금의 성격을 다음 세가지 구성요소를 가진 디지털 방식으로 구현하여, 중앙집권화된 디지털 화폐에 대한 대안을 제시합니다.

1. 비트코인(bitcoin(영어 소문자))
   예상가능하고 고정되고 한정적인 공급을 가진 디지털 자산 비트코인. 이 특성은 비트코인이 예상할 수 없는 공급량을 가진 정부나 중앙은행이 발행하는 통화와 선명히 대조되는 점입니다.

2. 비트코인 네트워크(The Bitcoin network)
   공개 소프트웨어를 실행해 누구나 접속할 수 있는 비트코인 네트워크. 이 컴퓨터 네트워크를 통해 비트코인(bitcoins) 발행, 해당 소유권 기록관리, 은행/회사/정부 같은 중개자를 통하지 않고 네트워크 참여자 간 해당 소유권의 이전이 가능해집니다.

3. 비트코인 클라이언트 소프트웨어(The Bitcoin client software)
   비트코인 네트워크에 접속하기 위해 누구나 각자의 컴퓨터에서 실행이 가능한 컴퓨터 소프트웨어. 이 소프트웨어는 오픈 소스(open source)로, 누구나 소프트웨어의 코드를 볼 수 있고, 신기능을 추가하거나 버그를 고치는 과정에 참여할 수 있습니다.

비트코인(Bitcoin)은 비트코인 클라이언트 소프트웨어를 실행하는 컴퓨터들의 네트워크입니다.

다음 섹션에서는 비트코인 탄생의 배경에 대해 알아보겠습니다.

비트코인의 시작 (Where Did It Come From?)

비트코인은 약 2008 년에 사토시 나카모토(Satoshi Nakamoto)라는 익명의 개발자가 발명하였습니다. 이 익명의 개발자가 개인인지, 단체인지 그 정체가 전혀 알려진 바가 없으며, 현재까지 알려진 바로는 그나마도 지난 수년간 활동을 멈추고 나타나지 않은 지 오래되었습니다.

2009 년 2 월 11 일, 사토시는 비트코인 프로토타입에 대한 자료를 사이퍼펑크(cypherpunk) 인터넷 포럼에 게시하였습니다. 사이퍼펑크란 개인의 프라이버시와 자유를 중시하는

암호기술(cryptography technology) 업계 종사자를 일컫는 말입니다. 비록 이 게시물이 비트코인의 공식 배포를 발표하는 내용은 아니었지만, 해당 글에서 사토시의 개발 동기를 잘 요약하고 있는 내용이 포함되어 있습니다.

관련된 핵심 내용이 아래에 정리되어 있습니다. 다음 섹션에서는 아래 서술을 자세히 살펴보고, 사토시가 현재 금융 시스템의 어떤 문제점을 해결하고자 했는지 이해해보도록 하겠습니다.

> *저는 비트코인이라고 하는 새로운 오픈소스 P2P 전자현금 시스템(open source P2P e-cash system)을 개발했습니다. 이 시스템은 중앙 서버나 신뢰 기관(trusted parties) 없이 완전히 분산되어 있어, 모든 요소가 신뢰 대신 암호기술을 통한 증명에 기반하고 있습니다. [...]*
>
> *전통적 화폐 시스템의 근원적 문제점은 시스템이 작동하기 위해 막대한 신뢰가 필요하다는 점입니다. 중앙은행은 화폐의 가치를 절하시키지 않기를 신임받지만, 법정화폐(fiat currencies)의 역사는 그런 신뢰가 깨어진 사례로 가득합니다. 은행은 예금자의 돈을 보관하고 이전하도록 신임받지만, 신용 버블과 부분지급준비제도를 통해 무분별한 대출이 일어납니다. 우리는 이들 기관에 프라이버시를 맡겨야만 하고, 신분 도용으로 인한 사고를 막아 주길 믿어야만 합니다. 이들 기관의 막대한 비용은 마이크로페이먼트(micropayments)의 실효성을 가로 막습니다.*
>
> *한 세대 이전, 다중 사용자 시분할 컴퓨터 시스템(multi-user time-sharing computer system) 또한 유사한 문제를 겪었습니다. 강력한 암호기술이 가능하기 전 사용자는 파일의 보안을 패스워드에 의존해야만 했습니다. [...]*
>
> *이후 강력한 암호기술이 대중화되면서 신뢰의 필요성은 사라지게 되었습니다. 데이터를 어떤 이유와 상황에도 불문하고 물리적으로 다른 사용자가 접근할 수 없도록 안전하게 보호할 수 있게 되었습니다.*
>
> *통화에 있어서도 이와 같은 해결책을 적용할 때가 되었습니다. 암호학적 증명에 기반을 둔, 제 3 의 중개기관을 신뢰할 필요가 없는 전자통화를 통해 돈은 안전해지고 거래는 쉬워질 수 있습니다. [...]*
>
> *비트코인의 솔루션은 P2P 네트워크를 통해 이중 지불(double spending) 위험을 막습니다. 간단히 말하자면, 네트워크가 현금의 첫번째 지출 거래를 인증하여, 분산된*

타임스탬프(timestamp) 서버 역할을 하는 것입니다. 이는 정보가 퍼지기는 쉬우나 억압하기는 어려운 특정을 활용한 것입니다. 더 자세한 설명은 링크 https://bitcoin.org/bitcoin.pdf 의 백서를 참고하십시오.

- *사토시 나카모토*

비트코인이 해결하는 문제점 (What Problems Does It Solve?)

사토시의 게시물을 문장 별로 살펴보겠습니다. 이 책은 각 컨셉이 실제로 어떻게 적용되는지를 다룰 것입니다. 본 섹션에서 이해가 충분히 되지 않는 부분이 있더라도 뒷부분에서 더 다룰 것이므로 걱정하실 필요 없습니다. 비트코인을 발명하는 과정을 되밟으면서 사토시의 애초 목표를 이해하고 이를 이루어 나갈 수 있도록 하는 것이 목적입니다.

저는 비트코인이라고 하는 새로운 오픈소스 P2P 전자현금 시스템(open source P2P e-cash system)을 개발했습니다.

P2P 는 *개인과 개인(peer to peer)*의 줄임말로, 한 사람이 가운데 어떤 중개자 없이 상대방과 동등한 입장(equal peers)에서 상호작용할 수 있는 시스템입니다. 넵스터(Napster), 카자(Kazaa), 비트토렌트(BitTorrent) 같은 P2P 파일 공유 시스템을 떠올리실 수 있을 겁니다. 이런 P2P 파일 공유 시스템을 통해 처음으로 사람들이 중개자 없이 음악과 영화를 서로 공유할 수 있게 되었습니다. 사토시는 이와 매우 유사한 방식으로 사람들이 전자현금을 중개자를 통하지 않고 직접 교환할 수 있도록 만들었습니다.

비트코인 소프트웨어는 오픈소스(open source)로, 누구든 소프트웨어가 작동하는 원리를 확인할 수 있고 업그레이드 작업에 기여할 수 있습니다. 이로 인해 최초 개발자인 사토시를 막연히 신뢰해야 할 필요가 없어집니다. 비트코인 소프트웨어의 코드를 직접 검증할 수 있기 때문에 비트코인 소프트웨어의 작동원리에 대해 사토시의 설명에 대한 믿음에 의존할 필요가 없습니다. 더불어 코드를 바꾸어 시스템의 기능을 더 개선해 나갈 수도 있습니다.

이 시스템은 중앙 서버나 신뢰 기관(trusted parties) 없이 완전히 분산되어 있어 ...

사토시는 *분산화*를 언급하여 비트코인 시스템을 중앙집권화된 시스템과 구분하였습니다. 1989 년 데이빗 차움(David Chaum)이 만든 DigiCash 와 같이 비트코인 이전 디지털화폐 개발 시도는 하나의 회사가 통제하는 *중앙 서버*가 화폐발행, 거래검증을 책임지는 방식에 기초했습니다.

이런 중앙집권화된 민간(private) 화폐는 실패할 운명일 수밖에 없었습니다. 특정 회사가 망하거나, 해킹 당하거나, 서버 사고를 겪거나, 정부로 인해 폐쇄되면 사라지고 말 화폐에 사람들이 의존할 리 없는 것입니다.

비트코인은 단일의 회사가 아닌 전세계 무수한 개인과 회사의 네트워크를 통해 운영 관리됩니다. 비트코인을 폐쇄시키려면 전세계 대부분 익명으로 흩어져 있는 수만, 수십만 컴퓨터를 모두 폐쇄해야 합니다. 이런 방식으로 비트코인 네트워크를 폐쇄하려는 시도는 새로운 비트코인 노드(nodes) 생성으로 이어져, 사실상 희망 없는 두더지 잡기 놀이에 그치게 됩니다.

... 모든 요소가 신뢰 대신 암호기술을 통한 증명에 기반하고 있습니다.

인터넷을 비롯해 현대 컴퓨터 시스템의 대부분이 암호기술에 기반해 만들어졌습니다. 암호기술은 정보를 변형해 오직 수신자만 해독할 수 있도록 만드는 방법을 뜻합니다. 비트코인은 어떻게 *신뢰*의 필요성을 제거하는 것일까요? 이 책의 뒷부분에서 더 다루겠지만, 기본 아이디어는 "저는 앨리스입니다" 혹은 "저는 계좌에 $10 를 가지고 있습니다" 같은 주장을 하는 누군가를 믿는 대신, 동일한 사실을 수신자가 검증하기는 매우 쉽되 조작하기는 불가능한 형태의 암호기술적 수학식으로 표현하는 것입니다. 비트코인은 설계 전반에 걸쳐 시스템 참여자가 다른 중앙 기관에 대한 신뢰에 의존하지 않고 다른 참가자의 행위를 검증할 수 있도록 암호기술적 수학을 활용합니다.

우리는 이들 기관에 프라이버시를 맡겨야만 하고, 신분 도용으로 인한 사고를 막아 주길 믿어야만 합니다.

은행 계좌, 디지털 결제 시스템, 신용카드를 사용할 때와 달리 비트코인은 양측 당사자가 거래하는데 개인 정보를 제공할 필요가 없습니다. 은행, 신용카드 회사, 결제 서비스, 정부에 저장된 중앙집권화 된 고객 데이터는 커다란 해킹 표적지가 됩니다. 사토시의 논지를 증명이나 하듯 2017 년 미국의 신용평가기관 Equifax 에 막대한 해킹 사고가 발생해 1 억 4 천만명 이상의 신상정보와 재무정보가 해커에게 유출되었습니다.

비트코인은 현실의 신상정보와 금융 거래를 분리시킵니다. 보통의 현금으로 지불할 때 상대방은 우리가 누구인지 알 필요가 없고 우리도 상대방이 거래 후 거래 과정에서 얻은 정보를 이용해 우리의 돈을 더 훔쳐갈지 걱정할 필요가 없습니다. 디지털 통화라면 이와 마찬가지거나 더 나아야 하지 않을까요?

> *중앙은행은 화폐의 가치를 절하시키지 않기를 신임받지만, 법정화폐(fiat currencies)의 역사는 그런 신뢰가 깨어진 사례로 가득합니다.*

법정화폐(fiat)는 라틴어로 "그렇게 정하다(let it be done)"라는 뜻이며, 정부나 중앙은행이 발행하고 정부가 법적으로 화폐의 지위를 선포된 화폐를 의미합니다. 역사적으로, 화폐는 생산이 어렵고, 검증과 운송이 쉬운 조개껍질, 유리 구슬, 은, 금 같은 재화로 만들어져 왔습니다. 특정 재화가 화폐로 사용되기 시작하면, 해당 재화를 더 생산하려는 유인이 생깁니다. 새로운 기술을 통해 해당 재화를 빠르게 대량생산할 수 있게 되면 해당 재화는 가치를 상실하게 됩니다. 이런 방식은 유럽인이 아프리카 대륙의 부를 탈취한 방법이기도 합니다. 유럽인들은 생산이 어려운 인간 노예의 대가로 생산이 쉬운 유리구슬을 지불했습니다. 금이 오랫동안 화폐로 사용하기 우수한 재화로 여겨진 이유가 바로 금을 쉽게 생산할 수 있는 방법이 없기 때문입니다[1].

세계 경제는 천천히 금을 화폐로 활용하는 단계에서 금에 대한 증서로 발행된 종이 화폐를 활용하는 체제로 전환되어 왔습니다. 궁극적으로, 1971 년 달러의 국제 금태환 종료를 선언한 닉슨 정부에 들어서 종이 화폐는 일절의 실물 기초자산로부터 단절되었습니다.

---

[1] 화폐의 역사에 대한 개괄로 닉 자보(Nick Szabo)의 에세이 Shelling Out 을 읽어보시길 추천합니다. https://nakamotoinstitute.org/shelling-out/

금본위 제도의 종말로 인해 정부와 중앙은행은 *시장 유통 화폐의 가치 하락*(*debasement*)을 담보로 화폐 공급을 언제든 증가할 수 있게 되었습니다. 다른 자산으로의 상환이 일절 보장되지 않는 정부 발행 법정화폐는 오늘날 우리가 익숙하게 여기는 일상적 화폐의 형태이지만, 세계역사의 관점에서 이는 비교적 최근부터 진행된 실험적 시도에 지나지 않습니다.

정부가 화폐 공급 능력을 남용하지 않도록 신용할 수밖에 없는 상황에 놓인 상황이지만, 그런 *신임의 위반*(*breaches of that trust*) 사례를 찾기는 어렵지 않습니다. 베네수엘라 같이, 정부가 화폐 공급에 대한 전권을 가진 독재적 중앙 계획경제 체제의 법정화폐는 사실상 가치를 상실했습니다. 베네수엘라 볼리바(Venezuelan Bolivar)는 2009 년 1 달러 당 2 볼리바에서 2019 년 1 달러 당 250,000 볼리바로 폭락하였습니다. 현재 베네수엘라는 정부의 경제 운영 실패로 인해 체제 붕괴의 직전에 몰린 상황입니다.

사토시는 항상 예측 불가하게 공급량이 증가하는 법정화폐에 대한 대안을 제시하고자 했습니다. *화폐의 가치 하락*(*debasement*)을 막기위해, 사토시는 최대 공급량이 고정되고 향후 공급일정을 예측할 수 있는 화폐 시스템을 설계하였습니다. 비트코인은 최대 2,100 만개만 생산될 예정이며, 이는 1 억 분의 1 비트코인을 지칭하는 단위인 사토시(satoshi) 기준으로 모든 신규 공급이 완료되는 약 2140 년에는 2,100 조의 사토시가 공급될 것을 의미합니다.

비트코인 이전에는 디지털 자산의 무한 복제를 막을 수 있는 방법이 없었습니다. 디지털 서적, 오디오 파일, 비디오는 싸고 쉽게 복제 전송할 수 있습니다. 예외적인 경우는 중개자가 통제하는 디지털 자산입니다. 예를 들어 아이튠즈(iTunes)에서 영화를 대여할 경우 아이튠즈는 해당 영화의 통제권을 유지하며, 소비자는 아이튠즈가 허용한 대여기간 동안만 소비자의 디바이스를 통해 접근할 수 있는 있습니다. 이와 유사하게 디지털 화폐의 통제권은 은행이 가지고 있습니다. 은행은 예금자의 보유액이 얼마인지 기록관리하고, 예금자가 송금을 하고자 할 경우 해당 송금 승인 여부를 결정합니다.

비트코인은 중개자를 두지 않고도 희소성을 담보하는 최초의 디지털 시스템이자, 변경 불가능한 공급량과 공급 일정이 사전에 완전히 공개되어 있는 인류 역사 상 최초의 자산입니다. 이는 금과 같은 귀금속도 가지지 못한 특성입니다. 금의 채굴은 수익성이 있는 한 지속될 수 있습니다. 지금까지 채굴된 양의 열배에 달하는 금을 보유한 소행성을 발견하는 경우도 상상해볼 수 있습니다. 이런 공급 충격의 경우 금 가격은 어떻게 반응할까요? 비트코인은 이런 발견이나 공급량 변경으로부터 완전히 자유롭습니다.

비트코인을 현재 알려진 이상 생산하는 것은 간단히 말해 불가능합니다. 이에 대해 다음 챕터에서 더 살펴보도록 하겠습니다.

화폐의 성격과 기존 화폐 시스템의 작용은 복잡다단하여 이 책에서 깊게 다룰 수는 없습니다. 화폐의 기본 특성이 비트코인에 어떻게 적용되는지 더 알고 싶으시면, 사이프딘 아무스(Saifedean Ammous)의 책, 비트코인 스탠다드(The Bitcoin Standard)가 좋은 출발점이라고 생각합니다.

> *데이터를 어떤 이유와 상황에도 불문하고 물리적으로 다른 사용자가 접근할 수 없도록 안전하게 보호할 수 있게 되었습니다. [...] 통화에 있어서도 이와 같은 해결책을 적용할 때가 되었습니다.*

은행 예치하는 방식 등 현재 우리가 가진 화폐 보관 방법은 모두 누군가에 대한 위임과 신임을 전제하고 있습니다. 중개자에 대한 이런 신임은 중개자가 권한을 오용하지 않을 것은 물론, 정부가 중개자를 압박해 예금자의 자금을 몰수하거나 동결하지 않을 것이라는 신뢰도 전제되어야 합니다. 그러나, 정부가 스스로에게 위협이 된다고 판단할 경우 특정 개인이나 집단의 화폐 접근을 차단하는 사례는 끊임없이 반복되어 왔습니다.

미국이나 다른 규제가 발달한 경제를 보유한 국가 거주자에게는 바보 같이 들릴 수 있지만, 하루 아침에 예금이 사라지는 경우는 지금도 항상 발생하고 있습니다. 저자는 단순히 수개월간 사용하지 않았다는 이유만으로 페이팔(PayPal) 계좌의 자금을 동결 당한 경험이 있었습니다. 저자 "자신의" 자금 접근권한을 회복하는 데까지 몇 주가 소요되었습니다. 미국에 사는 저자는 페이팔의 자금 동결에 대해 법적 조치를 취할 수 있고, 정부와 은행이 자금을 몰취하지 않을 것이라는 기본적 신뢰를 가질 수 있는 운이 좋은 경우에 속하는 경우입니다.

시민에게 자유가 덜 보장된 국가에서는 이보다 불행한 경우가 많이 있었고, 지금도 발생하고 있습니다. 그리스에서는 통화 붕괴 시기에 은행이 폐쇄되었으며, 사이프러스에서는 은행이 고객 자금 몰수를 통한 베일인(bail-ins) 제안이 있었으며, 인도에서는 특정 금액 화폐권의 통용을 예고없이 중단하기도 했습니다.

저자가 성장한 구 소련의 정부 계획 경제는 광범위한 재화 공급부족으로 이어진 바 있습니다. 당시 미국 달러 같은 외화를 보유하는 것은 불법이었습니다. 다른 나라로 떠날 때,

저자의 가족은 시장 환율에 훨씬 못 미치는 정부의 공식 환율을 통해 제한된 금액만을 달러로 환전할 수 있었습니다. 결과적으로, 저자의 가족은 당시 그나마 보유하고 있던 재산을 경제와 자본 이동의 통제를 통해 대부분 정부에 몰수당한 샘입니다. 독재 국가는 보통 엄격한 경제적 통제를 통해 시민들이 자금을 은행에서 인출하여 국외로 유출하거나 다른 국가의 화폐로 시장 환율에 따라 환전할 수 없게 막습니다. 이는 정부가 소련의 사회주의 체제 같은 광적인 경제 실험을 이행할 수 있도록 통제력을 확보하기 위함입니다.

비트코인은 자금의 보관에 있어 제 3 자 기관에 대한 신뢰에 의존하지 않습니다. 대신 비트코인은 자금 소유자의 특수한 키(key)가 없는 다른 사람은 *어떤 이유와 상황에도 불문하고,* 자금에 접근할 수 없도록 만들었습니다. 비트코인을 보유함에 재정적 자유(financial freedom)로 통하는 열쇠(key)를 얻게 되는 것입니다. 비트코인은 돈과 국가(money and state)를 분리시킵니다.

> *비트코인의 솔루션은 P2P 네트워크를 통해 이중 지불(double spending) 위험을 막습니다. [...] 간단히 말하자면, 네트워크가 현금의 첫번째 지출 거래를 인증하여, 분산된 타임스탬프(timestamp) 서버 역할을 하는 것입니다.*

여기에서 *네트워크*는 서로 연결되어 메시지를 주고받을 수 있는 여러 컴퓨터의 집합체를 의미합니다. *분산(distributed)이란* 통제권을 가진 중앙 기구 없이 모든 네트워크 참여자가 네트워크를 성공적으로 유지하고 운영하기 위해 협력하는 개념을 의미합니다.

중앙 기구의 통제가 없는 시스템에서는 다른 참여자의 부정 행위가 없었음을 검증하는 것이 중요합니다. *이중 지불(double spending)*이란 하나의 화폐를 두 번 지출하는 상황을 뜻합니다. 이런 상황은 지출하면 손을 떠나버리고 마는 물리적 화폐에서는 문제가 되지 않습니다. 그러나, 음악이나 영화처럼 복제가 가능한 디지털 거래에서 이중 지불은 중요한 문제입니다. 은행을 통한 송금 시에는 은행이 송금자가 해당 자금을 재사용 할 수 없도록 막습니다. 이런 중앙집권적 기구가 없는 시스템에서는 사실상 화폐 위조와 같은 효과를 가지는 *이중 지불*을 막기 위한 특별한 방법이 필요합니다.

사토시는 여러 거래의 순서를 검증하는 *타임스탬프(timestamp)*를 생성함으로써 어떤 거래가 먼저 일어났는지 확인하고 향후 동일한 자금을 다시 지출하려는 시도를 기각할 수 있도록 비트코인 네트워크 참여자가 협력하는 방법을 기술해 놓았습니다. 다음 챕터를 통해 이

시스템을 처음부터 설계하는 과정을 밟아가 볼 것입니다. 이 시스템을 통해 중앙 발행 기구나 거래 검증 기관 없이도 화폐 위조를 적발할 수 있습니다.

비트코인은 하루 아침에 일어난 발명이 아닙니다. 사토시는 글을 통해 웨이 다이(Wei Dai)의 b-money, 애덤 백(Adam Back)의 Hashcash 같은 다른 중요한 디지털 화폐 개발 시도를 인용하고 있습니다. 이처럼 비트코인의 발명은 이전 다른 거인의 어깨 위에 있으나, 비트코인이야 말로 그전부터 존재한 여러가지 구성요소를 한번에 묶어, 진정 희소한(truly scarce) 디지털 화폐를 중앙 기구 없이 발행하고 전송할 수 있는 시스템을 최초로 이룩했습니다.

사토시는 현재의 통화 시스템이 가진 프라이버시, 화폐 가치 하락(debasement), 중앙집권적 통제력의 문제를 해결하기 위해 몇 가지 흥미로운 기술적 난제와 씨름했습니다.

1. 어떻게 누구든 자발적으로 들어와 참여할 수 있는 P2P 네트워크 시스템을 만들 것인가?
2. 어떻게 정체성을 밝히거나 서로를 신뢰하지 않고, 일부 참여자가 정직하지 않더라도, 공동의 장부(a shared ledger of value)를 기록 관리할 수 있을 것인가?
3. 어떻게 화폐의 신규 공급이 무질서해지지 않도록 희소성을 유지하는 동시에, 중앙 발행 기구에 의지하지 않고도 위조 불가능한 화폐를 발행할 것인가?

비트코인이 처음 발행되었을 때 비트코인을 사용하고 비트코인 소프트웨어를 돌려 네트워크를 유지하는 *노드(nodes)*를 운영한 사람은 고작 몇몇에 불과했습니다. 당시 대부분이 비트코인을 농담거리로 치부하거나 얼마가지 않아 치명적 디자인 결함을 드러낼 것이라고 생각했습니다.

시간이 지나면서 비트코인 네트워크에 참여자 수는 점점 늘어나, 보유한 컴퓨터를 활용해 네트워크 보안 수준을 높이기도 하고, 다른 화폐와 교환하여 비트코인의 가치를 강화하기도 했으며, 재화와 서비스의 대가로 비트코인을 채택하기도 했습니다. 10 년이 지난 오늘날 전세계적으로 수백만 명이 비트코인은 사용하고, 수만에서 수십만 개의 노드가 무료 비트코인 소프트웨어를 운영하며, 수십만 명의 자발적 개발자와 회사가 비트코인 소프트웨어를 개발하고 있습니다.

자, 이제 비트코인을 어떻게 만드는지 알아볼 시간입니다!

2. 중개자를 없애다 (REMOVING THE MIDDLEMEN)

이전 챕터에서 비트코인이 가치 전송을 위한 P2P 시스템이란 점을 다루었습니다. 비트코인의 원리를 더 알아보기 전에 전통적 형태의 은행이나 결제 서비스 회사가 자산의 소유와 이전을 추적관리하는 방식을 이해할 필요가 있습니다.

은행의 본질은 거래의 기록(ledgers)이다

은행, 페이팔(PayPal), 애플페이(ApplePay) 등에서 지급된 디지털 거래는 어떻게 처리되나요? 매우 간단히 말해서, 이들 중개자는 계좌와 거래 정보를 기록한 원장에 지나지 않습니다.

은행의 목적은 고객의 예금을 보관하고 지키는 것입니다. 그러나 오늘날 예금은 대부분 동전이나 지폐가 아닌 전자적 형태를 띄고 있습니다. 따라서, 현재 은행의 업무는 계좌 데이터베이스를 유지하고 지키는 것입니다. 은행은 소프트웨어 침입 감지 시스템을 운용하고, 데이터 유실을 방지하기 위해 백업을 관리하고, 외부 기관의 감사를 통해 은행의 내부 절차가 훼손되지 않았는지 검증하고, 문제가 생길 경우를 대비해 보험을 가입합니다.

아래는 위 시스템의 작동 원리입니다. 이 사례에서는 *은행*이라고 표현했지만, 사실 결제를 처리하는 다른 어떤 기관의 경우를 대입해도 원리는 마찬가지입니다. 두 명의 고객, 앨리스와 밥의 은행 예금 계좌 정보를 나타내는 장부부터 설명하겠습니다.

<u>은행 장부</u>

1. 앨리스: 현금 예금 잔고 +$2
2. 밥: 현금 예금 잔고 +$10

앨리스가 $2를 밥에게 송금하려면, 앨리스는 은행에 전화하거나 컴퓨터나 휴대폰으로 은행에 접속해 사용자명과 비밀번호 혹은 PIN 코드로 사용자 인증을 거친 후, 송금 요청을 입력합니다.

은행 장부

1. 앨리스: 현금 예금 잔고 +$2
2. 밥: 현금 예금 잔고 +$10
3. 앨리스: 출금 -$2
4. 밥: 입금 +$2

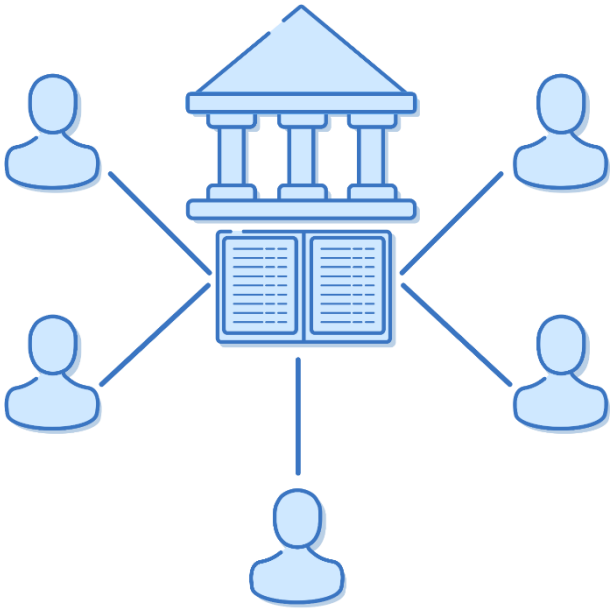
이제 은행은 새로운 출금과 입금, 대변과 차변을 기록하고 자금 송금이 완료되었습니다.

이중 지불의 문제 (The Double-Spending Problem)

이때 앨리스가 $2 를 다시 지출하려고 하면 어떤 상황이 벌어질까요? 이런 상황을 이중 지불의 문제라고 부릅니다. 앨리스는 은행에 지출 요청을 제출하지만 은행은 다음과 같이 반응합니다. "죄송합니다. 고객님의 $2 는 이미 밥에게 송금되었습니다. 고객님은 더 이상 송금할 수 있는 예금이 없습니다."

은행 같은 중앙집권적 기구가 존재하면 해당 중앙집권 기구가 쉽게 이중 지불 시도를 기각할 수 있습니다. 중앙집권 기구는 장부를 수정할 수 있는 유일한 기구이자, 백업과 컴퓨터와 사람을 통한 감사 과정을 통해 장부가 조작되지 않고 올바르게 기록되고 있도록 검증하는 내부 절차를 가지고 있기 때문입니다.

단일 통제 기구(single point of control)를 가진 이런 시스템을 *중앙집권적 시스템*이라고 부릅니다.



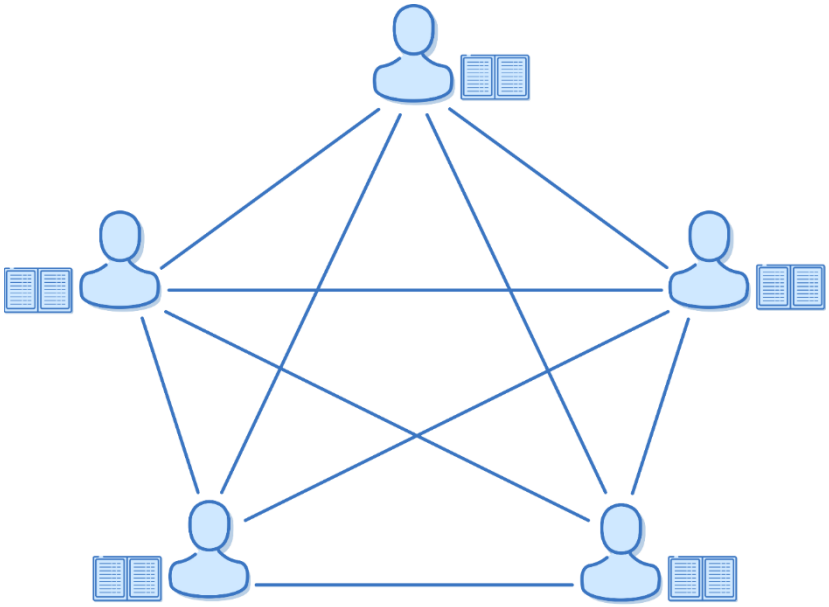
은행은 모두가 접근할 수 있는 장부를 관리하고, 모든 거래는 은행을 거칩니다.

장부의 분산화 (Distributing the Ledger)

비트코인이 해결하려는 첫번째 문제는 중개자를 신임할 필요가 없도록 *P2P 시스템*을 만드는 것입니다. 은행이 없어지고 새로운 금융 시스템을 만들어야 한다고 상상해 보겠습니다. 어떻게 중앙 기구 없이 장부를 기록하고 관리할 수 있을까요?

만약 하나의 중앙화된 장부가 없다면, 장부는 모두가 함께 소유하는 상황이라고 볼 수 있습니다. 혁명적입니다! (Vive la révolution!) 자세한 원리는 아래와 같습니다.

첫째, 여러 참여자가 모여 *네트워크*를 형성합니다. 이는 참여자가 서로 연락할 수 있는 방법이 생긴다는 의미입니다. 모든 참여자들끼리 전화번호나 스냅챗(Snapchat) 계정을 교환한다고 가정해보겠습니다. 앨리스가 밥에게 송금하고 싶으면 은행에 전화하는 대신, 앨리스는 모든 참여자에게 다음 내용을 직접 전달할 수 있습니다. "저는 밥에게 $2 를 송금하겠습니다." 모든 참여자는 내용을 확인하고 "좋아요. 확인했습니다." 라고 회신한 후, 송금 내용을 각자가 가지고 있는 장부에 반영합니다. 위 과정을 나타낸 도표는 아래와 같습니다.



모든 참여자는 독자적으로 접근할 수 있는 각자의 장부를 보유합니다.

이제, 하나의 은행 대신 모두가 각자의 장부를 가지게 되었습니다. 누군가 돈을 쓰려고 할 때마다, 당사자는 모든 사람에게 해당 거래 내용을 전달해야 합니다. 모두가 거래 내역을 각자의 장부에 기록하게 됩니다. 더 이상 장부가 하나가 아니기 때문에 *분산되었다고(distributed)* 표현하며, 중앙집권적 기구가 없기 때문에 *탈중앙화되었다고(decentralized)* 표현합니다. 이에 따라 결과적으로 중개자가 필요 없어집니다.

이제 중개자가 없어진 상황에서 이중 지불의 문제는 어떻게 해결해야 할까요? 은행 대신 누가 나서서 지출 거래 자금이 이미 사용한 자금이 아님을 검증해야 할까요? 모두가 각자의 장부를 가지고 있기에, 네트워크의 참여자 모두가 서로 거래를 검증하게 됩니다. 모두가 특정 버전의 상태를 진실로 받아들이기로 합의하는 이런 시스템을 *컨센서스 방식(consensus-based)*이라고 부릅니다.

앨리스가 밥에게 송금한 $2를 다시 사용하려고 한다면, 앨리스의 거래 요청은 각자의 장부를 확인하고 해당 자금이 이미 밥에게 송금되고 없음을 확인한 네트워크 참여자 모두에게 기각될 것입니다. 따라서 네트워크 참여자들은 앨리스의 두번째 지출 시도는 각자의 장부에 기록하지 않게 됩니다. 자금의 소유와 이전을 기록하는 P2P 컨센서스 네트워크가 탄생하는 순간입니다.

분산된 장부에 접근하는데 *승인(permission)*이 필요하고, 참여자 전부가 정직할 것으로 *신뢰(trust)*할 수 있는 한, 위 시스템은 정상적으로 작동합니다. 그러나 그런 방식으로는 전세계 수 백만명이 사용할 수 있도록 시스템을 확장(scale)할 수가 없습니다. 특정 집단으로만 구성된 분산 시스템은 본원적으로 불안정할 수밖에 없습니다. 참여자 일부가 종종 네트워크 접속을 중단하는 경우가 있을 수 있습니다. 해당 참여자는 접속을 중단하고 있는 기간의 네트워크 전체의 거래 내역을 알 수가 없습니다. 다른 참여자는 네트워크를 속이기 위해 특정 거래의 발생 여부에 대해 거짓 주장을 할 수도 있습니다. 신규 네트워크 참여자는 여러가지 다른 버전의 장부를 받게 될 수도 있습니다.

네트워크 참여자의 부정행위 가능성에 대해 더 알아보겠습니다.

이중 지불 공격 (The Double-Spend Attack)

앨리스는 다른 네트워크 참여자와 다음과 같이 *공모*할 수 있습니다. "제가 돈을 쓰더라도, 당신 장부에 기록하지 마세요. 그런 거래가 발생하지 않은 것처럼 행동해주세요." 앨리스는 아래 방법을 통해 이중 지불을 꾸밀 수 있습니다.

최초 예금 잔고 $2 를 가지고 앨리스는 아래와 같이 행동합니다.

1. 앨리스는 과자를 사기 위해 $2 를 밥에게 송금합니다. 앨리스의 수중에는 이제 돈이 없습니다.
2. 데이빗(David), 이브(Eve), 파라(Farrah)는 앨리스와 공모하여 밥에게 송금한 앨리스의 거래내역을 장부에 적지 않기로 합니다. 세 명의 장부에는 앨리스가 $2 를 사용하지 않고 계속 가지고 있는 것으로 기록되어 있습니다.
3. 샬럿(Charlotte)은 정직한 장부 관리자입니다. 샬럿은 앨리스의 송금 거래를 장부에 반영하고 앨리스의 잔고를 $0 으로 기록합니다.
4. 헨리(Henry)는 일주일의 휴가 기간 동안 앨리스의 거래 내역에 대해 듣지 못했습니다. 휴가가 끝난 헨리는 네트워크에 다시 참여하고 최신 버전의 장부를 요청합니다.
5. 헨리는 네 개의 위조 장부(데이빗, 이브, 파라, 앨리스)와 하나의 정직한 장부(샬럿)를 받았습니다. 헨리는 어떤 버전의 장부를 받아들일까요? 다른 좋은 방법이 있지 않는 한, 헨리는 대다수의 참여자를 믿고 위조 장부를 올바른 장부로 받아들일 것입니다.

6. 앨리스는 실제로는 가지고 있지 않은 $2 를 사용해 헨리에게 과자 하나를 삽니다. 헨리가 아는 한, 다른 사람에게서 확인한 모든 장부에 앨리스가 $2 를 가지고 있는 것으로 기록되어 있기 때문에 헨리는 앨리스의 거래를 받아들입니다.
7. 앨리스는 이제 과자를 두 개 가지고 있고 시스템에는 가짜 돈 $4 가 만들어졌습니다. 앨리스는 협력의 대가로 친구들에게 과자를 나눠주고, 앨리스와 친구들은 지금까지의 과정을 네트워크에 새로 들어오는 모든 사람을 대상으로 100 번 반복합니다.
8. 결국 앨리스는 모든 과자를 가지게 되고 다른 사람의 수중에는 가짜 돈만 남게 됩니다.
9. 사람들이 앨리스에게서 받은 돈을 쓰려고 하면 네트워크의 과반수를 지배력을 가진 데이빗, 이브, 파라는 가짜 돈을 쓰는 해당 지불 거래를 거부하게 됩니다.

이를 *컨센서스 실패(consensus failure)*라고 부릅니다. 위 사례의 네트워크 참여자들은 진실이 무엇인지에 대해 하나의 컨센서스를 형성하지 못했습니다. 이런 문제를 해결할 더 나은 해결책이 없는 상황에서 다수결의 원칙을 통해 정직하지 않은 사람들이 네트워크의 지배력을 차지하고 가짜 돈을 만들어 쓰는 상황으로 이어졌습니다.

누구든 허락 없이 네트워크에 참여할 수 있는, *승인이 필요 없는(permissionless)* 시스템을 만들기 위해서는 정직하지 않은 참여자의 행동에도 망가지지 않을 시스템이 필요합니다.

분산 컨센서스 문제의 해결 (Solving the Distributed Consensus Problem)

이제 우리는 일부 참여자가 정직하지 않거나 신뢰할 수 없는 상황에서 분산 컨센서스에 도달하는 방법을 찾으려 합니다. 비잔틴 장군 문제(Byzantine Generals Problem)라고 불리는 이 문제는 컴퓨터 과학 분야의 최고 난제 중 하나이자, 사토시 나카모토가 비트코인을 발명하는데 활용한 열쇠이기도 합니다. 어떤 장부가 사실대로 정직하게 거래를 기록했는지 알 수 없는 상황에서 전체 장부의 기록에 대해 많은 사람들이 컨센서스에 도달하도록 하는 것이 문제입니다.

이 문제에 대한 순진한 접근법은 정직한 관리자를 임명하는 방법입니다. 모두가 장부를 작성하는 대신 샬럿, 개리, 프랭크, 조 같은 거짓말 안하고 주말에도 나가 놀지 않는 참한 친구들을 뽑아 장부 작성을 전담시킵니다.

이제 거래를 처리할 때마다 네트워크 참여자 모두에게 거래를 알리는 대신, 우리는 샬럿과 친구들에게만 연락합니다. 샬럿과 친구들이 새 거래를 장부에 반영한 뒤 나머지 참여자들에게 새로운 거래의 반영 사항과 업데이트된 장부를 배포하고 참여자들은 새로운 장부를 각자 백업으로 보관합니다.

이 시스템은 한동안 잘 작동하지만, 어느 하루 정부 요원이 찾아와 이 사적 금융 시스템의 책임자를 소환합니다. 정부는 샬럿과 친구들을 체포해 가두어 이 분산 장부 시스템의 종지부를 찍습니다. 남은 네트워크 참여자들은 각자 서로 믿을 수 없는 백업 장부를 가지고 있지만 누구의 백업 장부를 기준으로 새로운 시스템을 시작해야 할 지 결정할 수 없습니다.

정부는 시스템을 완전 폐쇄하는 대신 장부 관리자들을 형량으로 협박하여 (불법적 상품을 거래하는 것으로 의심 중인) 앨리스와 관련된 거래를 승인하지 못하도록 막을 수도 있습니다. 이제 네트워크는 실질적으로 중앙 통제에 놓이게 되며, *승인이 필요 없는(permissionless)* 시스템이라고 보기 어려워집니다.

민주주의적 접근법은 어떨까요? 50 명의 정직한 사람들을 찾아 매일 선거를 통해 이 중 누가 장부를 기록할 권한을 가질 지 결정하도록 해보겠습니다. 네트워크 참여자 전체가 투표권을 가집니다.

이 시스템은 일부 참여자가 앞선 사례와 같은 목적을 달성하기 위해 아래와 같이 폭력이나 금전적 압력을 행사하여 무너질 수 있습니다.

1. 특정 장부 관리자가 당선되도록 유권자에 압력을 행사.
2. 가짜 거래기록을 반영하거나 특정 거래를 반영하지 않도록 당선된 장부 관리자에 압력을 행사.

문제는 바로 여기에 있습니다. 장부 관리를 위해 특정 사람을 임명해야 할 경우에는 그 사람이 정직할 것을 믿어야 하며, 다른 사람의 압박을 통해 정직하지 않은 행동이나 정부를 훼손하는 일이 일어나지 않도록 막을 수 있는 방법이 없다는 것입니다.

신원 오인과 시빌 공격 (Mistaken Identity and Sybil Attacks)

지금까지 두 가지 실패 사례를 살펴보았습니다. 첫번째는 특정 장부 관리자를 지정하는 방법이었고, 두번째는 선출된 사람이 돌아가며 장부 관리자가 되는 방법이었습니다. 이 두가지 방법이 실패한 이유는 시스템에 대한 신뢰의 기초가 실제 세계의 신원(identity)과 연결되어 있기 때문입니다. 앞서 살펴본 방법에서는 장부를 관리할 개개인의 신원을 구체적으로 확인해야만 했습니다. 개인의 신원을 시스템의 기초로 삼게 되면 시스템은 시빌 공격(Sybil Attack)에 노출됩니다. 시빌 공격이란 다중인격장애를 가진 실제 여성인 시빌(Sybil)의 이름에서 따온 용어로, 신원 위조(impersonation)을 뜻하는 전문 용어로 이해하시면 됩니다.

친구로부터 갑작스레 이상한 메시지를 받은 뒤 친구의 휴대폰이 해킹 됐었다는 것을 알게 된 경험이 있나요? 수억, 수조 달러의 돈이 걸린 일이라면 많은 사람들이 휴대폰을 훔쳐내어 거짓 메시지를 보내기 위해 어떤 종류의 폭력도 행사할 준비가 되어있을 것입니다. 따라서 장부 관리자가 애초에 어떤 방식으로도 압력을 받을 수 없도록 막는 것이 매우 중요합니다.

추첨 방식 (Let's Build a Lottery)

폭력이나 뇌물을 통해 사람들이 위협받을 가능성을 없애기 위해서는 참여자가 너무나 많아 그 모두에게 압력을 행사하는 것이 비현실적인 시스템을 구축해야 합니다. 누구든지 시스템에 참여할 수 있고, 폭력이나 투표 매수 등 압력의 목표가 될 수 있는 어떤 종류의 투표 과정도 필요 없어야 합니다.

그렇다면 추첨을 통해 매번 무작위로 누군가를 뽑아 장부 기록의 권한을 부여하면 어떨까요? 아래는 이런 시스템 디자인의 초안이 되겠습니다.

1. 어느 누구든 모두가 참여할 수 있는 시스템. 수만 명의 사람들이 제한 없이 이 장부 관리자 추첨에 참여할 수 있어야 합니다.
2. 돈을 쓰고 싶을 때에는, 이전에 다룬 방식처럼 네트워크 전체에 희망 거래내용을 알려야 합니다.
3. 모두가 거래를 기록하는 대신, 장부에 거래를 기입할 권리를 추첨을 통해 당첨된 사람에게 부여합니다.
4. 당첨자로 뽑힌 사람은 자신이 받은 모든 거래 내역을 장부에 반영합니다.

5. 당첨자가 장부에 모든 네트워크 참여자가 합의한 규칙에 따라 적법한(valid) 거래만 반영하면 그 대가로 수수료를 받습니다.
6. 모든 참여자가 위 당첨자가 기록한 거래가 반영된 장부의 사본을 보유합니다.
7. 참여자 대부분이 가장 최근 거래가 반영된 장부로 업데이트 할 수 있도록 잠시 시간을 가진 뒤, 다시 다음 번 추첨을 진행합니다.

이 시스템의 개선점은 다음과 같습니다. 이 시스템은 참여자의 신원을 알 수 없고, 다음 당첨자가 누가 될지 알 수 없기 때문에 현실적으로 참여자에 압력을 가하기 어렵게 되었습니다.

그러나, 우리는 아직 구체적 책임자 없이 어떻게 이런 추첨 과정을 운용할지, 당첨자가 정직하게 장부를 기록할지 믿어야 할지에 대한 뚜렷한 답은 찾지 못했습니다. 다음 챕터에서 이에 대한 해답을 찾아보겠습니다.

3. 작업 증명 (PROOF OF WORK)

앞서 디자인한 추첨 시스템에는 두가지 중요한 문제가 남아 있습니다.

1. 이미 어떤 중앙집권화된 신뢰 기관이 없는 시스템을 만들기로 결정한 상황에, 누가 추첨을 위한 복권을 팔고, 당첨 번호를 정할 것인가?
2. 당첨자가 어떻게 나머지 사람들을 속이지 않고 적법한 거래만을 장부에 기록할 것이라고 보장할 것인가?

누구든지 참여할 수 있는, *승인이 필요 없는(permissionless)* 시스템을 만들기 위해서는 특정 참여자에 대한 신뢰에 의존하지 않도록 *신뢰가 필요 없는(trustless)* 시스템이어야 합니다. 이런 시스템은 다음 속성들을 갖추어야 합니다.

1. 어떤 중앙집권적 기관도 신뢰할 필요가 없으려면, 누구든지 추첨 복권을 만들 수 있어야 합니다. 미국의 파워볼(Powerball) 같이 일반적 중앙집권화된 추첨 시스템은 무작위 숫자가 찍힌 복권을 만드는 관리책임자가 존재합니다. 중앙집권적 기구에 의존하지 않으려면 결국 모두가 각자 복권 번호를 만들 수 있어야 합니다.
2. 추첨에 참여하는데 비용이 발생하여 누군가 공짜로 무수히 많은 복권을 만들어내 추첨 확률을 독점해버리는 상황이 벌어지지 않도록 만들어야 합니다. 복권에 가격을 매기고 파는 별도의 관리책임자가 없이 어떻게 추첨에 참여하는데 비용이 발생하도록 만들까요? 추첨에 참여하려면 높은 비용을 가진 물리적 에너지를 사용해야만 하도록 만들어야 합니다.
3. 당첨자가 정당히 당첨되었다는 사실을 누구든지 쉽게 검증할 수 있어야 합니다. 파워볼의 사례에서는 관리책임자가 당첨 번호를 생성합니다. 분산화된 시스템에서 관리책임자를 둘 수는 없으나, 대신 모든 참여자가 합의한 특정 범위의 숫자를 미리 당첨 번호로 정해 놓고 추첨 번호가 그 범위에 들어올 참여자가 당첨되도록 할 수는

있습니다. 이를 위해 해시 함수(hash function)라고 부르는 암호학 기법을 활용하겠습니다.

작업 증명: 에너지 집약적 비대칭 퍼즐 (Proof of Work: an Energy Intensive Asymmetric Puzzle)

이 세가지 모든 문제에 대한 우아 한 해법이 바로 작업 증명(Proof of Work)입니다. 작업 증명은 사실 비트코인 훨씬 이전, 1993 년에 발명되었습니다. 작업 증명의 정확한 작동 원리는 아마도 비트코인을 이해하는데 있어 가장 어려운 부분일 수 있습니다. 따라서, 다음 몇 개의 챕터를 통해 작업 증명의 원리를 천천히 세부적으로 살펴보도록 하겠습니다.

추첨에 참여할 수 있는 "복권"을 무한정 복권을 찍어내지 못하도록 복권을 만드는 비용이 충분히 높을 필요가 있습니다. 무엇이 만드는데 비용이 들면서, 어떤 중앙 기구의 통제에도 놓이지 않을까요?

이 대목에서 물리학이 적용됩니다. 열역학 제 1 법칙에 따르면 에너지는 만들어 지지도 없어지지도 않습니다. 다시 말해, 에너지에 있어서 공짜 점심이란 있을 수가 없습니다. 전력은 전력생산자에게서 구매하거나 직접 발전기를 돌리기 위한 생산비용이 항상 수반됩니다. 어느 쪽이든 전력을 얻는데 비용이 든다는 사실은 바뀌지 않습니다.

작업 증명의 개념은 주사위를 굴리는 것과 비슷한 랜덤한 과정에 참여하는 것입니다. 다만 작업 증명은 6 개의 경우를 가진 정육면체 주사위 대신, 우주 전체에 원자 수와 맞먹는 무수한 경우의 수를 가진 주사위를 사용합니다. 이 작업 증명 주사위를 굴리기 위한 연산과정에서 참여자의 컴퓨터는 전력을 소모해 참여자에게 비용을 일으킵니다.

추첨에 당첨되기 위해서는, 장부에 반영할 거래 기록에서 수학적으로 도출된 숫자에 주사위 값을 더한 복권 값을 생성해야 합니다. 이때 당첨 숫자를 찾기 위해서는 주사위를 수억, 수조, 수경 번 굴려야 될 수 있어 수천 달러 어치 에너지가 사용됩니다. 이 모든 과정이 무작위로 진행되기 때문에 중앙집권적 기구 없이도 누구든 난수(random number)를 생성하는 컴퓨터와 장부에 반영할 거래기록 목록을 이용해 각자의 복권을 만들 수 있습니다.

당첨 숫자를 찾는 데에는 수천 달러 어치의 에너지가 사용될 수 있지만, 다른 사람들이 당첨자의 숫자를 검증하는 데에는 몇 가지 간단한 확인만 진행하면 됩니다.

1. 당첨 숫자가 모두 미리 합의한 목표 숫자(Target Number) 범위 안의 숫자인가?
2. 당첨 숫자가 장부에 반영하고자 하는 거래 목록에서 수학적으로 도출된 숫자인가?
3. 당첨자가 반영하려는 거래가 비트코인의 규칙에 어긋나지 않는가?
   (이중 지불(double spending)이 아닐 것, 비트코인의 발행 일정에 어긋나지 않을 것 등)

작업 증명 시스템의 중요한 속성은 *물리적 비용을 발생시킨다(real world costly)*는 점입니다. 따라서 작업 증명 시스템에서 참여자에게 압력을 행사해 네트워크를 공격하려면, 각 참여자의 집에 찾아가 컴퓨터를 탈취해야 할 뿐 아니라 그 전기세 고지서도 대신 납부해야 하는 것입니다.

각 참여자들은 이렇게 에너지를 사용했다는 것을 어떻게 증명할 수 있을까요? 이를 설명하기 위해 컴퓨터 공학의 기본 개념인 해시(hashing)와 비트(bits)를 간단히 살펴보도록 하겠습니다.

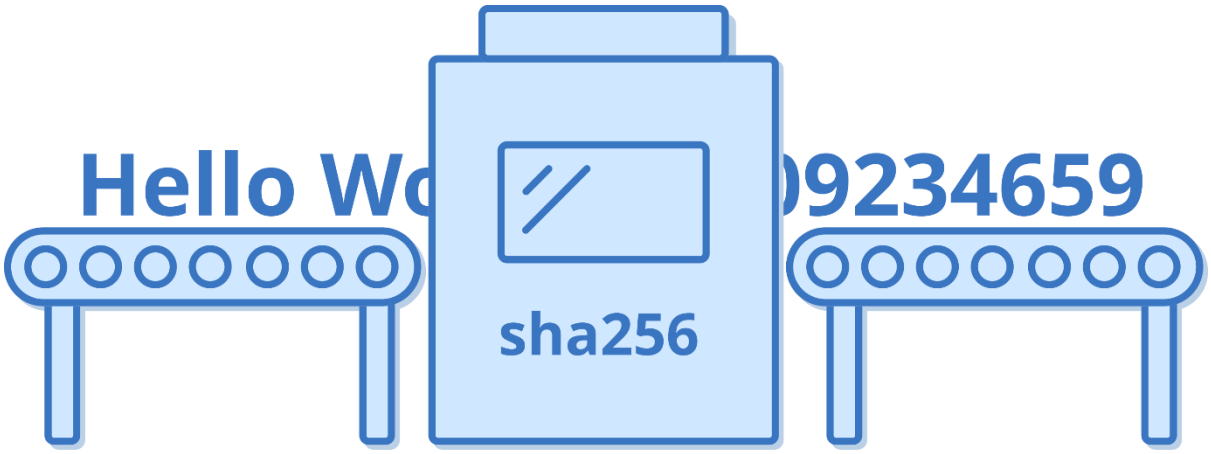
해시 (Hashing)

비트코인의 비대칭 작업 증명 퍼즐은 해시 함수(hash function)를 활용합니다. 기본적으로 대수학(algebra)에서 함수란 *입력 값* x에 대응하는 *결과 값* $f(x)$로 이루어져 있습니다. 예를 들어 함수 $f(x) = 2x$ 는 입력 값에 2 를 곱합니다. 따라서 입력 값 $x = 2$ 는 결과 값 $f(x) = 4$ 를 도출합니다.

해시 함수는 특별한 함수로, 임의의 문자, 숫자, 또는 데이터를 집어넣으면 언뜻 무작위의 큰 숫자가 나오는데 아래는 "Hello World"라는 단어를 해시 함수에 입력한 결과입니다.

111181171325821924266132935775749045845 5
489044664361600112658434663354150209 5

위에서 "Hello World"라는 입력 값을 해시 연산하기 위해 활용된 해시 함수가 sha256 라고 불리는 해시 함수로, 비트코인이 사용하는 해시 함수입니다.



해시 함수에 데이터가 입력되면 예측할 수 없는 큰 숫자가 결과로 산출됩니다.

해시 함수 sha256 에는 다음과 같은 유용한 속성이 있습니다.

1. 결과 값은 결정성(deterministic)을 가집니다. 각 입력 값의 결과 값은 변하지 않고 항상 같습니다.
2. 결과 값은 예측할 수 없습니다. 입력 값에 문자 하나를 바꾸거나 띄어쓰기 하나만 바뀌어도 결과 값이 극단적으로 바뀌어, 최초 입력 값에 따른 결과 값을 전혀 예측할 수 없습니다.
3. 입력 값이 아무리 커져도 해시 결과 값을 빨리 연산할 수 있습니다.
4. 같은 결과 값에 대응하는 두 개의 해시 값(string)이 없습니다.
5. 결과 값으로 거꾸로 입력 값을 도출할 수 없습니다. 이런 함수를 일방 함수(one-way function)이라고 합니다.
6. 결과 값은 256 비트로 항상 동일한 데이터 크기를 가집니다.

비트의 간단한 개념 정리 (A Quick Primer on Bits)

우리에게 익숙한, 0 에서 9 까지의 숫자로 구성된 숫자 시스템은 10 개의 수로 이루어져 *십진법(decimal)*이라고 부릅니다. 반면, 컴퓨터는 보통 전기 신호가 있고 없음을 나타내는 1 과 0 으로만 이루어진 숫자 시스템을 사용하며, 이를 *이진법(binary)*이라고 부릅니다.

십진법에서 우리는 0 부터 9 까지의 *아라비아 숫자(digits)*만을 활용합니다. 아라비아 숫자 한 단위로 나타낼 수 있는 값은 0 부터 9 까지, 총 열 개입니다. 아라비아 숫자 두 단위로는 00, 01 에서 99 까지 총 10 x 10 = 100 개의 다른 값을 나타낼 수 있습니다. 세 단위의 경우 000, 001 에서 999 까지 총 10 x 10 x 10 = 1,000 개의 다른 값을 나타낼 수 있습니다.

이제 패턴이 보이기 시작했을 것입니다. 십진법에서 숫자 N 개의 단위로 나타낼 수 있는 값의 종류가 몇 개인지 계산하려면, 10 을 N 번 제곱하면 되며 수학적으로는 10^N 또는 10 의 N 승으로 표시합니다.

이진법도 방식은 동일합니다. 한가지 다른 점은 값을 나타내는데 활용할 수 있는 숫자의 개수입니다. 십진법이 열 개의 아라비아 숫자를 활용하는데 반해, 이진법의 *이진법 숫자(binary digit)*, 다시 말해 *비트(bits)*에는 영과 일의 두가지 값만 존재합니다.

1 비트가 두 개의 값을 나타낼 수 있다면, 2 비트는 00, 01, 10, 11 의 네 가지 값을 나타낼 수 있습니다. 이는 총 2 x 2 = 2^2 = 4 개로 계산할 수 있습니다.

3 비트는 000, 001, 010, 011, 100, 101, 110, 111 로 총 2 x 2 x 2 = 2^3 = 8 개의 값을 나타낼 수 있습니다.

N 단위의 이진법 수는 2^N 개의 다른 값을 나타낼 수 있습니다.

따라서, sha256 해시 함수의 크기인 256 비트를 통해 나타낼 수 있는 고유한 값은 총 2^{256} 개입니다. 이는 상상도 하기 힘든 큰 숫자입니다. 십진법으로 표현하면 이는 총 78 자리의 숫자입니다. 이해를 돕기 위해 비교해보자면 이는 현재까지 알려진 우주 전체에 있을 것으로 추산되는 모든 원자의 수와 비슷한 값입니다.

2^{256}=115,792,089,237,316,195,423,570,985,008,687,907,
853,269,984,665,640,564,039,457,584,007,913,129,639,936

위 숫자가 sha256 해시 함수에 입력 값을 넣었을 때 얻을 수 있는 가능한 모든 결과 값의 개수입니다. 따라서, sha256 해시 함수의 결과 값을 예측하기란 불가능합니다. 이는 동전 던지기의 결과를 256 번 연속으로 맞추거나, 우주 전체에서 무작위의 특정 원자 위치를 맞추는 것과 같은 일입니다.

결과 값이 매번 모두 표기하기에는 너무 길기 때문에 앞으로는 2^{256} 으로 줄여서 표기하도록 하겠지만, 이 숫자가 얼마나 상상하기 어려울 정도로 큰 수인지 감을 잡으셨기를 바랍니다.

해시 연산 해보기 (Let's Hash Some Strings)

다음은 몇 가지 문자열과 해당 문자열의 SHA-256 해시 값입니다. 실제 컴퓨터는 0 과 1 의 이진법으로 계산하고 표시하겠지만 아래에서는 십진법으로 표현하였습니다.

핵심은 입력한 문자열이 조금만 변해도 결과 값이 얼마나 완전히 다른 값이 되는지 확인하는 것입니다. 해시 함수 SHA-256 의 결과 값은 입력 값을 통해 예측할 수 없습니다.

"Hello world!"
52740724284578854442640185928423074974
81806529570658746454048816174655413720

"Hello world!!"
95863319874939535731602344194643497258 3
74513872780665335270495834770720452323

어떤 사람도, 어떤 컴퓨터도 위 sha256 함수의 결과 값을 토대로 원래 입력 값이 무엇이었는지 알아낼 수 없습니다. SHA-256 해시 함수를 좀 더 다루어 보고 싶으시면 https://passwordsgenerator.net/sha256-hash-generator/ 링크를 활용하시기 바랍니다.

작업 증명 추첨을 위한 해시 연산 (Hashing to Win the Proof of Work Lottery)

자, 이제 진짜 마법을 다룰 준비가 되었습니다. SHA-256 함수의 결과 값은 2^{256} 가지 경우의 수를 가지고 있다는 점을 확인한 바 있지만, 논의의 목적 상 1,000 가지의 해시 결과 값이 가능하다고 가정해보겠습니다.

추첨 방식은 다음과 같습니다.

1. 앨리스가 $2 를 밥에게 송금하겠다는 의사를 공표합니다.
2. 네트워크 참여자 모두가 "앨리스가 밥에게 $2 를 송금하다"라는 거래 정보 끝에 *논스(nonce)*라고 하는 일회용 숫자를 추가합니다. 이 논스로 인해 모두의 입력 문자열과 해시 결과 값이 달라지고 당첨 숫자를 가려낼 수 있습니다.
3. 만약 해시 값이 다음 챕터에서 다룰 *목표 숫자(Target Number)*보다 작으면 당첨 숫자가 됩니다.
4. 만약 해시 값이 목표 숫자보다 크면, 논스 값을 바꾸어 다시 해시 연산을 합니다. "앨리스가 밥에게 $2 를 송금하다 nonce=12345"에서 "앨리스가 밥에게 $2 를 송금하다 nounce=92435", 다시 "앨리스가 밥에게 $2 를 송금하다 nounce=132849012348092134" 등으로 계속 논스 값을 바꾸어 가며 목표 숫자보다 작은 해시 값을 찾을 때까지 해시 연산을 이어갑니다.

목표 숫자보다 낮은 해시 값을 찾으려면 연산을 무한정 반복해야 할 수 있습니다. 실제로, 목표 숫자를 조정하여 당첨 숫자를 찾는데 걸리는 시간을 확률적으로 통제할 수 있습니다. 결과 값 경우의 수가 1,000 개라면 목표 숫자를 100 으로 설정하였을 때 해시 값이 목표 숫자보다 낮을 확률을 추측할 수 있습니다.

계산은 단순합니다. 경우의 수 1,000 개 중 목표 숫자보다 낮은 수가 100 개라면 해당 수가 나올 확률은 100 / 1,000 = 10%가 됩니다. 따라서 특정 해시 함수가 1,000 개의 다른 결과 값을 만들어 낸다면, 목표 숫자 100 미만의 해시 값이 생성될 확률은 10%입니다.

비트코인의 추첨 방식은 이렇게 진행됩니다. 네트워크 참여자가 합의한 목표 숫자를 토대로, 네트워크 상 공표된 거래 기록을 묶어 무작위의 논스를 추가한 후 해시 값으로 변환합니다. 누군가 목표 숫자 미만의 해시 값을 산출하면 그 결과를 다음과 같이 네트워크 전체에 발표합니다.

여러분!

- 저는 다음 거래기록을 전송받았습니다: "앨리스가 밥에게 $2 를 송금하다, 샬럿이 앨리스에게 $5 를 송금하다".
- 저는 다음 논스를 추가하였습니다: "32895".

- 위 문자열은 목표 숫자 100 미만의 해시 값 42 를 산출하였습니다.
- 저의 작업 증명은 다음과 같습니다: 거래기록 데이터, 추가된 논스 값, 위 문자열에 따라 산출된 해시 값.

당첨 숫자를 찾은 사람은 해당 해시 값을 산출하기 위해 수억 번의 해시 연산을 반복하고 수천 달러의 전력을 사용했을 수 있지만, 다른 사람들은 당첨자의 작업을 즉시 검증할 수 있습니다.

해시 함수의 입력 값(거래기록과 논스)과 그에 대응하는 결과 값(해시 숫자)가 알려져 있기 때문에 누구든 동일한 해시 연산을 직접 반복하여 실제 당첨자가 제공한 데이터를 검증할 수 있습니다.

해시 연산은 거래기록을 포함하는 문자열 입력 값에 따라서 영부터 우주 전체의 원자 개수가 결정되는 거대한 주사위를 굴리는 작업으로 생각할 수 있습니다. 목표 숫자 미만의 주사위 값이 나오면 당첨이 되며, 당첨자는 해당 해시 값을 산출한 데이터를 공개해야 합니다.

이 모든 작업이 어떻게 전력 사용으로 이어질까요? 모든 해시 값의 경우의 수는 우주에 있는 모든 원자의 개수와 비견될 만하다고 설명한바 있습니다. 이때 목표 숫자를 설정하기에 따라 일부 극소수의 해시 값만이 목표 숫자 미만이 되도록 정할 수 있습니다. 이는 곧 목표 숫자 아래의 해시 값을 산출하기 위해 수많은 연산 시간과 그에 따른 전력이 소요된다는 의미입니다.

목표 숫자가 낮아질수록 해시 값을 찾기 위한 연산 시도가 더 많이 필요하게 됩니다. 목표 숫자가 높아지면 해시 값을 찾기 위한 연산과정은 더 빨라지게 됩니다. 목표 숫자 미만의

해시 값을 찾을 확률이 백만 대 일이라면 해당 해시 값을 찾았음을 증명하여 백만 번의 연산을 진행했음을 증명하게 됩니다.

4. 채굴 (MINING)

작업 증명(Proof of Work)을 통해 비트코인 장부에 기록할 수 있는 권한을 추첨하는 방식을 흔히 *채굴(mining)*이라고 부릅니다. 다음은 채굴의 원리입니다.

1. 채굴을 하려는 사람은 누구든, 컴퓨터를 사용해 비트코인 네트워크에 접속해 네트워크 상에 공표되는 거래를 수신하는 것으로 참여할 수 있습니다.
2. 앨리스가 몇 개의 비트코인을 밥에게 보내려는 거래의사를 네트워크 상에 공표합니다. 네트워크 상의 컴퓨터가 서로 소문을 퍼뜨리듯 이 거래의사를 네트워크 전체로 퍼뜨립니다.
3. 추첨에 참여하려는 모든 컴퓨터는 네트워크 상 공표된 거래의사를 목록으로 묶은 뒤 논스(nonce)를 추가하여 SHA-256 해시 함수 연산을 진행합니다.
4. 평균적으로 대략 매 10 분마다 당첨자가 목표 숫자보다 낮은 해시 값을 산출해냅니다.
5. 당첨자는 당첨 숫자에 해당하는 해시 값과 그 입력 값(거래기록 및 논스)을 네트워크에 공표합니다. 이 과정은 몇 시간이 걸릴 수도, 몇 분이 걸릴 수도 있습니다. 거래기록, 논스, 작업 증명 해시 정보를 모두 합쳐서 *블록(block)*이라고 부릅니다.
6. 당첨자가 아닌 모든 사람들이 거래기록과 논스를 합친 입력 값으로 해시 연산을 재수행하고, 결과 값이 목표 숫자보다 낮은지, 블록이 무효한 거래를 포함하고 있지 않은지, 이전 블록의 거래기록과 모순되는 점이 없는지 확인하여 블록을 검증합니다.
7. 모두가 새로운 블록을 장부에 반영하고 기존 블록 사슬에 덧붙임으로써 *블록체인(blockchain)*을 생성합니다.

여기까지입니다. 우리는 막 블록을 처음 생성하고 장부에 처음으로 반영해보았습니다.

여러분은 아마 미디어를 통해 비트코인 채굴 과정에서 복잡한 연산 문제를 해결하는 과정이 포함되어 있다는 내용을 여러 차례 들어 보았을 것입니다. 이제 여러분은 그것이 사실이 아니라는 것을 알고 있습니다. 비트코인 채굴 과정은 복잡한 연산 문제를 해결하는 과정이라기보다, 거대한 가상의 주사위를 굴려 특정 값 사이의 결과 값을 얻는 과정이라고 볼 수 있습니다. 이는 전력 비용을 야기하는 단순한 확률 게임입니다.

새로운 비트코인은 어떻게 주조되나요? (How are New Bitcoins Minted?)

지금까지 앨리스가 밥에게 어떻게 $2를 송금하는지 알아보았습니다. 앞으로는 달러 이야기는 더 하지 않도록 하겠습니다. 비트코인 그 자체는 달러와는 사실 전혀 무관하기 때문입니다. 비트코인은 비트코인 네트워크 상 가치 값을 나타내는 디지털 단위 그 자체일 뿐입니다.

앞선 사례를 다시 살펴보면, 실제 앨리스가 "자산 명의의 계좌"에 등록되어 있는 2 개의 비트코인을 밥에게 송금하겠다는 의사를 네트워크에 공표하여 2 개의 비트코인을 송금한 것으로 해석할 수 있습니다. 이후, 작업 증명 추첨에 당첨된 누군가가 앨리스가 공표한 거래 내역을 장부에 반영하게 됩니다.

이때, 앨리스가 가지고 있던 2 개의 비트코인은 애초에 어디에서부터 온 것일까요? 비트코인은 어떻게 시작되었으며, 지금처럼 달러 같은 법정통화를 통해 비트코인을 매입할 수 있기 전 어떻게 비트코인을 획득할 수 있었을까요?

비트코인을 처음 만들 때, 사토시는 2,100 만개의 비트코인 모두를 자신이 가진 것으로 데이터베이스를 만든 후 다른 사람들에게 비트코인을 판매할 수도 있었습니다. 그러나, 이 경우 한 사람이 모든 부를 독점하고 있는 시스템에 다른 사람들이 가치를 부여할 이유가 부족합니다. 계정 등록을 통해 이메일을 이용해 가입하는 사람에게 코인을 당첨 받을 수 있게 할 수도 있지만, 이런 방식은 수백만 개의 이메일 주소를 만드는 것이 거의 공짜에 가깝기 때문에 *시빌 공격* (신분 위조)에 취약합니다.

사실, 작업 증명 추첨을 거친 뒤 장부 작성 권리를 획득하는, 일련의 채굴 과정이 바로 새로운 코인을 만드는 과정이기도 합니다. 많은 양의 에너지를 소요해 당첨 해시 값을 찾아, 적합한 블록을 찾으면 네트워크에 공표된 어떤 거래내역이든 블록에 포함하여 비트코인 장부에 반영할 권리를 획득합니다. 이때 당첨자는 *추가적으로* 특별한 거래내역을 장부에 반영할 수 있게 되는데, 이를 *코인베이스 거래(coinbase transaction)*라고 부릅니다. 이

코인베이스 거래의 내용은 기본적으로 다음과 같습니다: "12.5 개의 비트코인이 새롭게 주조되어 채굴 활동을 통해 이 블록을 채굴한 보상으로 채굴자 매리에게 제공되었습니다."

이렇게 새로운 비트코인이 주조됩니다. 이 과정으로 인해 중앙집권적 기구 없이도, 신분을 밝히지 않아도, 채굴 과정에 필요한 전력 비용만 감당할 수 있으면, 세계 누구든 새로운 비트코인을 주조할 수 있게 됩니다. 이 채굴 과정으로 인해 비트코인 주조 과정은 *시빌 공격*을 견뎌낼 수 있게 됩니다. 코인을 갖고 싶으면 에너지를 소요하거나 돈을 지불하여 채굴을 해야 하는 것입니다.

블록 보상(The Block Reward)

당첨자는 일정량의 새로 주조된 비트코인을 가지게 됩니다. 왜 수천 개가 아니라 굳이 12.5 개일까요? 규칙을 어기고 원하는 양만큼 가지고 가버릴 수 없는 걸까요?

비트코인은 *분산 컨센서스* 시스템입니다. 이는 곧 무엇이 적정한 것인지 모든 참여자가 합의해야만 한다는 뜻입니다. 전체 합의에 이르기 위해 참여자는 각자의 컴퓨터를 통해 비트코인 컨센서스 규칙이라고 부르는 규칙을 검증합니다. 네트워크 상 모든 블록은 이 규칙에 따른 검증을 거칩니다. 블록이 검증을 통과하면 모두가 해당 블록을 각자의 장부에 기록하고 블록 상 거래내용은 사실로 입증됩니다. 검증을 통화 못한 블록은 거부됩니다. 컨센서스 규칙 전체는 다소 복잡하지만, 아래는 몇 가지 예시입니다.

- 검증 완료된 신규 블록은 비트코인 소프트웨어에 정해져 있는 고정된 발행 일정에 따른 특정양의 새 비트코인을 주조합니다.
- 거래기록은 관련 거래자가 지출을 승인했음을 확인할 수 있는 서명을 포함해야 합니다.
- 새로운 블록과 이전 블록에서 이미 지출한 코인을 지출하는 거래기록이 없어야 합니다.
- 블록에 포함된 데이터 크기가 일정 용량 이하여야 합니다.
- 블록의 작업 증명 해시가 목표 숫자보다 낮아야 합니다. 블록이 목표 숫자보다 낮은 해시를 가지고 있다는 사실이 해당 블록을 채굴하는데 실제로 전력을 소모하였음을 통계확률적으로 증명합니다.

메리(Mary)가 자신이 채굴한 블록에 컨센서스 규칙보다 많은 신규 비트코인을 주조하려고 한다면 다른 모든 컴퓨터가 메리가 채굴한 블록을 *부적합한(invalid)* 블록으로 분류하고 *기각(reject)*하게 됩니다. 모두가 실행하고 있는 비트코인 클라이언트 소프트웨어에는 "현재 블록 보상(Block Reward)은 정확히 비트코인 12.5 개이며, 다른 수의 비트코인을 주조한 블록은 채택하지 말 것" 이라는 명령이 들어있습니다.

메리가 규칙을 어기고 *부적합한* 블록을 만들려고 해도 아무도 그 블록을 각자의 장부에 반영하지 않을 것이고, 결과적으로 메리는 아무도 원하지 않는 위조 코인을 만드는데 전력만 낭비한 셈이 됩니다. 비트코인은 이런 방식을 통해 디지털 화폐의 선구자인 닉 사보(Nick Szabo)가 Shelling Out 이라는 에세이를 통해 확립한 개념인 *위조할 수 없는 높은 생산비용(unforgeable costliness)*을 확보하게 됩니다. 위조하기 쉬운 돈이 돈으로서 가치가 없을 것이란 점은 직관적으로 이해할 수 있습니다. 비트코인은 간단한 수학식을 통해 진품여부를 가려낼 수 있기 때문에 위조가 불가능한 것입니다.

사토시는 최초로 주조된 비트코인을 포함한 가장 첫 번째 블록, *제네시스 블록(genesis block)*을 채굴했습니다. 비트코인의 오픈 소스 코드를 통해 누구든 제네시스 블록 채굴이 어떻게 진행되었는지 들여다볼 수 있고 어떤 속임수는 없었는지 직접 검증할 수 있습니다. 사토시 또한 제네시스 블록을 채굴하기 위해 수십억 번의 계산을 반복해 작업 증명 추첨에 참여해야 했습니다. 비트코인 시스템의 설계자임에도 전력을 소모하지 않고 특혜를 누리거나 속임수를 쓸 수가 없었습니다.

사토시 이후에 네트워크에 참여한 누구라도 제네시스 블록의 해시를 목표 숫자와 거래 내역과 대조하여 사토시가 실제로 전력을 소모하여 통계적으로 희소한 목표 숫자를 산출했음을 확인할 수 있습니다. 법정 화폐 기반의 전통적 금융 시스템을 이러게 명확하게 실시간으로 검증하는 것을 상상이나 할 수 있을까요!

반감(The Halving)

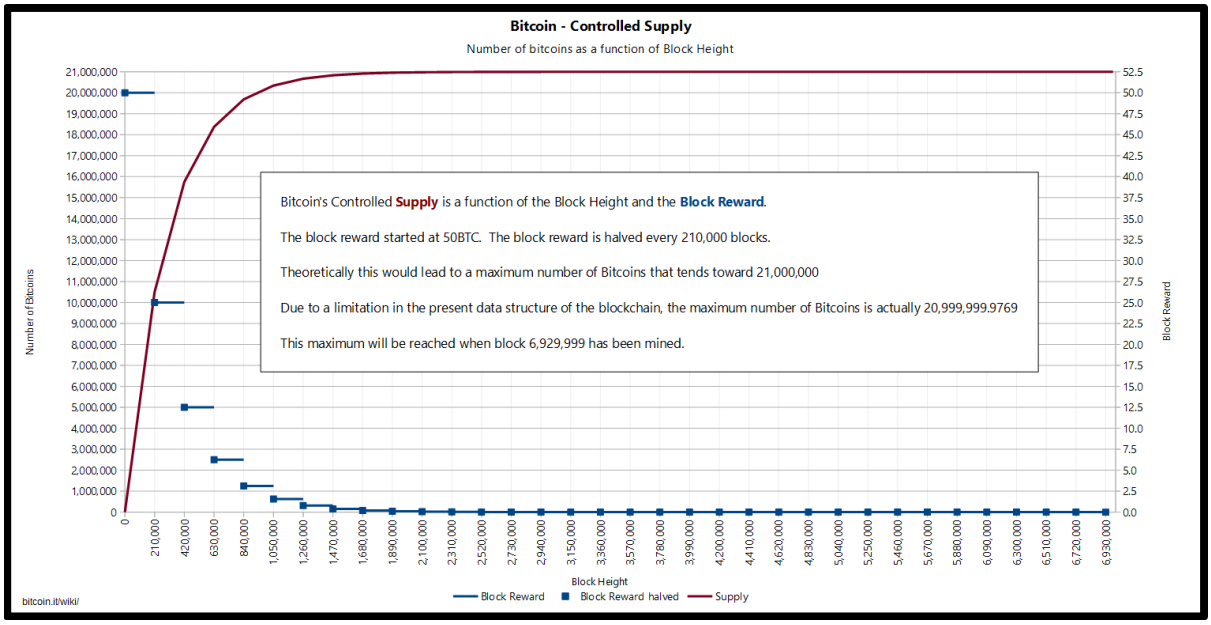
채굴 과정에서 새로운 비트코인이 주조됩니다. 사토시는 *희석(debase, 통화 가치 하락)*되지 않는 시스템을 만들고자 했습니다. 사토시는 통화 공급량이 무한정 증가하기를 바라지 않았습니다. 대신 사토시는 발행율이 초기에는 높다가 점점 줄어들어 궁극적으로 신규 발행이 완전히 멈추는 발행 일정을 설계했습니다.

최초 블록 보상은 비트코인 50 개였습니다. 비트코인 초기 채굴자와 마찬가지로, 사토시가 채굴한 제네시스 블록이 주조한 비트코인이 50 개였습니다.

비트코인 코드는 블록 보상 반감기(Block Reward Halving)를 통해 대략 4 년 주기로 블록 보상을 절반으로 감소시킵니다. 반감기는 시간의 경과가 아니라 채굴된 블록 수를 기준으로 결정되지만, 대략 매 10 분마다 새로운 블록이 채굴되기 때문에 시간을 기준으로 보아도 대체로 무방합니다.

블록 보상은 2008 년 50 개, 2012 년 25 개, 2016 년 12.5 개였습니다. 2019 년 6 월 8 일 현재 기준으로 비트코인의 탄생 이래 579,856 개 블록이 채굴되었으며 새로운 블록 당 비트코인 보상은 12.5 개입니다.

50,144 개 블록이 추가 채굴된 후인 2020 년 5 월쯤이면 블록 보상은 6.25 개로 줄어들고, 매년 신규 비트코인 공급량은 약 1.8% 수준으로 떨어집니다. 두 번의 반감기를 더 거친 10 년 후에는 비트코인 총공급예정량의 99% 이상의 채굴이 끝나고 블록 보상은 비트코인 1 개 미만으로 줄어듭니다. 블록 보상 반감기(Block Reward Halving) 진행 상황은 bitcoinblockhalf.com 을 통해 확인할 수 있습니다.



https://en.bitcoin.it/w/images/en/4/42/Controlled_supply-supply_over_block_height.png

결국 약 2140 년경이 되면 블록 보상은 완전히 사라지고, 채굴자는 거래자가 지불하는 거래 수수료를 통해서만 보상 받게 됩니다.

이 발행 일정과 블록 보상 체계는 오픈 소스 비트코인 코드에 강제되어 있고, 이전에도 설명한 바 있지만, 누구든 그 내용을 검증할 수 있습니다. 따라서 비트코인의 역사가 길어지더라도 이런 규칙을 지키지 않는 블록은 같은 규칙을 기반으로 검증하는 모든 검증자에게 거부당합니다.

발행 일정과 채굴 기간 간격(Controlling the Issuance and Mining Interval)

채굴에는 컴퓨터와 전력이 필요합니다. 따라서 더 많은 하드웨어와 전력을 통제할수록, 다른 사람에 비해 작업 증명 추첨 번호를 찾을 확률은 올라갑니다. 예를 들어, 네트워크 상 동일 전력을 소모하는 100 대의 컴퓨터가 있고 여러분이 10 대의 컴퓨터를 통제하고 있다면 전체 채굴 블록의 *대략 10% 정도*를 채굴하게 됩니다. 하지만, 채굴은 확률과 무작위에 기반한 과정이기 때문에 몇 시간, 길게는 며칠 동안도 블록이 채굴되지 않을 가능성도 있습니다.

이전 챕터를 통해 채굴자가 마음대로 자신이 받을 블록 보상 규모를 정할 수 없음을 살펴보았습니다. 규칙을 따르지 않은 채굴자의 블록은 다른 노드가 거부하게 됩니다. 하지만 만약 채굴 과정을 가속시킬 정도로 많은 전력을 쏟아부어 많은 양의 비트코인을 확보하고, 정해진 발행 일정을 가진 비트코인 시스템의 설계구속조건(design constraint)을 위반한다면 어떻게 될까요?

가능한 해시 경우의 수가 단 천 개에 불과하고 목표 숫자가 100 인 사례로 다시 돌아가 보겠습니다. 각 해시 연산 시 목표 숫자 100 이하의 숫자를 산출해 블록을 채굴할 확률은 10%입니다.

각 해시 연산에 1 초가 걸린다고 가정해보겠습니다. 매초 거래 기록과 무작위의 논스를 해시로 전환하는 연산을 통해 일종의 "주사위"를 굴리면, 유효 해시를 찾는데 평균 10 초가 걸릴 것으로 기대할 수 있습니다.

연산 컴퓨터가 두 대라면 어떨까요? 해시 연산은 두 배로 빨라지고 5 초 내에 유효 해시를 찾을 것이라고 기대할 수 있습니다. 연산 컴퓨터가 10 대라면 어떨까요? 매초 10 대의 컴퓨터 중 하나는 유효 해시를 찾을 것입니다.

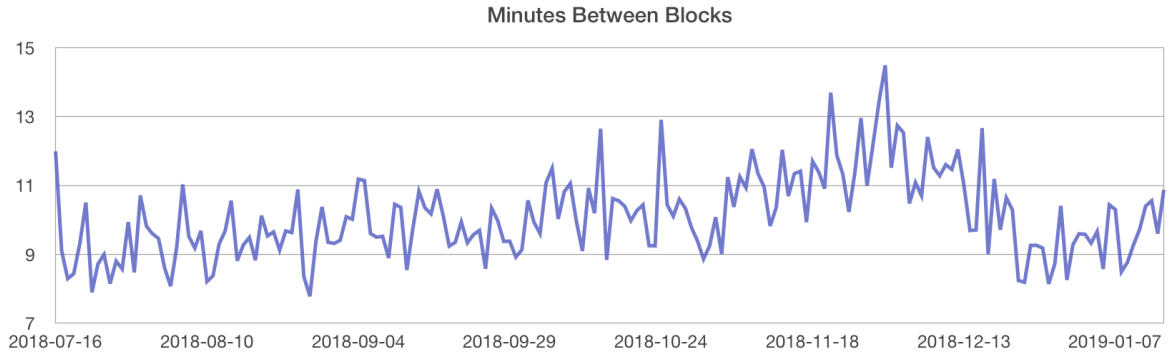
여기에서 문제가 생깁니다. 채굴자가 많아질수록, 블록 채굴 주기가 빨라진다는 것입니다. 이는 두 가지 원하지 않는 결과로 이어집니다.

1. 예정된 발행 일정에 차질이 생깁니다. 2140 년경 모든 발행이 완료되고 발행 시기가 더 빨라지지 않도록 일정을 지키기 위해서는 비트코인 발행 속도가 매 순간 상대적으로 일정한 수준이어야 합니다.
2. 네트워크 컨센서스에 문제가 발생합니다. 블록이 너무 빨리 채굴되어 새로운 블록의 내용이 네트워크 전체에 도달하기도 전에 다음 블록이 채굴되어 버리면, 네트워크 전체가 공유하는 하나의 거래기록 컨센서스에 도달할 수 없습니다. 여러 채굴자가 같은 거래내용을 블록에 포함시켜 다른 블록에서 이미 지불된 거래를 포함한 부적합 블록으로 이어지게 되기 때문입니다.

또한, 채굴자 수가 줄어들면 반대의 문제가 생깁니다.

1. 비트코인 생성 주기가 너무 늦어지면서, 예정된 발행 일정에 다시 차질이 생깁니다.
2. 거래가 장부에 반영되기까지 몇 시간, 며칠, 혹은 그 이상이 소요되면서 비트코인 시스템이 불안정해질 수 있습니다.

비트코인 네트워크의 채굴자 전체의 초당 해시 연산 횟수를 *해시율(hash rate)*라고 부릅니다.



각 블록 간 시간은 해시율의 변동과 무작위 확률에 따라 달라집니다.

난이도 조정: 목표 숫자 도출(Difficulty Adjustments: Agreeing on the Target)

비트코인은 자발적이고 승인이 필요 없는(voluntary and permissionless) 시스템으로, 누구든 언제나 참여할 수 있고 중앙 관리자가 없기 때문에 특정 시점의 채굴자 수는 크게 변할 수 있습니다. 따라서 채굴자 수가 변하더라도 블록 채굴 속도가 빨라지지도 느려지지도 않도록 일정하게 유지할 방법이 필요합니다.

비트코인의 발행 일정과 블록 시간이 일정하도록 추첨에 참여하는 채굴자가 많아지면 해시를 찾기 어렵게 조정하고 채굴자가 줄어들면 해시를 찾기 쉽게 조정하려면 어떻게 해야 할까요?

비트코인 채굴이란 목표 숫자보다 낮은 무작위 숫자를 연산하는 추첨 과정이라는 점을 떠올려 보겠습니다.

저기 작은 공간을 맞추는 것이 목표입니다. 전체 산출 가능한 결과값이 너무나 많기 때문에 목표 숫자보다 낮은 결과값을 산출하기 위해서는 오랫동안 수 없이 많이 주사위를 굴려야만 합니다.

비트코인은 이 문제를 *채굴 난이도 조정(mining difficulty adjustment)*을 통해 해결합니다. 모두가 같은 규칙을 따르고, 해당 시점까지의 블록 기록을 갖고 있고, 같은 코드를 실행하고 있기 때문에 모두가 독립적으로 블록이 얼마나 빨리 만들어지고 있는지 계산할 수 있습니다.

대략 2 주에 걸쳐 매번 2016 개의 블록이 만들어질 때마다[2], 해당 기간 동안 블록을 만드는데 걸린 시간을 계산해서 목표 숫자를 조정하여 블록 생산 속도를 올리거나 낮춥니다.

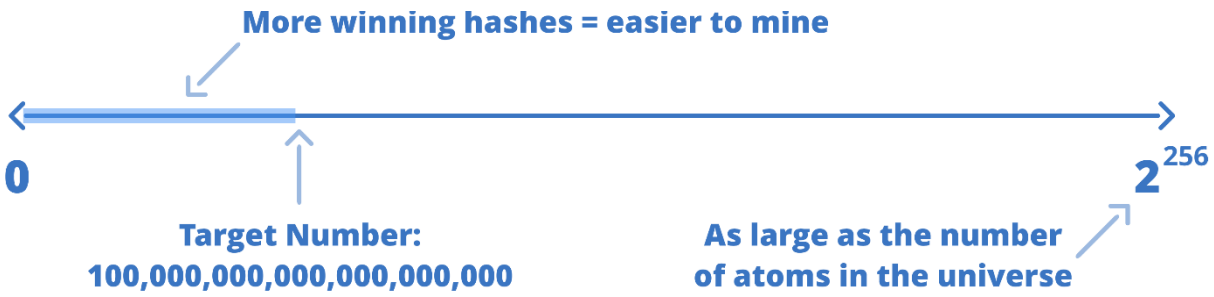
---

[2] 조정 기간에 해당하는 2016 개의 블록은 목표 블록 생성 기간인 10 분을 기초로 산출됐습니다. 10 분 x 2016 개 블록은 약 2 주입니다. 이 블록 기간은 대부분의 노드가 최신 블록까지 싱크 하기까지 충분하다고 생각되는 기간을 사토시가 임의적으로 정한 기간입니다.

모두가 최근 2016 개의 블록을 생성하는데 소요된 시간을 2016 으로 나누어 블록 하나를 만드는데 평균적으로 걸린 시간을 산출합니다. 평균 시간이 10 분을 넘기나요? 그렇다면 너무 느린 것입니다. 평균 시간이 10 분에 못 미치나요? 그렇다면 너무 빠른 것입니다.

이제 오픈 소스 코드를 통해 10 분을 기준으로 더 빠른지 느린지에 따라서 목표 숫자를 비례적으로 조정할 수 있게 되었습니다.

목표 숫자를 높이면 적정 해시가 많아져 채굴자가 정답 해시를 찾을 확률이 높아지고 블록에 소요되는 에너지가 줄어듭니다. *난이도를 낮추는 것*입니다.



목표 숫자를 높이면 맞춰야 되는 공간이 늘어나면서 맞출 확률이 높아지고, 소요된 에너지의 관점에서 비용도 낮아집니다.

마찬가지로, 목표 숫자를 낮추어 적정 해시가 적어져 채굴자가 적정 블록 해시를 찾기 위해 더 많은 에너지를 소요하게 됩니다. *난이도를 올리는 것*입니다.

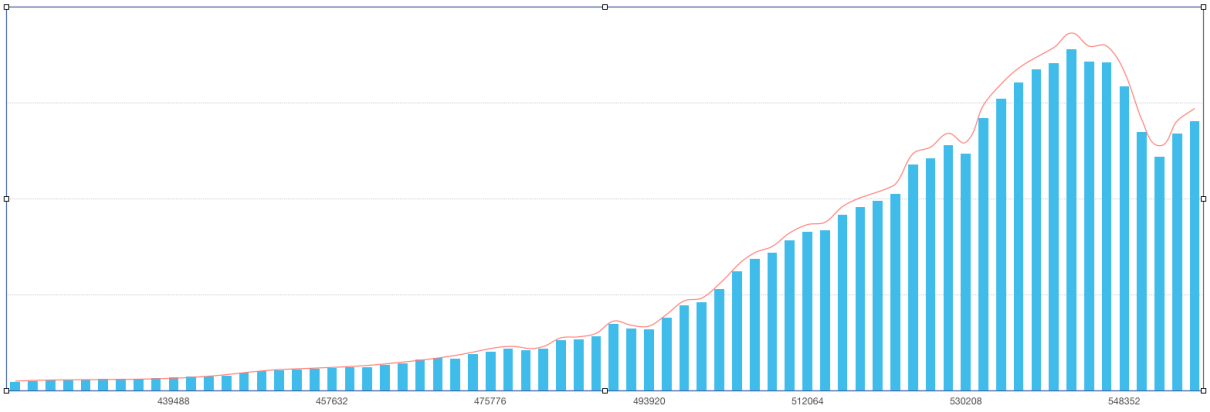
이는 다른 의미로, 2016 개 블록 기간 동안 목표 숫자가 무엇인지 정확히 알 수 있다는 뜻입니다. 해당 기간 동안 생성될 블록에 대해 작업 증명 해시 값의 당첨 기준이 되는 마법의 숫자인 셈입니다.

난이도 조정과 목표 숫자 산출은 비트코인이 이룬 혁신 중 하나로, 누구든 독립적으로 목표 숫자를 계산하여 추첨 숫자의 당첨 여부를 검증할 수 있게 됩니다. 이 방식을 통해 당첨 숫자가 무엇인지 알려주는 관리자 없이도 추첨을 진행할 수 있습니다.

---

2 주의 조정기간은 다소 임의적으로 정한 기간이지만, 해시율의 급격한 변동에 따라 시스템이 휘둘리지 않도록 방지하는 역할을 하기도 합니다.

아래 차트는 시간에 따른 해시율을 선으로, 난이도를 바로 나타내고 있습니다. 난이도는 2016 개 블록마다 조정되기 때문에 계단식으로 나타납니다. 해시율이 난이도를 넘어갈 때마다 난이도가 계단식으로 상승하며 해시율을 따라잡는 것을 확인할 수 있습니다. 2018 년 10 월부터 12 월까지처럼 해시율이 떨어질 때에는 난이도도 계단식으로 떨어집니다. 난이도 조정은 항상 2016 개 블록의 난이도 기간 (2 주) 동안의 해시율에 뒤쳐져 따라 움직입니다.



해시율 vs. 난이도

2016 개 블록 기간만큼 난이도 조정에 시차가 있기 때문에, 해시율의 급격한 변동이 발생하면 해당 2016 개 블록 기간 동안 비트코인 생산 속도가 목표보다 빨라질 수도 늦어질 수도 있고 발행 일정에 다소 차질이 발생합니다.

해시율이 늘어난다는 것은 대체로 대량의 신규 하드웨어가 생산된다는 뜻이기에, 해시율의 급증은 드물며 그리 큰 영향을 미치지 않습니다. 해시율이 급변하더라도 그 영향은 2016 개 블록에 한정되고, 다음 난이도 조정을 통해 평균 블록 생산 기간은 10 분으로 돌아갑니다.

해시율과 비트코인 가격(Hash Rate and the Dollar Value of Bitcoin)

비트코인이 자동으로 난이도를 조정하는 기준은 모든 추첨 참가자의 연산 능력인데, 이는 곧 채굴자가 해시 연산에 소요되는 에너지의 양이기도 합니다. 이 부분이 바로 물리 세계와 디지털 세계가 만나는 지점입니다. 비트코인의 가격, 하드웨어와 에너지의 가격, 난이도를 반영한 목표 숫자가 서로 피드백 순환고리를 만듭니다.

1. 투자자와 투기자가 가격이 올라갈 것을 기대하고 비트코인을 매수하여 가격을 X 달러로 올립니다.
2. 채굴자는 채굴에 비트코인 하나당 최대 X 달러까지 에너지와 하드웨어에 지출합니다.
3. 매수자의 높은 수요가 가격을 높이고, 높아진 수익성에 따라 더 많은 채굴자가 채굴에 뛰어듭니다.
4. 채굴자가 늘어나는 것은 곧 해시율 증가, 비트코인 생산에 소요되는 에너지의 증가, 네트워크 보안의 상승을 의미합니다. 매수자는 비트코인의 보안에 대해 더 확신을 얻을 수 있으며, 이는 때로 더 가격을 올리는 피드백 순환고리로 이어지기도 합니다.
5. 2016 개 블록이 생성된 후, 올라간 해시율을 반영해 난이도가 상향 조정됩니다.
6. 난이도가 올라간다는 것은 목표 숫자가 낮아진다는 의미입니다. 블록을 찾기 어려워지면 채굴자의 운용비용은 올라가게 됩니다.
7. 채굴에 소요되는 운용 비용이 채굴 비트코인을 매각해서 얻는 수익보다 높아지면서 채굴자 일부가 손실을 기록하기 시작합니다. 해당 채굴자들이 채굴 하드웨어 운용을 멈추면서 전체 해시율이 하락합니다.
8. 또 다른 2016 개의 블록이 생성됩니다. 채굴자 일부가 오프라인 상태가 되면서, 난이도는 이전보다 쉬워지게 재계산됩니다. 목표 숫자는 상승합니다.
9. 난이도가 낮아지면서 이전까지 수익성이 없었던 채굴자도 다시 온라인 상태로 돌아와 채굴을 시작하고, 새로운 채굴자도 유입됩니다.
10. 1 단계부터 다시 반복합니다.

하락장에서는 사용자가 코인을 매도하고, 가격 하락을 이끌어, 채굴자의 수익성이 악화되는 방식으로, 사이클이 반대 방향으로 진행될 수 있습니다.

난이도 조정 알고리즘을 통해 비트코인 가격과 채굴에 참여 중인 총 해시율은 항상 균형을 되찾습니다. 가격이 큰 폭으로 하락해 현재 해시율이 절반으로 줄어들어도, 다음 난이도 조정을 통해 새로운 균형 가격 수준에서 채굴은 수익성을 회복합니다.

난이도 조정은 본질적으로 비효율적 채굴자를 밀어내고 가장 저렴한 에너지와 낮은 운용비용을 바탕으로 한 채굴자를 보상합니다. 따라서 시간이 지날수록 채굴자는 충분히

활용되지 않았거나 완전히 새로운 에너지원을 찾아 지구상 점점 더 외딴 곳으로 밀려나갈 것입니다. 코인쉐어즈(CoinShares)는 2019 년 보고서[3]를 통해 비트코인 채굴의 약 75%가 신재생 에너지를 활용하고 있는 것으로 추산했습니다.

지난 몇 년간 비트코인 가격은 총 해시율과 함께 매우 가파르게 올랐습니다. 다음 블록에 무엇이 기록될지 결정할 수 있는 권리를 얻기 위해서는 네트워크 전체 대비 과반의 에너지와 하드웨어를 수중에 두어야 하기 때문에, 해시율이 높아질수록 네트워크를 공격하기는 그만큼 어려워집니다. 오늘날 비트코인 네트워크에 들어가는 에너지는 어지간한 국가 수준과 맞먹습니다.

수수료와 블록 보상의 소진

블록 보상이 완전히 소진되면 채굴자가 에너지를 들여 네트워크 보안을 유지하도록 어떻게 인센티브를 줄 수 있을까요? 이에 대한 비트코인의 답은 거래 수수료입니다. 거래 수수료는 점진적으로 블록 보상을 대체할 뿐 아니라, 대체로 채굴자가 블록 보상만을 위해 빈 블록을 생산하지 않을 유인을 제공하기도 합니다.

거래 수수료는 한정된 자원인 블록 공간에 대한 사용자의 수요를 바탕으로 자유 시장 시스템을 통해 결정됩니다. 거래를 송신하는 사용자는 채굴자에게 지불하고자 하는 거래 수수료는 표시하고 채굴자는 그 거래 수수료 수준에 맞추어 해당 거래의 블록 포함 여부를 결정합니다. 다음 블록에 포함되기를 기다리는 거래 내용이 많지 않을 때에는 경쟁이 없어 수수료가 매우 낮습니다. 블록 공간이 점점 더 채워지면서 자신의 거래가 확정되는 시점이 늦춰지지 않기를 바라는 사용자는 더 높은 수수료를 감수하게 됩니다. 높은 수수료를 감수할 의향이 없는 사용자는 언제든 블록 공간에 여유가 많아질 때까지 좀 더 기다리기로 결정할 수 있습니다.

전통적 금융 시스템에서 거래 수수료는 거래 규모의 일정 비율로 결정되는 경우가 많습니다. 비트코인에 있어 거래 규모는 거래 수수료와 연관성이 없습니다. 대신 수수료는 거래에 필요한 희소 자원인 블록 공간의 크기에 비례합니다. 수수료는 소비된 블록 공간 바이트 (byte, 8 비트) 당 사토시 (Satoshi, 1 억 분의 1 비트코인) 단위로 측정됩니다. 따라서 백만

[3] 현재 채굴 상황에 대한 자세한 내용은 다음 보고서를 통해 확인하시기 바랍니다. https://coinshares.co.uk/bitcoin-mining-cost-june-2019/

비트코인을 일대일로 전송하는 거래가 비트코인 하나를 10 명의 수신자에게 나누어 송금하는 경우보다 블록 공간을 적게 차지하기 때문에 수수료도 저렴할 수 있습니다.

과거 2017 년 말 거대한 상승장처럼 비트코인의 수요가 매우 높았던 기간이 있었습니다. 이 기간에는 거래 수수료가 매우 높아졌었습니다. 그 이후로 비트코인 네트워크에 수수료 상승 압력을 덜어줄 몇 가지 새로운 기능이 추가되었습니다.

이 중 하나가 블록 데이터의 표시 방식을 수정한 Segregated Witness 입니다. Segregated Witness 의 정확한 원리는 이 책이 다루는 범위를 벗어나지만, 이를 적용한 거래는 기존 1MB 의 블록 공간 이상을 사용할 수 있게 됩니다.

수수료 상승 압력을 해소하는 다른 방안은 배칭(batching)입니다. 비트코인 생태계 내 거래소나 거래가 잦은 다른 참여자가 여러 유저의 비트코인 거래를 하나의 거래로 묶는 것입니다. 은행이나 페이팔(PayPal)을 통한 전통적 송금과 달리 비트코인 송금은 여러 입금과 출금을 한 거래로 합칠 수 있습니다. 따라서 100 명에게 각각 출금을 진행해야 하는 거래소는 이를 하나의 거래로 처리할 수 있습니다. 이 방법을 통하면 블록 공간의 효율이 매우 향상되어, 초당 몇 건에 불과한 비트코인 거래가 수 천 건의 거래로 향상될 수 있습니다.

세그윗(SegWit, Segregated Witness)와 배칭을 통해서 블록 공간의 수요 압력이 많이 감소했습니다. 또한, 블록 공간 효율성을 향상시킬 여러 추가 개선안이 계속 적용될 예정입니다. 그럼에도 불구하고 수요가 계속 늘어나고 블록 공간이 모자라게 되면 비트코인 수수료가 높아지는 시기는 다시 찾아올 것입니다.

이제 비트코인의 개발을 거의 마쳤습니다.

1. 중앙 은행을 분산 원장(distributed ledger)으로 대신했습니다.
2. 원장을 작성할 사람을 정하는 추첨 방식을 도입했습니다.
3. 추첨 참가자가 추첨에 참여하기 위해서 해시 연산의 방식으로 에너지를 소모할 수밖에 없도록 만들고, 각자 독립적으로 계산한 목표 숫자를 기준으로 당첨자의 해시 값과 비교하는 방식으로 모두가 당첨자의 진위를 쉽게 검증할 수 있게 만들었습니다.

4. 추첨 참가자가 규칙을 어기면 *코인베이스 거래(coinbase transaction)*를 포함해 해당 참가자의 블록을 기각해, 당첨되더라도 이익을 볼 수 없도록 만들어 부정 행위의 경제적 유인을 낮추고 네트워크 규칙을 준수할 경제적 유인을 높였습니다.
5. 참여자 모두가 명시된 규칙과 최근 2016 개 블록 기록을 바탕으로 각자 목표 숫자를 산출할 수 있도록 목표 숫자 재계산 시점과 계산방식을 확립했습니다.
6. 해시율의 증감에 따라 난이도 조정을 통해 비트코인 발행 일정이 변하지 않도록 고정시켰습니다.
7. 오픈 소스 코드를 통해 참여자 모두가 거래의 적정성, 블록 보상, 난이도 계산에 같은 규칙이 적용되고 있는지 직접 검증할 수 있도록 만들었습니다.

이제 중앙 기구가 필요 없어졌습니다. 완전히 분산되고 탈중앙화된 시스템을 확립했습니다. 이제 거의 모든 그림이 완성되었습니다. 하지만 한가지 문제가 남아있습니다. 네트워크에 새로 참여하는 참여자가 장부를 요청했을 때, 다른 노드로부터 각각 다른 히스토리를 가진 장부를 받을 가능성이 있습니다. 어떻게 해야 하나의 선형적 히스토리를 확립하여 채굴자가 과거 기록을 수정할 수 없도록 막을 수 있을까요?

5. 비트코인의 보안 (SECURING THE LEDGER)

지금까지 추첨 시스템과 컨센서스 형성을 통한 입증을 활용해 강압이나 부정을 막으면서 분산화 장부를 보관하고 작성하는 방법을 다루었습니다.

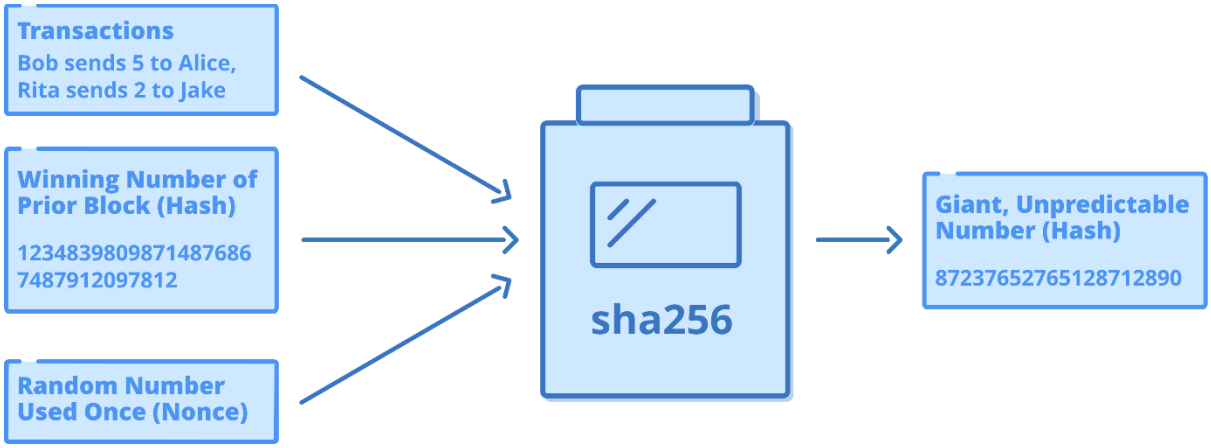
하지만 당첨자가 악의를 품으면 어떻게 될까요? 채굴자가 과거 장부 기록을 변경할 수 있지 않을까요? 이브(Eve), 데이브(Dave), 파라(Farrah)의 사례처럼 악의를 품은 참여자가 결탁하여 과거 기록을 바꾸거나 잔고를 조작하고 더 많은 코인을 탈취할 수 있는 건 아닐까요?

바로 이 부분에 활용되는 것이 *블록체인(blockchain)*입니다. 이제는 테크 산업에서 널리 퍼진 마케팅 용어가 되어버린 블록체인은, 사실 여러 개의 비트코인 *블록(blocks)*을 *사슬처럼 이어붙여(chained)* 각 거래기록의 묶음을 연결시키는 방법에 불과합니다. 이 방법을 통해 2009 년 사토시의 *제네시스 블록(genesis block)*부터 오늘날까지의 모든 코인 발행과 지출의 기록이 단일한 선형적 히스토리를 확립합니다.

이전 챕터에서 논의의 편의를 위해서 다루지 않은 부분이 있습니다. 작업 증명 추첨(Proof of Work lottery)을 통해 채굴을 진행할 때 해시 함수의 투입 값은 블록에 기록될 거래 기록과 랜덤한 논스(nonce) 뿐만이 아닙니다. 직전 블록의 해시 값도 추가하여 직전 블록과 다음 번 블록을 연결합니다.

해시 함수의 결과 값이 예측할 수 없고 모든 입력 값에 따라 크게 바뀐다는 점을 떠올려 보시기 바랍니다. 이제 블록 해시 값에 다음 세가지 입력 값이 포함됩니다.

1. 장부에 기록하려는 거래 기록
2. 랜덤한 논스(nonce)
3. 장부의 히스토리 상 직전 블록의 해시 값



추첨에 활용되는 해시 연산의 세가지 입력 값에는 이제 직전 블록의 당첨 해시 값이 포함되어, 직전 블록과 다음 블록을 잇는 연결고리가 됩니다.

위 방식을 통해 모든 블록을 이어 붙여 사토시가 채굴한 최초 블록, 제네시스 블록까지 이어지는 블록의 역사를 확립할 수 있게 됩니다. 새로운 블록을 연결할 때 해당 블록이 이전 다른 블록에서 이미 지출된 비트코인을 사용하는 거래가 없는지 검증해야만 합니다.

해시 입력 값이 조금이라도 바뀌면 해시 결과 값은 예측할 수 없이 급격하게 바뀝니다. 과거 블록 내 데이터를 조작하면 그 결과 값도 바뀌게 됩니다. 하지만 그 해시 값이 다음 블록의 해시 함수 입력 값으로도 사용되었기 때문에, 다음 모든 블록의 해시 값도 연쇄적으로 바꾸어 버리게 됩니다. 가장 마지막 블록의 해시 값은 이전 모든 해시 값과 연결되어 있는 셈이기 때문에 해당 시점까지 블록 연결고리 상 모든 기록에 대한 지문과 같은 역할을 하는 것입니다!

작업 증명(Proof of Work) 방식은 모두가 목표 숫자(Target Number)를 바탕으로 각 블록에 얼마나 에너지가 소요되었는지 알 수 있기 때문에 부정행위가 통하지 않습니다. 누군가 과거 블록을 바꾸고 싶다면 바꾸려는 블록의 작업 증명 해시는 물론, 그 블록 이후의 모든 블록의 해시 값을 모두 재계산해야만 합니다. 블록체인 조작은 쉽게 눈에 띌 뿐만 아니라, 조작에 *소요되는 비용은 막대합니다(extremely costly).*

새로운 블록이 채굴될 때마다 해당 시점까지의 작업 증명 해시를 재계산하는데 필요한 전력이 늘어나기 때문에, 실질적으로 해당 블록 이전의 모든 블록의 보안이 강화됩니다. 오늘날 비트코인을 다루는 사업체 대부분은 특정 블록 이후에 6 개의 추가 블록이 채굴된 블록의 거래 기록을 최종적인 것으로 간주합니다. 오늘날 해시율을 고려했을 때 여섯 개

분량의 해시 연산을 재계산하려면 막대한 양의 에너지가 소요될 것입니다. 100 개 전의 블록을 바꾼다? 불가능이라고 봐야합니다.

블록체인의 기록을 다운로드하면 각 블록의 모든 거래 기록이 투명하게 공개되며 작업 증명 해시를 직접 검증하여 어떤 내용도 조작되지 않았음을 확인할 수 있습니다.

블록 충돌

컨센서스 시스템을 완성하는데 한가지 요소가 남아있습니다. 어떻게 해야 채굴자가 동시에 두 개의 블록을 채굴하고 모두에게 전송해도 모두가 동일한 선형의 거래기록을 확립하게 만들 수 있을까요?

전세계적인 네트워크를 운용한다고 상상해보시기 바랍니다. 미국에서부터 중국까지, 세계 각지의 사람들이 이 글로벌 네트워크에 접속해 작업 증명 채굴 추첨(Proof of Work mining lottery)에 참여한다고 상상해보시기 바랍니다.

시카고에서 누군가가 유효 블록을 채굴합니다. 이 사실이 네트워크에 공시되고 미국 전역에 있는 컴퓨터에 그 내용을 수신합니다. 한편, 상하이에서도 시카고에서 유효 블록이 채굴된 시점과 불과 몇 초 차이로 누군가 유효 블록을 채굴합니다. 중국에는 아직 미국에서 블록이 채굴된 사실이 알려지지 않았고, 중국 사람들은 오히려 중국에서 채굴된 블록의 소식을 먼저 접합니다.

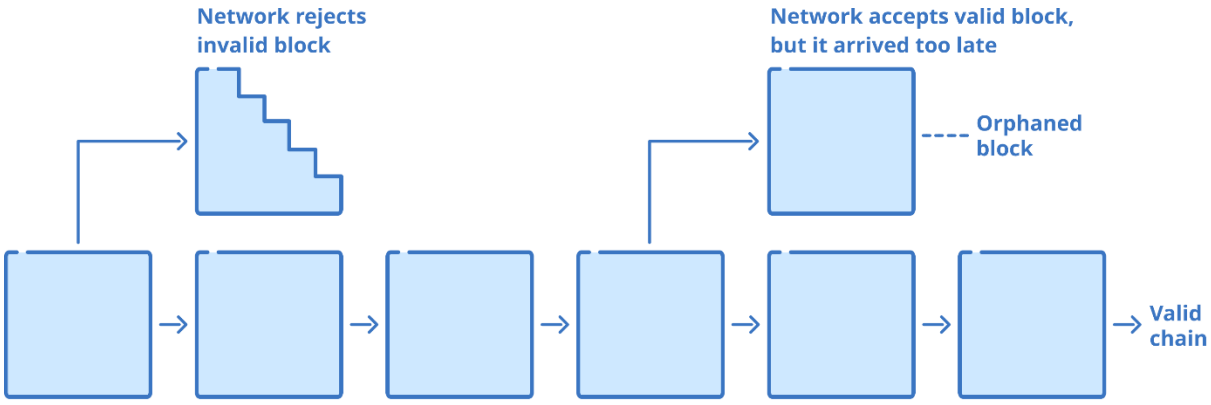
두 가지 블록 모두 1 개의 비트코인을 앨리스가 밥에게 송금하는 거래를 담고 있습니다. 하지만, 해당 비트코인을 수신한 즉시 밥은 찰리에게 다시 그 비트코인을 송금합니다. 미국 블록은 이 거래를 반영하여 밥의 잔고는 0 으로 기록됩니다. 그러나, 시점 차이로 인해 중국의 블록은 밥이 찰리에게 1 개의 비트코인을 전송한 거래가 알려지기 전에 채굴됩니다. 중국 블록에는 밥의 잔고가 비트코인 1 개로 반영됩니다.

두가지 블록체인이 모두 이전 모든 기록과 연결된 유효한 거래기록을 가지고 있기 때문에, 어떤 블록체인이 올바른 체인인지에 대한 관점에 따라 네트워크가 나뉘게 됩니다. 두가지 블록체인 모두 유효 분량의 작업 증명을 보유합니다. 이런 상황을 *체인 분열(chain split)*이라고 부릅니다. 어느 쪽이 올바른지 판단에 의존할 수 있는 중앙기관은 따로 없습니다. 어떻게 해야 할까요?

비트코인은 간단한 해결책을 제시합니다. 기다려보는 것입니다. 채굴자는 어떤 블록에 이어서 채굴할지 자유롭게 선택할 수 있습니다. 미국 채굴자와 중국 채굴자는 각자 먼저 소식을 접했던 블록에 이어서 채굴을 이어갈 것입니다.

이후 약 10 분이 지나면 새로운 블록이 채굴됩니다. 비트코인 코드 상에는 전체 블록에 소요된 에너지의 합이 가장 큰 체인이 채택된다는 규칙이 있습니다. 각 체인의 작업 증명량을 합하여 가장 누적 작업 증명량이 많은 체인을 유효 체인으로 채택하는 비트코인의 이 핵심 규칙을 사토시의 이름을 따 나카모토 컨센서스(Nakamoto Consensus)라고 부르기도 합니다.

위 사례에서 중국인이 다음 블록을 채굴했다고 가정해 보겠습니다. 이제 중국 체인이 미국 체인보다 총 작업 증명량에서 한 블록을 앞섭니다. 이 사실이 네트워크 상에 공표되면 미국 내 노드는 중국의 노드가 누적 기준으로 더 무거운 작업 증명 체인을 만들었음을 확인하고 *재조직(reorganize, reorg)*을 진행합니다. 이는 중국 체인의 두개 블록을 채택하고 기존 미국 체인의 마지막 블록을 탈락시키는 과정입니다.



체인 분열(chain split)은 채굴자가 각기 다른 블록을 동시에 채굴할 때 발생하는 자연스러운 과정입니다. 총 작업 증명량 기준으로 가장 무거운 체인이 유효 체인으로 채택되고 나머지는 탈락합니다.

탈락된 미국 체인의 마지막 블록을 *오펀(orphan, 고아)*이라고 부릅니다. 해당 블록이 기각되었기 때문에 이 블록을 채굴한 채굴자는 보상을 받지 못하고, 해당 블록에 포함된 어떤 거래도 장부에 반영되지 않습니다. 하지만, 이때 기각된 거래가 유실되지는 않습니다. 일부 거래는 동시에 채굴된 중국 블록에 포함되었을 것이며, 나머지 포함되지 않은 거래도 궁극적으로 향후 블록에 포함되어 장부에 반영됩니다.

채굴자는 네트워크 상 수집된 모든 거래를 멤풀(mempool)이라고 하는 각자 컴퓨터 내 특수한 공간에 저장합니다. 기각된 블록에 포함되었던 거래는 모두 다시 멤풀에 저장됩니다. 해당 거래는 새로운 블록 거래 기록들과 대치되지 않는 한 향후 다른 블록에 포함되어 채굴됩니다.

비록 위 사례에서 여러 노드를 미국 노드와 중국 노드로 지칭했지만 실제로 노드는 서로의 신원이나 지리적 위치를 전혀 모릅니다. 노드에게 필요한 정보는 어떤 체인이 작업 증명량 기준 가장 무거운 체인인지, 그 체인 상 모든 거래가 유효한지(이중지출 검증 등) 여부를 아는 것뿐입니다.

이런 체인 분열은 비트코인에게는 때때로 발생하는 지극히 정상적인 현상입니다. 체인 분열은 보통 다음 블록 생성시 해소됩니다. 이 현상은 채굴자 간에 블록 전파 기술과 네트워크 연결성의 개선을 통해 시간이 갈수록 점차 더 안정화될 것입니다. 현재 비트코인은 블록 하나에 허용된 데이터 용량에 상한을 정해 놓고 있는데, 이는 앞으로도 유지될 비트코인의 특성입니다. 비트코인이 상대적으로 작은 용량의 블록을 10 분의 간격을 두고 생성하는 이유 중 하나가 오펀 블록 생성 확률을 낮게 관리하기 위한 것입니다.

채굴은 확률적 특성을 띠고 있습니다. 때로는 블록 생성에 10 분이 소요되기도 하고 때로는 불과 몇 초 만에 이루어질 수 가능성도 있습니다. 블록이 매초 생성되거나 블록 용량이 매우 크다면 서로 지리적으로 멀리 떨어져 있고 블록 전파에 시간이 오래 걸리는 미국과 중국의 블록은 높은 확률로 충돌을 일으키게 됩니다. 오펀 블록이 너무 자주 발생하면 해당 블록체인은 흐트러지게 됩니다. 오펀 블록 위에 또 오펀 블록이 생성되고, 노드가 마지막 블록 검증을 채 마치기 전에 다음 블록이 채굴됩니다.

새로운 블록이 채굴되기 전에 네트워크 전체가 최신 블록을 수신할 수 있으려면 블록 용량을 작게 유지하는 것이 중요합니다. 또 다른, 어쩌면 더 중요한 이유는 노드를 운용하는 하드웨어 요구사항을 상대적으로 낮게 유지해 시간이 갈수록 더 많은 노드와 채굴의 탈중앙화를 장려하는 것에 있습니다. 블록이 대용량화 되면 채굴자의 수익성에 악영향을 주는 오펀 블록을 생성하지 않기 위해 채굴이 데이터 센터와 특정 지역에 집중될 유인이 높습니다.

하나의 진짜 체인(One True Chain)

챕터 3 에서 헨리가 처음 네트워크에 참가하는 상황으로 돌아가보겠습니다.

헨리의 노드는 네트워크의 다른 노드에 접속하고, 접속한 노드에 연결된 또 다른 노드와 접속하는 식으로 네트워크의 노드를 찾아가는데 이를 노드 탐색(node discovery)이라고 합니다.

새로 연결된 노드 중 일부가 악의를 가지고 헨리의 노드에게 거래 서명이나 적법한 작업 증명 해시가 없는 위조 비트코인을 포함한 거짓 장부기록을 제공할 수 있습니다. 이런 경우, 해당 장부는 완전히 기각되고, 관련 노드는 즉시 헨리 노드에 대한 접근이 금지됩니다[4].

다른 정직한 노드도 서로 상충되는 내용의 장부기록을 가지고 있을 수 있습니다. 예를 들어, 일시적으로 오프라인 상태가 되어 한두 개 블록 분량만큼 장부기록이 뒤처져 있을 수 있습니다. 다운로드한 여러 블록체인 기록이 모두 적법하면서도 서로 다른 내용을 포함하고 있으면, 헨리의 노드 소프트웨어는 나카모토 컨센서스(Nakamoto Consensus) 규칙을 적용해, 누적 증명 작업량이 가장 많은 체인(heaviest cumulative Proof of Work chain)을 진짜 체인을 판단하게 됩니다.

노드들은 끊임없이 서로 정보를 주고받으며 가장 최신 블록을 탐색합니다. 모든 노드가 나카모토 컨센서스 규칙을 동일하게 준수하기 때문에, 무엇이 유일한 진짜 블록체인 기록인지 네트워크 전체에 컨센서스가 형성됩니다. 헨리는 다수의 노드가 악의를 품으면 무너질 수 있는 다수결의 원칙에 의존할 필요가 없어집니다.

헨리가 접속한 수많은 노드가 업데이트 되지 않았거나 적대적인 노드이더라도, 그 중 단 하나의 노드만 정직하다면 헨리의 비트코인 노드 소프트웨어는 태초 제네시스 블록부터 현재까지 누적 증명 작업량이 가장 많은 블록체인, 가장 무거운 블록체인을 바로 가려낼 수 있습니다. 이 점의 중요성은 아무리 강조해도 지나치지 않습니다. 헨리는 누구도 신뢰할 필요없이 노드가 모든 블록체인을 검증하여 찾아낸 진짜 체인을 바로 확인할 수 있습니다.

따라서 적대적인 해커가 거짓 블록체인을 전파하기란 극히 어려운 일입니다. 특정 노드를 어떤 정직한 노드에도 접속할 수 없도록 차단하고, 해커가 통제하는 가짜 노드로만 연결되도록 고립시켜야 합니다.

---

[4] 비트코인에서 부적합한 블록이 어떻게 처리되는지 다음 에세이가 잘 설명하고 있습니다. http://hackernoon.com/bitcoin-miners-beware-invalid-blocks-need-not-apply-51c293ee278b

거래의 가역성(Reversibility of Transactions)

두 개의 서로 다른 체인이 경쟁하는 상황은 보통 확률적으로 발생한 일시적 상태로 곧 해소됩니다. 하지만, 공격자가 전체 네트워크의 50%가 넘는 해시율을 손에 넣으면 나카모토 컨센서스를 이용해 네트워크를 공격할 가능성이 생깁니다. 공격자가 전력 비용만 감당할 용의가 있다면, 과반수의 해시를 이용해 원하는 내용이 담긴 누적 증명 작업량이 가장 많은 체인을 만들어낼 수 있습니다. 이 체인이 네트워크에 송출되면, 다른 노드들도 이 체인을 진짜 체인으로 받아들이게 됩니다. 과반수의 해시율이 필요한 이런 공격을 51% 공격(51% attack)이라고 부릅니다.

51% 공격이나 오펀 블록의 가능성 때문에, 비트코인에는 엄밀한 의미의 거래기록 최종성(finality)이 존재하지 않는다는 점이 중요합니다. 따라서, 비트코인 거래 시 특정 거래기록을 포함한 블록 이후에 몇 개 블록이 더 생성되어야 해당 거래가 확정된 것으로 간주하는 게 통상적입니다. 해당 시점이 되면 거래기록을 뒤집기 위해 필요한 에너지 비용이 워낙 막대해 실제 발생할 가능성이 없습니다.

특정 거래를 포함한 블록 이후에 추가로 생성되는 블록을 확증(confirmation)이라고 부릅니다. 비트코인 거래에 여섯 건의 확증이 있다는 표현은, 그 거래를 포함한 블록 이후에 6 개의 블록이 더 생성되었다는 뜻입니다. 개당 판매가격이 크지 않은 전자서적 판매라면 확증이 하나만 있거나, 하물며 확증이 없어도 네트워크 상에 해당 거래가 송출된 것만 확인하면 전자서적을 제공하는데 문제가 없을 것입니다. 하지만 만약 집을 사고파는 거래라면 12 건의 확증이 생성될 때가지 2 시간 정도 기다리는 것이 나을 수 있습니다. 시간이 지날수록 특정 블록 이후에 투입되는 작업 증명은 늘어나고, 그만큼 해당 거래를 되돌리는데 필요한 전력 비용도 커집니다. 오늘날 통상적으로 여섯 건의 확증이면 대부분의 경우 충분한 결재 증빙으로 간주합니다.

비트코인 해시율이 하락하고 각 블록 생성에 투입되는 전력이 줄어든다면, 언제든지 결제 확증 기준을 늘릴 수 있습니다. 결제 최종성이 없다는 사실은 처음에는 불편한 사실일 수 있지만, 신용카드 거래가 보통 거래일로부터 120 일까지도 결제를 되돌릴 수 있다는 점을 생각해볼 필요가 있습니다.

반면에 비트코인 거래는 불과 몇 개의 블록만 생성되면 사실상 되돌릴 수 없습니다. 이런 관점에서 보면, 오히려 결제대금을 지불 받는 상품 판매자에게는 비트코인의 불가역성(irreversibility)과 최종성(finality)이 전통적 결제 네트워크에 비해 비약적 개선이라고 볼 수 있습니다.

오늘날, 공격자가 국가 규모의 전력자원과 전세계 모든 비트코인 채굴장비를 확보하고 비트코인 네트워크에 투입되는 에너지 전체를 독점적으로 투입하더라도, 지금까지 누적된 블록체인 기록을 전부 재작성해서 더 무거운 블록체인을 생산하려면 일년 이상의 시간이 소요될 것으로 보고 있습니다. 관련 데이터는 웹사이트 http://bitcoin.sipa.be 에서 확인하실 수 있습니다.

6. 포크와 51% 공격 (FORKS AND 51% ATTACKS)

사토시는 첫 번째 비트코인을 채굴할 때 컴퓨터 CPU(central processing unit, 중앙처리장치)를 사용했습니다. 당시에는 채굴 난이도가 높지 않았기 때문에 개인 컴퓨터를 사용할 수 있을 정도로 채굴 비용이 낮았습니다.

시간이 지나 채굴 소프트웨어가 수정을 거듭하고 효율성이 계속 향상되면서, 주로 컴퓨터 게임에 사용되던 특수한 GPU(graphics processing unit, 그래픽처리장치)가 채굴에 활용되게 됩니다.

GPU 를 사용하게 되면서 채굴 효율성은 CPU 채굴과 비교해 수천 배 향상되었습니다. GPU 로 인해 시스템의 해시율이 폭발적으로 증가하면서 채굴 난이도 또한 빠르게 상승했습니다. 이에 따라 CPU 채굴은 수익성을 잃었고 채굴자는 CPU 채굴기를 멈추어야 했습니다.

GPU 채굴의 발명 이후, ASIC(Application Specific Integrated Circuit)이라고 부르는 주문형 반도체의 도입을 통해 채굴의 효율성은 다시 한번 향상됩니다. ASIC 은 특정 용도에 최적화되어 설계 생산된 반도체로, ASIC 채굴기는 오직 비트코인 해시함수 SHA-265 연산작업만을 위해 최적화된 하드웨어입니다. 비트코인 채굴 연산에 최적화되어 있는 ASIC 채굴기는 GPU 보다 수천 배 효율성이 높았고, 채굴 난이도는 다시 빠르게 상승해 곧 CPU 채굴처럼 GPU 채굴도 수익성을 잃었습니다. 새로운 ASIC 장비의 효율성이 크게 향상되면서 이전 세대 채굴장비가 수익성을 잃는 사이클이 매번 몇 년에 걸쳐 발생하고 있습니다.

첫 채굴자는 비트코인 채굴에 소액의 전기료를 투입하는 정도에 불과했습니다. 비트코인의 가격이 상승함에 따라, 더 많은 채굴자가 참여하게 되고 채굴 난이도가 올라가면서 비트코인 채굴 원가도 점점 상승했습니다. 오늘날 비트코인의 가격에 따라 채굴자는 비트코인 당 수천, 수만 달러 어치의 전기료를 채굴에 투입하고 있습니다.

채굴 풀(Mining Pools)

채굴에 있어서 한가지 이슈는 주사위를 굴리는 것처럼, 채굴도 그 결과가 비확정적(non-deterministic)이라는 점입니다. 채굴자가 많은 전력을 소모하고도 블록을 채굴하지 못할 수도 있다는 뜻입니다.

채굴자들이 전력을 투입하고도 채굴 보상을 얻지 못할 가능성을 해결하기 위해 2010 년에 채굴 풀(mining pool)이라는 기술이 도입되었습니다. 채굴 풀은 리스크를 공유하는 풀(risk shared pool)로, 보험과 그 원리가 비슷합니다.

채굴자가 연산능력을 하나의 채굴 풀에 모으고 채굴 풀은 마치 거대한 단일 채굴자처럼 채굴에 참여합니다. 채굴 풀에 소속된 어떤 채굴자가 블록을 채굴하더라도, 채굴 보상은 채굴 풀에 속한 각 채굴자가 기여한 해시율에 비례하여 골고루 나누어집니다. 이 방식을 통해 규모가 작은 채굴자도 보유한 해시율에 비례한 채굴 보상을 받을 수 있습니다. 협력과 조율의 서비스를 제공한 채굴 풀은 수수료로 채굴 보상의 일부를 나누어 갖습니다.

사용자들이 대형 채굴 풀에 몰리게 되면서 이 방식은 일정 부분 채굴의 중앙화를 야기했습니다. 하지만, 채굴 풀의 해시율은 채굴 풀이 직접 소유하는 것이 아니라 사용자들이 제공하는 것이고, 사용자들은 다른 채굴 풀로 옮겨 갈 수 있다는 점을 잊지 말아야 합니다.

실제 너무 커져버린 채굴 풀을 견제하기 위해 사용자들이 떠난 선례가 있습니다. 2014 년 채굴 풀 Ghash.io 가 확보한 채굴능력은 전체 네트워크에 절반에 육박했으나 Ghash.io 가 점점 중앙화 되어가는 것을 본 채굴자들은 자발적으로 다른 채굴 풀로 떠나버렸습니다.

오늘날까지도 채굴 풀은 어느정도 중앙화된 성격을 띄나, 개별 채굴자의 독립성을 확대하고 채굴 풀 의존도를 낮추는 BetterHash 같은 기술이 도입되면서 채굴 기술의 개선은 계속되고 있습니다.

51% 공격(51% Attacks)

채굴 풀 중앙화는 몇몇 대형 채굴 풀의 결탁이 51% 공격으로 이어질 수 있을 것이라는 우려를 낳았습니다. 지금도 알려진 채굴 풀 중 상위 다섯개가 전체 네트워크의 절반을 넘는 해시율을 보유하고 있습니다. 이러한 공격이 발생할 수 있는 경우와 위험요소에 대해 알아보도록 하겠습니다.

공격자가 네트워크 과반의 해시율을 확보하면 단독으로 가장 무거운 체인을 만들 수 있기 때문에 장부에 기입될 내용을 독단적으로 결정할 수 있게 됩니다. 나카모토 컨센서스 방식에 따르면 네트워크 상 모든 노드가 누적 증명 작업량이 가장 많은 체인(heaviest cumulative Proof of Work chain)을 진짜 체인으로 받아들이게 되기 때문입니다.

간단한 51% 공격 시나리오를 그려보면 다음과 같습니다.

1. 네트워크 전체가 초당 1,000 번의 해시 연산을 수행하고 있다고 가정합니다.
2. 공격자가 초당 2,000 번의 해시 연산을 수행할 수 있는 채굴 하드웨어와 전력을 매집합니다. 공격자가 네트워크 해시율의 67% (= 2,000 / 3,000)를 확보합니다.
3. 공격자는 아무 거래내용을 포함하지 안는 빈 블록을 생산합니다.
4. 약 2 주 뒤, 공격자는 그간 생산한 빈 블록을 네트워크로 송출합니다. 정직한 채굴자보다 공격자가 두배 빨리 채굴할 수 있기 때문에 공격자의 체인이 누적 증명 작업량이 두배 많은 체인이 됩니다. 송출된 공격자의 빈 블록이 정직한 블록을 대체하고 재조직(reorg)이 일어나면서 지난 2 주 간의 거래내역이 소실됩니다.

빈 블록을 생성해서 체인을 사용할 수 없도록 만드는 방법 외에 이중 지출 공격이 일어날 수도 있습니다.

1. 공격자가 거래소로 비트코인을 송금합니다.
2. 송금한 비트코인을 달러로 환전해 인출합니다.
3. 인출이 완료된 후, 거래소 송금 기록을 누락한 블록을 네트워크로 송출합니다.
4. 공격자는 송금했던 비트코인과 인출한 달러를 모두 확보합니다.

현재 비트코인 해시 연산에 투입되는 전력량은 웬만한 국가 수준에 달합니다. 이런 네트워크를 공격할 하드웨어와 전력을 확보하려면 막대한 비용이 수반됩니다. 현재 51% 공격 비용은 시간당 약 70 만 달러로 추정되며 그 추정치는 시간이 갈수록 계속 증가하고 있습니다. 이 수치는 정직한 채굴자의 대응은 감안하지 않은 값으로, 정직한 채굴자들의 반응에 따라 비용은 더 늘어날 가능성이 높습니다. 웹사이트 https://www.crypto51.app 에서 비트코인 및 다른 암호화폐 네트워크 공격 비용의 추정치를 확인하실 수 있습니다.

이런 규모의 공격을 감행하면 정체를 노출시킬 단서를 남기게 될 확률도 매우 높습니다. 결국 중형 국가 규모의 전력을 투입하고 엄청난 양의 하드웨어를 매집하면서 거래소와 대규모의 송금 및 인출 거래를 실행해야 하기 때문입니다.

하지만 무한정한 자원을 휘두를 수 있는 국가 정부 같은 공격자가 장기간 공격을 감행하기로 결정했다고 가정해 보겠습니다. 이론상 네트워크는 작업 증명 해시함수를 SHA-256 에서 다른 함수로 바꾸어 대응할 수 있습니다. 이 대응은 SHA-256 연산만 수행할 수 있는 공격자의 하드웨어 채굴기를 무용지물로 만들어 버립니다. 해시함수를 바꾸는 방법은 정직한 채굴자의 채굴 하드웨어도 모두 함께 무용지물로 만들어 버리는, 핵무기와 같은 최후의 방안입니다. 어찌됐든, 비트코인 네트워크는 생존하고 다시 성장할 수 있습니다.

51% 공격의 비현실성에 더해, 공격자가 과반의 해시율을 가지고 있어도 가장 중요한 두가지는 공격할 수 없습니다.

1. 코인 생산량은 정해진 발행 일정을 위반할 수 없습니다. 공격자가 아무리 많은 해시율을 가지고 블록을 만들더라도 블록에 포함된 신규 발행량이 컨센서스 규칙을 위반하면 그 블록은 기각됩니다.
2. 공격자는 직접 가지고 있지 않은 코인을 지출할 수 없습니다. 공격자는 적법한 디지털 서명을 제공할 수 없고, 컨센서스 규칙을 위반한 거래가 되어 해당 블록은 기각됩니다.

비트코인으로 결제를 받는 노드는 대다수의 채굴자가 악의를 가지고 행동하더라도 네트워크가 비트코인의 규칙을 준수하도록 묵묵히 검증을 계속할 것입니다. 이런 관점에서 보면 51% 공격은 실제로 보안 문제라기보다 성가신 걱정거리에 가깝습니다. 아마도, 상상할 수 있는 최악의 시나리오는 많은 자원을 활용할 수 있는 국가 단위의 개체가 비트코인을 무력화하려는 경우일 것입니다. 그러나, 이런 공격이 무한정 지속될 수는 없습니다. 비트코인이 이런 공격으로부터 살아남으면, 비트코인의 끈질긴 생명력을 반증하게 되는 꼴이며, 결국 공격자에게는 더 큰 골칫거리가 될 것입니다.

비트코인은 아직까지 51% 공격을 당한 적이 없으나, 해시율이 낮아 보안이 취약한 다른 블록체인은 이미 이런 공격을 받은 사례가 있습니다. 이런 경우, 애초에 상장되지 않았어야

할지 모를 낮의 해시율의 코인 때문에 거래소들이 이중 지불 공격의 희생자가 되고 손실을 입었습니다.

7. 익명 계정 (ACCOUNTS WITHOUT IDENTITY)

우리는 지금까지 중앙 기구가 필요 없는 분산 원장(distributed ledger), 거래 기록 권한을 결정하는 추첨 방식, 정직한 채굴자를 보상하고 나쁜 채굴자를 벌하는 보상 체계, 고정된 발행 일정을 유지하고 분쟁을 방지할 채굴 난이도 조정 방식, 그리고 체인의 총 작업 증명량과 거래 기록을 확인하여 체인의 유효성을 검증하는 방식을 살펴보았습니다.

이제 사용자의 신원(identity)을 다룰 차례입니다. 전통적 은행 시스템에서는 사용자는 송금과정에서 은행에게 자신의 신원을 밝히게 됩니다. 신분증을 제시하거나, ATM 을 사용하면서 PIN 코드를 입력하고, 앱에 사용자명과 비밀번호를 적어 넣게 됩니다. 은행은 한 신원이 다른 사용자가 공유하지 않도록 관리합니다.

이제 신원정보를 관리하는 중앙 기구 없이 비트코인 기반의 금융 시스템에서는 어떻게 계좌를 개설할 수 있을까요? 신원 탈취(identity theft)나 중앙집권 기구의 관리에 신원 정보를 제공해야 하는 문제를 피하고자 금융 시스템에서 신원정보를 제거하고자 했던 사토시의 목표를 어떻게 해야 달성할 수 있을까요? 우리의 사례처럼 앨리스(Alice)가 밥(Bob)에게 송금 요청을 송출하려 할 때 어떻게 송금 요청을 낸 사람이 앨리스 자신이며, 앨리스 자신에게 송금의 권한이 있다는 것을 증명할 수 있을까요?

"비트코인 계좌" 만들기

모든 계좌 정보의 관리를 위해 은행 같은 중앙화된 매개체(central middlemen)에게 의존할 수는 없습니다. 모두 각자가 자신의 사용자명과 비밀번호를 등록하도록 만들면 어떨까요? 보통의 경우라면 은행이 사용자명이 겹치지 않는지 확인하겠지만, 신원정보를 다루는 중앙 기구가 없는 지금 같은 경우에는 불가능합니다. 사용자명과 비밀번호보다 더 크고 센 고유의 방식이 필요합니다. 지난 챕터를 통해 이제는 충분히 익숙해진, 큰 자릿수의 난수(random number)가 필요한 순간입니다.

커다란 난수를 이용해 티켓을 만들어 추첨에 누구든 참여할 수 있도록 만들었던 것과 마찬가지로, 계좌를 만드는 데에도 같은 해결책을 적용할 수 있습니다. *주소*라고 부르는 "비트코인 계좌"를 만들려면 먼저 *퍼블릭/프라이빗 키 페어(public/private key pair)*라고

부르는, 수학적으로 서로 연결된 256 비트의 숫자 한 쌍을 만듭니다. 256 비트 수는 대략 우주 전체의 모든 원자의 수와 비슷하다는 점을 떠올리신다면, 두 사람이 우연히 같은 키 페어를 만들 확률은 불가능에 가깝습니다. 퍼블릭 키는 우리 계좌에 코인을 송금하려는 모두에게 뿌립니다. 프라이빗 키는 코인을 지출할 때 사용합니다. 원리는 이렇습니다.

암호화(encryption)란 일단의 데이터를 숨겨서, 열쇠를 가진 특정인만 해독을 통해 원본 메시지를 확인할 수 있게 하는 방법입니다. 어릴 때 기초적인 암호기/해독기를 가지고 메시지를 뜻이 없는 엉뚱한 말로 바꾸고, 다시 그런 메시지를 원래대로 해석하는 놀이를 해본 분들이 있을 것입니다. 키를 하나만 사용하는 이런 종류의 암호화를 대칭 방식(symmetric)이라고 합니다. 암호화에 사용하는 키, 해독에 사용하는 키가 따로 있는 퍼블릭/프라이빗 키 페어 방식은 *비대칭 방식(asymmetric)*이라고 부릅니다.

퍼블릭 키는 전세계에 공개해도 아무 문제가 없습니다. 특정 퍼블릭 키 주소로 메시지를 전송하려는 사람이라면 해당 퍼블릭 키를 이용해 전송할 메시지를 암호화합니다. 이제 프라이빗 키를 가진 사람만이 이 암호를 해독할 수 있습니다.

앨리스가 어떻게 밥에게 코인을 송금하는지 살펴보겠습니다. 밥은 코인을 수령하기 위해서 키 페어를 생성하고, 프라이빗 키를 비밀로 유지합니다. 그리고 퍼블릭 키의 해시를 바탕으로 만들어진 큰 숫자를 이용해 *주소(address)*를 생산합니다. 밥은 이 주소를 앨리스에게 공유합니다.

주소는 일종의 우편함으로 생각할 수 있습니다. 앨리스는 이 우편함에 편지 대신 코인을 넣을 수 있습니다. 하지만, 이 우편함의 프라이빗 키를 가지고 있는 밥만이 이 코인을 꺼내 쓸 수 있습니다.

은행을 통해 돈을 송금할 때에는 사용자명과 비밀번호를 대야 합니다. 수표를 발행할 때에는 수표를 발행하는 사람이 자신이라는 것을 증명하기 위해 서명을 제공해야 합니다. 비트코인을 송금할 때에는 해당 코인을 보관하고 있는 주소의 소유자임을 증명하는 키를 제공해야 합니다.

앨리스는 자신의 퍼블릭 키 우편함의 프라이빗 키를 가지고 있다는 점을 증명해야 하지만, 동시에 자신의 프라이빗 키가 해커에게 노출되는 것은 바라지 않습니다. 프라이빗 키가 노출되면 누군가 자신의 우편함에서 코인을 빼내어갈 수 있기 때문입니다.

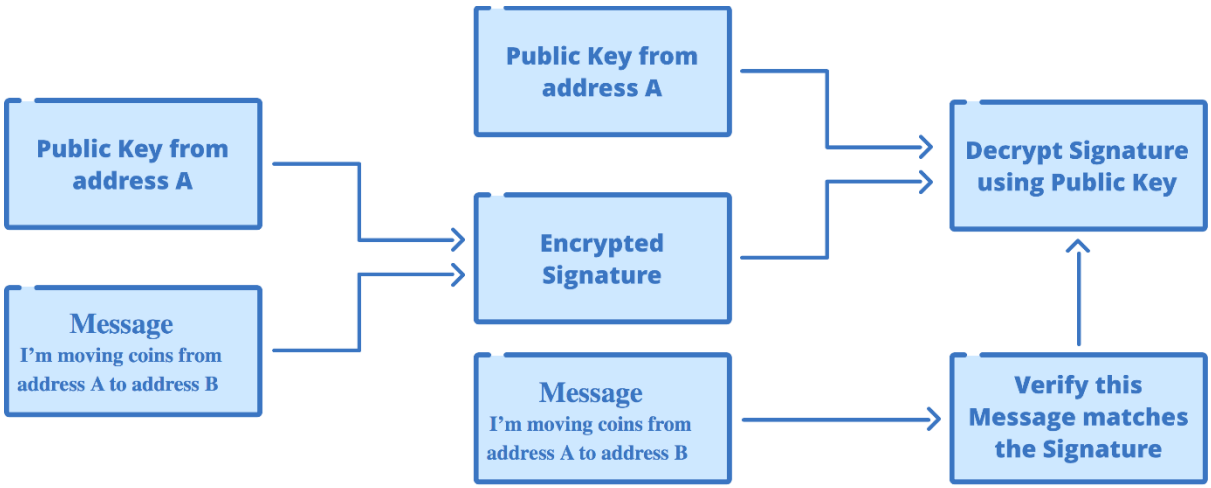
앨리스가 키를 소유하고 있다는 증명을 *디지털 서명(digital signature)*이라고 부릅니다. 앨리스는 아래 내용과 같은 형태의 거래 내용을 작성합니다.

비트코인 2.5 개를 보유하고 있는 주소 12345 에서 비트코인 2 개는 주소 56789 로 송금하고, 비트코인 0.5 개는 주소 12345 로 송금함.

실제로 주소 숫자는 160 비트 단위의 거대한 숫자로 이루어집니다. 앨리스는 이 거래 내용을 프라이빗 키로 암호화해 *디지털 서명(digital signature)*을 만듭니다.

앨리스가 위 거래 내용을 네트워크 상 다른 노드에게 송출하면, 앨리스가 비트코인을 가지고 있는 우편함의 퍼블릭 키와 프라이빗 키로 암호화한 디지털 서명이 공개됩니다. 앨리스가 공개한 내용은 다음과 같습니다.

- 나는 주소 12345 에서 코인을 송금합니다.
- 주소 12345 의 퍼블릭 키는 이 값입니다. 누구든 퍼블릭 키를 해시 연산하면 위 주소값이 산출되는 것을 검증할 수 있습니다.
- 내가 프라이빗 키로 암호화한, 이 주소의 서명은 이 값입니다. 누구든 퍼블릭 키로 서명을 해독하면 내가 지금 보내는 거래 내용과 일치하는 것을 검증할 수 있습니다.



코인을 송금하는 거래 내용은 프라이빗 키를 이용해 암호화되고, 공개된 퍼블릭 키로 해독됩니다.

앨리스의 우편함에 대응되는 퍼블릭 키가 공개되어 있기 때문에, 누구든 디지털 서명을 해독할 수 있습니다. 퍼블릭 키를 이용해 디지털 서명을 해독할 수 있기 때문에 모두가 거래 내용을 송출한 앨리스가 프라이빗 키를 사용했다는 사실을 알 수 있습니다. 앨리스가 프라이빗 키를 사용하지 않았다면, 같은 짝인 프라이빗 키로 암호화한 메시지만 해독할 수 있는 퍼블릭 키를 활용해서 암호를 해독할 수 없었을 것이기 때문입니다. 하지만 중요한 점은 앨리스가 프라이빗 키를 사용해서 전자 서명을 했다는 증거 외에는, 여전히 누구도 앨리스의 프라이빗 키 자체가 무엇인지 아무도 보지 못했다는 사실입니다.

수표에 쓰는 서명이나 은행 비밀번호와는 달리, 전자 서명은 서명을 날인하는 거래 내용마다 매번 값이 다릅니다. 따라서 전자 서명은 도용하여 다른 거래에 사용할 수 없습니다. 거래를 보내는 주소와 프라이빗 키가 같더라도, 입력 값이 바뀌면서 전자 서명의 해시 값이 바뀌기 때문에 매 거래 내용에 다른 전자 서명이 찍힙니다.

프라이빗 키를 유추할 수 있나요?

특정 주소의 프라이빗 키를 유추해 해당 주소의 코인을 마음대로 이체할 수 있게 될 확률을 알아보겠습니다. 키가 256 비트 단위의 숫자로 이루어진다는 점을 기억하시기 바랍니다. 각 비트의 값은 1 과 0, 두 가지 경우 밖에 없습니다. 각 비트의 값이 동전 던지기의 결과에 따라 결정된다고 상상 해보실 수 있습니다.

1 비트의 프라이빗 키를 정한다면 동전 던지기를 한번 하는 것과 같습니다. 앞면 혹은 뒷면, 1 혹은 0. 결과를 맞출 확률은 둘 중 하나, 1/2 입니다.

간단한 복습을 해보겠습니다. 특정 경우가 여러 번 발생할 확률은 해당 경우가 한번 발생할 확률을 여러 번 곱해서 계산할 수 있습니다. 동전을 한번 던져 앞면이 나올 확률이 1/2 이라면, 동전을 두 번 던져 모두 앞면이 나올 확률은 1/2 x 1/2 = 1/4 로 25%입니다.

여덟 번의 동전 던지기 결과를 모두 맞출 확률은 $2^8 = 256$가지 경우 중 하나로, 256 분의 1 입니다.

차량 번호판은 여섯 개의 문자와 숫자로 이루어져 있습니다. 영어 알파벳은 26 개와 숫자 10 개, 모두 합해 36 개의 값이 들어갈 수 있습니다. 이 중 여섯 개가 들어가기 때문에 가능한 차량 번호판의 경우의 수는 36^6 가지로, 차량 번호판을 맞출 확률은 20 억 분의 1 입니다[5].

신용카드 번호는 16 자리입니다. 각 자리 수에 들어갈 수 있는 값 10 가지가 16 자리 있으므로, 신용카드 번호를 유추할 확률은 10^{16} 분의 1, 10,000,000,000,000,000 분의 1, 1,000 경 분의 1 에 해당합니다.

지구 상에는 원자가 약 10^{50} 개 존재합니다. 이 중 무작위로 하나의 원자를 고른다면 해당 원자를 맞출 확률은 아래와 같습니다.

1,000,000,000,000,000,000,000,000,000,000,000,000,000,000,000,000,000 분의 1

프라이빗 키는 256 비트로, 이진수로 2^{256}, 십진수로 약 10^{77} 에 해당합니다. 프라이빗 키를 유추할 확률이란 전 우주에서 하나의 원자를 집어낼 확률이나, 파워볼 복권(Powerball Lottery)에 9 번 연속으로 당첨되는 확률과 같습니다.

115,792,089,237,316,195,423,570,985,008,687,907,853,269,
984,665,640,564,039,457,584,007,913,129,639,936 분의 1

하지만, 연산을 대신할 강력한 슈퍼컴퓨터가 있다면 어떨까요? 이 주제에 대해서는 다음 링크 https://bit.ly/2Dbw9Qd 의 레딧 게시물에서 너무나 잘 설명하고 있어, 읽어 보시기를 권합니다. 게시물의 설명이 다소 기술적이긴 하나, 마지막 단락이 256 비트의 키를 모두 연산하는데 얼마나 걸릴지 잘 설명하고 있습니다.

---

[5] 이 단락의 내용은 여러 가지 상황이 발생할 확률을 다룬 훌륭한 글에서 영감을 받았습니다. 맥락의 이해를 위해서 전문을 읽어보시길 권합니다.
http://medium.com/@kerbleski/a-dance-with-infinity-980bd8e9a781

"따라서, 지구 전체를 하드 드라이브로 활용하고 원자당 1 바이트를 쓰고, 항성의 에너지를 써서, 초당 1 조의 키를 연산한다고 가정했을 때, 저장공간으로 $37 \, x \, 10^{11}$ *개의 지구, 에너지 원으로 2,370 억개의 태양,* $3.6717 \, x \, 10^{21}$ *년이 걸립니다."*

- 서브레딧 Bitcoin 의 사용자 PSBlake

사실상 누군가의 프라이빗 키를 유추하기는 불가능합니다. 오히려, 비트코인 계좌의 경우의 수는 아주 많아서, 실무적에서는 각 거래에 매번 새로운 주소를 만드는 방법을 권장할 정도입니다. 따라서, 하나의 은행 계좌 대신 매 비트코인 거래에 하나씩, 수천 수백만 개의 비트코인 계좌를 가지게 될 수도 있습니다.

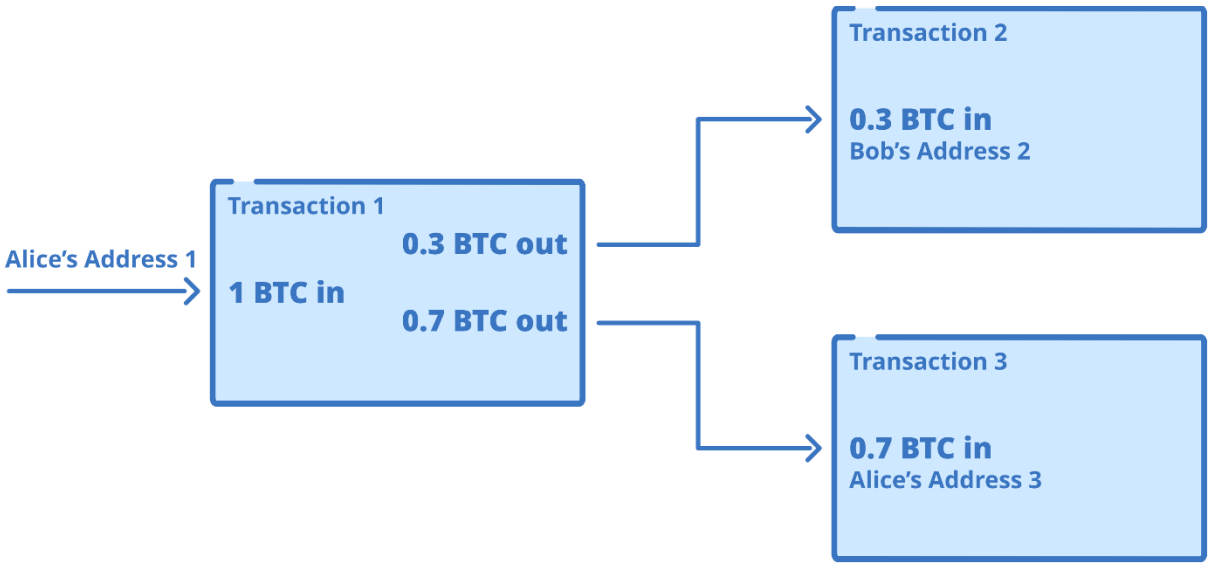
여러분의 비트코인 계좌의 보안이 단순히 확률을 통해서 지켜지고 있다는 점이 불안하게 느껴질지 모르겠으나, 은행 계좌 비밀번호를 해커의 공격 대상이 될 수 있는 중앙집중화된 서버에 저장하는 것보다 훨씬 더 안전한 방식이라는 점을 위 설명을 통해 이해하셨기를 바랍니다.

잔고 추적

이전 챕터에서 설명을 위해 생략하였던 마지막 내용을 설명할 차례입니다. 비트코인 장부에 실제로 잔고 정보는 기록되지 않습니다. 대신, 비트코인은 UTXO(Unspent Transaction Outputs)이라고 모델을 사용합니다. 거래 출력(transaction output)이란, 누군가가 여러분에게 전송한 코인이든 채굴을 통해 받은 *코인베이스 거래(coinbase transaction)*든, 이전 거래에서 받은 코인을 일컫는 용어에 불과합니다.

백원 짜리나 오백원 짜리처럼 액면가가 정해져 있는 금속 주화와 달리 비트코인은 1 억 분의 1 단위까지 자유롭게 분할할 수 있는데, 비트코인의 최소 단위인 1 억 분의 1 비트코인을 사토시(satoshi)라는 부릅니다. 따라서, 여러분의 주소로 송금된 비트코인의 양에 따라 다양한 주소의 비트코인을 하나의 묶음으로 합치거나, 송금을 하기 위해 큰 UTXO 를 작은 단위로 쪼개는 작업이 필요해집니다. 여러 동전을 다 녹여서 어떤 액면가의 동전이든 마음대로 만들어 낼 수 있는 기계를 상상해보시면 됩니다. 이런 작업은 대체로 비트코인 지갑이 처리하며 사용자는 단순히 송금하고 싶은 금액을 정하기만 하면 됩니다. 비트코인 지갑에 대해서는 다음 챕터에서 다루도록 하겠습니다.

앨리스가 비트코인 1 개를 가지고 있는 주소를 보유하고 있다고 가정하겠습니다. 앨리스는 밥에게 0.3 개의 비트코인을 전송하려 합니다. 앨리스는 입력 값으로 자신의 주소에 있는 1 개의 비트코인을, 두개의 출력 값으로 밥 주소에 송금할 0.3 개의 UTXO 비트코인과 자신의 주소로 돌려보낼 0.7 개의 UTXO 비트코인을 가진 거래 정보를 생성합니다. 0.7 개의 잔돈은 기존 비트코인 주소로 보낼 수도 있고, 프라이버시를 위해 새로 만든 앨리스의 비트코인 주소로 보낼 수도 있습니다.



정확히 송금할 금액에 해당하는 UTXO 가 없으면, 분할이 진행됩니다.
여러 개의 UTXO 를 합쳐 더 큰 UTXO 를 만들 수도 있습니다.

누가 어떤 주소를 소유하고 있는지 확인할 방법은 없습니다. 이를 위해서는, 해당 주소에 대응되는 프라이빗 키와 해당 키를 소유한 실제 인물이 누구인지를 모두 알아야만 합니다. UTXO 모델은 거래가 생길 때마다 잔돈을 새로운 주소에 옮기는 방식의 프라이버시 메커니즘을 장려합니다. 따라서, 자주 비트코인 거래를 했다면 한 사람이 수백, 수 천개의 주소를 소유할 수도 있습니다. 지금까지의 과정은 지갑 소프트웨어가 모두 처리하므로, 세부 내용은 사용자가 걱정하지 않아도 됩니다.

따라서, 특정 주소의 "잔고"를 확인하기 위해서는 해당 주소를 출력 값으로 가지고 있는 UTXO 를 모두 합해야 합니다. 비트코인 네트워크 상 총 UTXO 의 개수는 사용자가 하나의 주소에서 여러 주소로 송금할 때 늘어나며, *통합 거래(consolidation)*라고 부르는 과정을 통해 여러 주소에서 하나의 주소로 송금될 때 줄어듭니다.

UTXO 모델 상 각 UTXO 는 단 한번만 활용될 수 있기 때문에, 쉽고 효율적인 이중 지불 검증이 가능해집니다. 특정 계좌의 모든 지출 내역을 확인할 필요가 없어지기 때문입니다.

다양한 입력/출력 값 조합을 가진 복잡한 거래를 통해 한번에 원하는 개수만큼의 UTXO 를 만들거나 없앨 수 있습니다. 이 아이디어를 구체화한 것이 코인조인(CoinJoin) [6] 이라는 방식으로, 여러 사람의 거래를 한번에 묶어 입력 값과 출력 값을 뒤섞어 UTXO 의 기록 추적을 어렵게 만드는 방법입니다. 이런 방식의 기술들이 더 보편화되고 있는데, 이는 프라이버시와 *대체가능성(fungibility)* 관점에서 중요합니다. 대체가능성이란 특정 비트코인이 같은 양의 다른 비트코인과 모든 면에서 동일한(equivalent) 가치를 가지는 것을 의미합니다. 이로 인해, 특정 비트코인이 나쁜 집단의 수중에 떨어지더라도 추후 범죄에 한번 사용된 비트코인으로 영원히 얼룩지지 않게 됩니다.

지갑

계정 생성은 임의의 256 비트 키 페어를 생성하는 것에 지나지 않습니다. 수천 수백만개의 주소를 생성할 수 있기 때문에 이 주소들을 관리할 방법이 필요합니다. 비트코인에서 *지갑(wallet)*이란 사용자의 키를 관리하는 모든 장치를 일컫는 개념입니다. 지갑은 종이 한 장의 간단한 방식일 수도, 기계장치처럼 복잡한 방식일 수도 있습니다.

사토시가 처음 발표한 최초의 비트코인 코드는 소프트웨어 지갑 방식을 차용하였습니다. 이 지갑을 통해 주소를 생성하고, 키를 저장하며, 지출할 UTXO 를 선택하여 원하는 만큼의 금액을 간단히 송금할 수 있었습니다.

일반적으로 은행이 개발한 모바일이나 웹 기반의 애플리케이션인 은행 지갑과 달리, 비트코인은 완전한 오픈 시스템입니다. 따라서, 비트코인 지갑은 수십 가지가 있고, 대부분이 무료이자 오픈 소스입니다. 하드웨어 지갑도 여러가지 종류가 있으며, 앞으로도 더 많은 지갑이 개발될 것입니다. 컴퓨터 프로그래밍 지식을 갖춘 사람이면 누구든 직접 지갑을 만들거나, 오픈 소스 지갑의 코드에 수상한 내용이 포함되지는 않았는지 검증할 수 있습니다.

누구든 프라이빗 키만 있으면 비트코인을 지출할 수 있기 때문에, 프라이빗 키가 유출되지 않도록 각별히 유념해야만 합니다. 신용카드를 도난당하면, 신용카드 회사에 신고하고 지출액을 환수할 수도 있습니다. 비트코인에는 신용카드 회사 같은 중개인이 없습니다.

---

[6] https://en.bitcoin.it/wiki/CoinJoin

누군가에게 프라이빗 키가 유출되었다면 코인을 소유하는 건 그 사람이며, 도움을 요청할 사람도 없습니다.

프라이빗 키는 분실에 취약합니다. 지갑을 컴퓨터에 저장했는데 그 컴퓨터가 도난 되거나 화재로 유실된다면 문제일 수밖에 없습니다. 보안을 위한 비트코인 관례를 따라 코인을 송금 받을 때 마다 새로운 주소를 생성한다면, 프라이빗 키를 안전하게 저장하고 보관하는 것은 곧 골칫거리가 되어 버립니다.

비트코인 생태계는 시간이 지나면서 이 문제에 대한 여러가지 해결 방안을 내놓았습니다. 2012 년 BIP32 (Bitcoin Improvement Proposal, 비트코인 개선 제안이라고 하며, 비트코인을 개선하는 방안을 논의하는 방식)을 통해 계층 결정적 지갑(Hierarchical Deterministic Wallets)를 적용하는 방안이 제시되었습니다. 이 방식은 시드(seed)라고 부르는 하나의 임의의 수를 사용해 계속적으로 비트코인 주소와 프라이빗 키를 나타내는 여러가지 키 쌍을 생성할 수 있게 됩니다.

최근에는 널리 쓰이는 어떤 소프트웨어 및 하드웨어 지갑을 사용하더라도 사용자는 하나의 마스터 키만 보관하면 되도록, 지갑이 모든 거래에 각각 새로운 키를 자동으로 생성합니다.

2013 년에는 BIP39 를 통해 키 보관이 더욱 편리 해졌습니다. 임의의 수를 사용하는 대신, 사람이 읽을 수 있는 단어의 조합을 통해 키를 생성할 수 있게 되었습니다. 아래는 시드의 한 예입니다.

witch collapse practice feed shame open despair creek road again ice least

이 방식을 통해 키 보관은 매우 쉬워졌습니다. 종이에 시드를 적어 금고에 보관할 수 있도록 말입니다. 하물며 시드를 외워 별도의 소지품을 지니지 않고도 전재산을 머리 속에 넣어 베네수엘라 같은 경제 위기 지역에서 유유히 빠져나올 수도 있게 된 것입니다.

게다가, 비트코인 주소에 접근하는데 두 개 이상의 프라이빗 키가 필요하게 만들 수도 있습니다. 멀티시그니쳐(Multi-signature) 또는 *멀티시그(Multisig)* 주소라고 불리는 방식을 통해 매우 다양한 보안 방식이 가능합니다. 예를 들어, 1/2 멀티시그 방식을 통해 두 사람이 한 개씩 멀티시그를 나눠 가지고 각각 단독 거래 승인권을 가질 수도 있습니다.

2/2 멀티시그 방식으로는 거래 승인에 두 개의 멀티시그가 모두 필요하도록 만들어 비즈니스 파트너이 만장 일치로만 거래를 승인할 수 있도록 할 수도 있습니다.

2/3 멀티시그 방식을 활용하면 간단한 에스크로 시스템을 만들 수 있습니다. 키 하나는 매수자가, 다른 하나는 매도자가, 나머지 하나는 중재자가 보유합니다. 매수자와 매도자가 동의하면 자금을 집행할 수 있습니다. 분쟁이 발생할 경우에는 중재자가 어느 한쪽의 입장을 대변하여 자금의 동결을 해제할 수 있습니다.

3/5 멀티시그 방식을 활용하면 5 개 중에 최대 2 개의 프라이빗 키를 분실하더라도 계좌에 접근 권한을 잃지 않도록 대비할 수 있습니다. 2 개의 키는 각기 다른 장소에, 다른 2 개의 키는 서로를 모르는 믿을 수 있는 친구에게, 나머지 1 개의 키는 빗고(BitGo) 같은 특수 신탁 서비스 회사에 보관하면서 비트코인을 도난하기 매우 어렵게 만들고, 프라이빗 키의 분실 위험에서도 스스로를 보호할 수 있습니다.

더 나아가, 조건 명제("if this, then that") 같은 프로그래밍 구조를 통해 복잡한 조건부 형식의 주소를 활용할 수도 있습니다. 주소를 만든 당사자조차 시간이 지나기 전에 코인을 쓰도록 코드를 수정할 수 없도록 특정 주소의 코인을 10 년 동안 동결시킬 수도 있습니다.

갈수록 더 다양한 준예탁 솔루션(semi-custodial solutions)이 카사(Casa)나 언체인드 캐피탈(Unchained Capital) 같은 회사를 통해 제공되고 있고, 키를 안전하게 보관하기 용이해지고 있습니다. 고객의 계좌를 동결할 수 있는 은행과 달리 위와 같은 부분 예탁 솔루션(partial custody solutions)은 백업 저장소나 수탁 공동 서명권자의 역할을 가질 뿐, 주소 소유자의 키 없이 스스로 주소의 자금을 취할 수 있는 능력은 없습니다. 은행 앱과 달리 지갑 소프트웨어는 수정과 배포에 어떤 승인이나 권한이 필요 없기 때문에 지금도 지속적으로 진화하고 있습니다. 따라서 지갑 개발 시장에는 지속적으로 더 많은 신규 진입자와 혁신이 생겨나고 있습니다.

위 현상은 세상을 바꿀 중대한 의미를 내포하고 있습니다. 유사 이래 처음으로 압류나 절도로부터 완벽히 안전한 방법으로 부를 이전할 수 있게 된 것입니다.

8. 누가 규칙을 정하나요? (WHO MAKES THE RULES?)

여기까지 가치(value)를 기록하고 전송할 수 있는 분산 시스템을 만들었습니다. 시스템의 구성을 다시 살펴보면 아래와 같습니다.

1. 모든 참여자가 사본을 가지는 분산 원장
2. 작업 증명(Proof of Work)과 난이도 조정을 통해 매수와 부정 등 간섭에서부터 자유롭고 발행 일정이 변하지 않는 네트워크
3. 모든 참여자가 오픈소스 비트코인 클라이언트를 사용해 전체 블록체인 기록을 검증할 수 있는 컨센서스 시스템
4. 디지털 서명을 사용해 중앙집권 기구 없이도 계정으로 쓸 메일함을 생성할 수 있는 아이덴티티 시스템(identity system)

이제 가장 흥미로우면서도 언뜻 직관에 어긋나 보이기도 하는 비트코인의 특성을 다룰 차례입니다. 비트코인의 규칙은 어디에서 나오며, 어떻게 시행되며, 어떻게 바뀌지 알아보겠습니다.

비트코인 소프트웨어

이전 챕터를 통해 네트워크 상 모두가 다음과 같이 동일한 규칙을 검증하는 것으로 가정하였습니다. 이중 지출이 기각되며, 모든 블록이 적정한 작업 증명량을 보유하고 있음을 보장하고, 모든 블록이 직전의 블록과 연결되며, 모든 거래가 해당 주소 소유자의 디지털 서명을 보유하고 있으며, 이 외에도 시간이 지나면서 규정된 다양한 규칙이 있습니다.

비트코인이 오픈소스 소프트웨어라는 점을 다룬 바 있습니다. 오픈소스란 누구든 소프트웨어의 코드를 읽고, 각자의 버전으로 원하는 코드 변경 사항을 업데이트할 수 있다는 뜻입니다. 비트코인에는 업데이트 변경 사항이 어떻게 반영될까요?

비트코인은 *프로토콜(protocol)*입니다. 컴퓨터 소프트웨어에서 프로토콜이란 특정 소프트웨어가 준수하는 일단의 규칙을 의미합니다. 하지만, 프로토콜의 규칙을 모두 준수하는 한, 소프트웨어는 원하는 대로 수정할 수 있는 것입니다. 소위 "비트코인 노드를 돌린다(run Bitcoin nodes)"라는 것은, 엄밀히 말하면 비트코인 프로토콜을 준수하는 소프트웨어를 돌리는 것으로 이해할 수 있습니다. 이 소프트웨어들은 다른 비트코인 노드와 의사소통하고, 거래와 블록을 주고받고, 해당 노드와 연결된 다른 노드를 찾아내는 등 여러가지 작업을 할 수 있습니다.

비트코인 프로토콜을 어떻게 적용할 것인지의 세부적인 내용은 개개인의 선택에 달려 있습니다. 비트코인 프로토콜의 적용 버전은 여러가지가 있습니다. 가장 인기있는 프로토콜은 비트코인 코어(Bitcoin Core)로, 사토시 나카모토(Satoshi Nakamoto)의 최초 버전으로부터의 연장선이기도 합니다.

물론 비트코인 코어와 다른 컴퓨터 언어로 쓰인 다른 사람들에 의해 유지관리 되는 다른 버전의 비트코인 소프트웨어도 존재합니다. 비트코인에 있어 컨센서스는 매우 중요한데, 다시 말해 특정 블록이 유효한지 혹은 무효한지 모든 노드의 의견이 합치하여야 하기 때문에, 혹시 발생할지 모를 버그로 유효한 블록을 기각하는 노드가 발생할 가능성을 피하기 위해 절대 다수의 노트가 비트코인 코어 소프트웨어를 활용하고 있습니다. 사실 비트코인 프로토콜에는 문서화된 완전 사양(complete written specification)이 따로 없기에, 비트코인 클라이언트 소프트웨어를 개발하는 최선의 방식은 혹여 버그가 있더라도, 오리지널 코드에서 벗어나는 점이 없도록 만드는 것입니다.

누가 규칙을 정하나요?

비트코인을 구성하는 규칙은 비트코인 코어 클라이언트(Bitcoin Core client)에 코드로 표현되어 있습니다. 하지만 누가 이런 규칙을 만들까요? 누군가 이런 소프트웨어를 수정해서 2,100 만개의 비트코인 발행량 상한을 4,200 만개로 바꿔버릴 수 있다면 어떻게 비트코인이 희소하다고 말할 수 있을까요?

비트코인은 분산화 시스템이기 때문에 모든 노드가 규칙에 합의해야만 합니다. 채굴자가 자기 자신에게 현재 네트워크 상의 블록 보상(Block Reward) 설정치보다 두배의 보상을 지급하도록 자신의 소프트웨어를 바꾼다면, 실제 블록을 채굴하게 되었을 때, 네트워크 상 다른 모든 노드가 해당 블록을 거부하게 됩니다. 수천 개의 노드가 전세계에 퍼져서

비트코인의 규칙을 감시감독하기 때문에 비트코인의 규칙을 바꾸는 것은 극히 어려운 일입니다.

비트코인의 거버넌스 모델은 특히 서구 민주주의 사회에 살고 있는 사람의 관점에서 보면 언뜻 직관에 어긋납니다. 민주주의 사회에서 살아온 우리들은 투표를 통한 의사 결정에 익숙합니다. 과반수의 결정을 통해 법을 소수의 의사에 반하는 법을 통과시키는 등 여러가지 일을 진행할 수 있습니다. 하지만, 비트코인의 거버넌스는 민주주의보다 무정부 상황에 가깝습니다.

비트코인으로 결제 받는 사람이 각자 스스로에게 무엇이 비트코인인지 결정하는 것입니다. 누군가 발행량이 210 억개로 정의된 비트코인 소프트웨어를 돌리는 상황이라면, 해당 정의를 벗어난 소프트웨어를 통해 생산된 비트코인은 위조 코인으로 분류되고 거부될 것입니다.

비트코인 세계에서 각 참여자들이 어떻게 서로를 견제와 균형을 이루는지 살펴보겠습니다.

노드(Nodes): 비트코인 네트워크 상의 참여자는 각각 노드를 운용합니다. 노드 운용자는 어떤 소프트웨어를 기반으로 노드를 운용할 지를 결정합니다. 대부분은 사토시 나카모토가 시작한 이래 현재 전세계 수백명의 독립 개발자들과 여러 회사들이 개발하고 있는, 비트코인 프로토콜의 대표적 클라이언트인 비트코인 코어(Bitcoin Core) 소프트웨어를 운용합니다. 그러나 만약 이 소프트웨어에 인플레이션 같은 악의적인 변경 사항을 적용된다면 아무도 이 소프트웨어를 선택하지 않을 것입니다. 노드 운용자는 비트코인 결제를 도입한 상인, 거래소, 지갑 서비스 회사 및 어떤 목적으로든 비트코인을 사용하는 다양한 사람들로 구성되어 있습니다.

채굴자(Miners): 일부 노드는 채굴 작업을 통해서 비트코인을 주조하고, 거래를 기록하고, 비트코인 장부의 조작의 대가가 높도록 유지합니다. 채굴자만 비트코인 장부에 기록할 수 있다는 점을 떠올리면 채굴자가 비트코인 네트워크의 규칙을 결정한다고 생각하기 쉽지만, 실은 그렇지 않습니다. 채굴자는 노드가 비트코인의 받아들일지 여부를 결정하는 규칙을 따를 뿐입니다. 채굴자가 규칙을 벗어난 규모의 채굴 보상을 포함한 블록은 생산하면 다른 노드는 해당 블록을 받아들이지 않을 것이고 해당 블록에 포함된 블록 보상 또한 쓸모 없게 되어버릴 것입니다. 따라서, 모든 노드 운용자는 어떤 규칙을 토대로 비트코인을 검증하고 받아들일지 각자 스스로 결정하고, 해당 규칙을 위반하는 채굴 결과를 전면적으로 부정하는 방식을 통해 무정부적 거버넌스(anarchic governance)를 이끌어 나갑니다.

사용자/투자자(Users/Investors): 사용자란 노드를 운용하는 것 외에도 비트코인 화폐를 사고 파는 사람을 의미합니다. 오늘날 일부 사용자는 노드를 직접 운용하기보다, 사용자의 필요와 바람을 대변하는 일종의 프록시로써 지갑 서비스에서 제공하는 노드에 의존하기도 합니다. 사용자는 오픈 마켓의 수요와 공급을 통해 코인의 가치를 결정합니다. 혹 채굴자와 거래소가 공모하여 인플레이션 같이 급진적인 변경 사항을 반영하게 되면, 사용자들은 해당 화폐를 대량 매도하여 가격이 떨어뜨려 해당 위반을 일으킨 회사를 파산으로 몰고 갈 것입니다. 소수 굴하지 않는 사용자들만으로도 오리지널 규칙을 따르는 버전의 비트코인의 명맥을 이어갈 수 있습니다.

개발자(Developer): 비트코인 코어(Bitcoin Core) 소프트웨어는 가장 대중적인 비트코인 클라이언트 프로젝트입니다. 비트코인 코어는 수백명에 달하는 최고의 크립토 개발자들과 회사들로 끌어들여 구성된 풍요로운 생태계를 구성했습니다. 비트코인 코어 프로젝트는 이제 수천억 달러 이상의 가치를 지닌 네트워크를 관장하는 만큼 매우 보수적입니다. 모든 개선안은 BIP(Bitcoin Improvement Program, 비트코인 개선 프로그램)[7] 이라고 불리는 과정을 통해 코드 변경내용 하나하나 동료 심사(peer review)를 거치게 됩니다. 개선안 제안과 심사 과정은 완전히 공개적으로 진행되는데, 누구나 참여하여 코멘트하거나 코드를 제출할 수 있습니다. 개발자가 악의적으로 변해 누구도 원하지 않는 내용을 제시한다고 해도 사용자들은 단순히 다른 소프트웨어를 돌리면 그만입니다. 이전 버전의 소프트웨어를 업데이트하지 않고 계속 사용할 수도, 개별적으로 새로운 개발을 시작할 수도 있는 노릇입니다. 이로 인해 비트코인 코어 개발자들은 사용자들이 일반적으로 원하는 개선 사항을 개발할 수밖에 없으며, 그렇지 않은 경우 표준 소프트웨어(reference implementation)의 지위를 잃고 누구도 사용하지 않을 위험에 처하게 됩니다.

포크(fork)를 통한 규칙 변경

[7] 비트코인 코어의 개발과정을 다룬 제임슨 롭(Jameson Lopp)의 Who Controls Bitcoin Core?를 읽어 보시기 바랍니다.
https://medium.com/@lopp/who-controls-bitcoin-core-c55c0af91b8a

이제 비트코인 소프트웨어를 통해서 사람들이 선택한 규칙이 어떻게 시행되는지, 그리고 사람들이 각자 믿는 규칙을 시행하기 위해 운용할 소프트웨어를 어떻게 선택하는지에 대한 대강의 개념을 새우셨기 바랍니다.

채굴자는 어떤 규칙을 따라 블록을 생성할지 결정할 수 있지만, 동시에 사용자가 원하는 블록을 채굴하지 않으면 블록이 받아들여지지 않고 블록 보상을 잃을 위험을 감수해야합니다.

앞서 우리는 비트코인 소프트웨어가 누적 작업 증명량이 가장 많은(heaviest) 유효 체인을 하나의 진짜 체인(One True Chain)으로 받아들이며, 이 과정에서 두개 이상의 블록 생산이 동시에 이루어질 때 자연적으로 포크가 발생할 수 있다는 사실을 다루었습니다.

비트코인 네트워크 참가자의 방대한 다양성으로 인해, 비트코인의 규칙은 시작부터 거의 확정된 것으로 볼 수 있습니다. 지금까지 비트코인에 이루어진 업그레이드 사항들은 하위호환(backward-compatible)이 되도록 핵심 컨센서스 규칙을 보존하고 있기 때문에 업그레이드를 하지 않아도 노드 운용에 문제가 없습니다.

이제 실제 규칙이 어떻게 바뀌는지 알아보겠습니다. 의도적 포크(intentional fork)란 사용자나 채굴자가 현재 비트코인 규칙에 동의하지 않아 규칙을 바꾸고자 할 때 발생합니다. 실제로 발생한 적이 있는 규칙 변경 포크는 두가지가 있습니다. 하위 호환성을 가진 소프트포크(soft-fork)와 하위 호환이 되지 않는 하드포크(hard-fork)가 그 두가지입니다. 이 두가지 경우가 이론적으로 어떻게 발생할 수 있는지 알아본 후, 과거 사례를 살펴보겠습니다.

*소프트포크(soft-fork)*는 하위 호환이 가능한 컨센서스 규칙의 변경으로, 규칙의 강화를 의미합니다. 이는 신규 규칙으로 업그레이드하지 않은 구형 노드도 신규 규칙 하에 생산된 블록을 유효 블록으로 받아들인다는 의미입니다. 예를 통해 명확히 살펴보겠습니다.

2010 년 9 월 12 일, 소프트웨어에 새로운 규칙이 도입되었습니다. 블록의 최대 용량이 1MB 로 정해진 것입니다. 이 규칙은 블록체인 상의 스팸에 대응하기 위한 조치였습니다. 이 규칙 이전에는 모든 용량의 블록이 유효했습니다. 새로운 규칙에 따라, 유료 블록의 최대 용량이 줄어들었고, 규칙은 강화된 것입니다. 이때, 업그레이드하지 않은 구형 노드의 관점에서도 새로운 규칙 하의 작은 용량의 블록은 유효하고, 구형 노드는 새로운 업그레이드에 영향을 받지 않는 것입니다.

노드 운용자가 천천히 시간을 두고 자율적으로 새로운 소프트웨어로 업그레이드할 수 있기 때문에 소프트포크는 시스템에 지장을 주지 않는 업그레이드 방식입니다. 업그레이드를 하지

않더라도 모든 블록을 전과 같이 처리할 수 있는 것입니다. 새로운 규칙을 반영한 1MB 용량의 블록을 생산하려면 채굴자만 새로운 업그레이드하면 됩니다. 채굴자만 1MB 소프트포크로 업그레이드를 마치면, 그때부터는 모든 블록이 1MB 용량으로 생산됩니다. 사용자는 구버전의 소프트웨어를 쓰더라도 이 모든 과정에서 아무런 영향을 받지 않습니다.

반면에 *하드포크(hard-fork)*의 경우에는 하위 호환이 되지 않는 변경이 도입됩니다. 하드포크 시에는 규칙의 확대로 인해 원래 무효했던 블록이 유효한 블록으로 분류됩니다. 업그레이드를 하지 않은 구형 노드는 새로운 규칙을 바탕으로 생산된 블록을 무효한 블록으로 분류하게 되고 따라서 새로운 블록을 처리할 수 없게 됩니다. 결국, 구형 노드는 업그레이드를 하지 않는 한 구형 체인에 갇히게 되는 셈입니다.

하드포크가 네트워크 상 거의 모든 노드의 만장일치를 바탕으로 진행된다면 문제될 것이 없습니다. 모든 노드가 새로운 규칙으로 즉시 업그레이드를 이행할 것이기 때문입니다. 일부 뒤처진 노드가 생긴다면 새로 생성되는 블록의 업데이트를 받지 못할 것이고, 소프트웨어가 작동을 멈춘 것을 확인한 후에는 이론적으로 자연히 업그레이드를 할 수밖에 없어집니다.

실제로 하드포크가 이렇게 수월하게 진행되는 경우는 거의 없습니다. 진정으로 분산화된 무정부적 시스템 하에서 새로운 규칙을 모두에게 강요할 수가 없습니다. 2017 년 8 월, 일부 사람들이 저비용 결제수단으로서 비트코인 체인의 방향성에 불만을 품은 바 있습니다. 이들은 포크를 통해 블록 용량을 늘린 새로운 체인을 만들기로 결심합니다. 비트코인은 2010 년 진행된 소프트포크의 결과 블록의 용량 상한이 1MB 로 제한되어 있었기 때문입니다. 이에 하드포크를 통해 만들어진 블록 용량 상한이 증가된 새로운 체인이 비트코인 캐쉬(Bitcoin Cash)입니다.

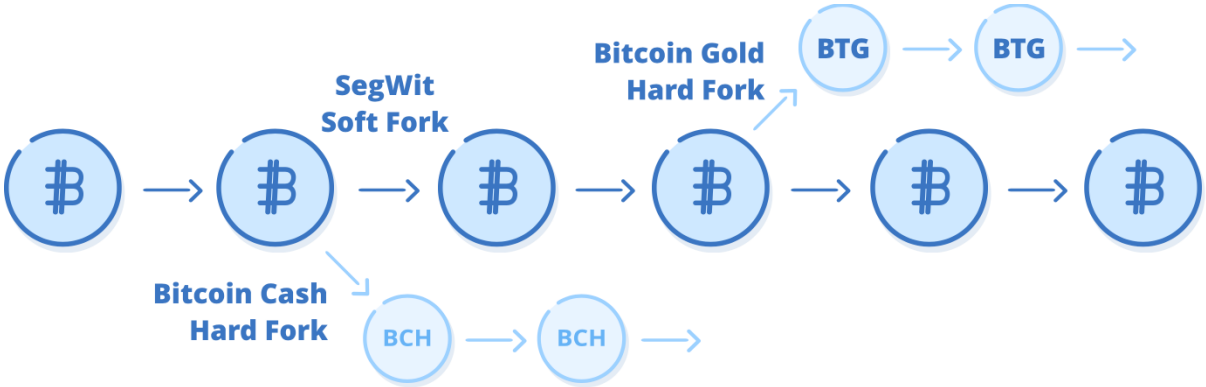
비트코인 캐쉬처럼 기존 채굴자와 노드의 만장일치 참여를 이끌어내지 못한 채 기존 컨센서스를 벗어난 하드포크는 새로운 블록체인의 생성으로 이어집니다. 이런 체인은 UTXO 정보(계정 잔고)를 비롯해 포크 시점까지의 모든 체인 히스토리를 기존 체인과 공유합니다. 그러나, 포크 시점부터는 새로운 체인에서 생성된 코인은 비트코인 네트워크 상 어떤 노드도 받아들이지 않으므로 더 이상 비트코인이 아닙니다.

비트코인 캐쉬 포크 후 어떤 체인이 비트코인이고 어떤 체인이 비트코인이 아닌 지에 대한 뜨거운 논쟁이 이어졌습니다. 비트코인 캐쉬 쪽 사람들 중에는 비트코인이 십 수년 전 사토시의 최초 백서에서 쓰여진 의미에 따라 정의되어야 한다고 주장했습니다. 이들은 비트코인 백서 상 일부 자구를 취사선택하여 자신들의 논리를 뒷받침했습니다. 하지만 컨센서스 기반의 시스템은 권위에 대한 호소가 통하지 않습니다. 컨센서스 기반의 시스템은

어떤 소프트웨어를 돌릴지, 공개시장에서 어떤 코인을 사고 팔 것인지 등에 대해 수많은 개인의 선택이 모두 합쳐져 결정됩니다.

위 포크의 사례에서는 지갑, 거래소, 상인 등 노드를 운용하는 사람들의 절대 다수가 상대적으로 개발자 저변도 좁고, 해시율도 낮은 소프트웨어로 전환하기도 원치 않았고, 이런 소위 "업그레이드" 기존 네트워크 생태계를 교란할 만한 가치가 있는지에 대해서도 의구심을 가졌습니다. 하드포크의 문제점은 모든 참여자가 합의를 해야만 성공할 수 있다는 점입니다. 한 명의 이탈자만 발생하더라도 두개의 코인이 만들어지고 맙니다. 따라서, 비트코인은 비트코인으로 남고, 비트코인 캐쉬는 별도의 코인이 된 것입니다. 포크 이전에 비트코인을 보유하고 있던 모두에게 비트코인 캐쉬가 주어졌기 때문에 많은 사람들이 비트코인 캐쉬를 매도해 일종의 "공짜 돈"을 챙겼고 비트코인 캐쉬의 가격을 더 떨어뜨리는 요인이 되었습니다.

오늘날, 비트코인의 포크는 비트코인 SV(Bitcoin SV, 비트코인 캐쉬의 포크), 비트코인 골드(Bitcoin Gold), 비트코인 다이아몬드(Bitcoin Diamond), 비트코인 프라이빗(Bitcoin Private)까지 수십가지 종류에 이릅니다. 이런 코인은 모두 해시율, 개발자층, 체인 활동 수준(on-chain activity), 거래소 유동성 등이 매우 미약합니다. 부족한 유동성으로 인해 가격을 끌어올린 후 폭락시키는 수법을 통해 이익을 취하려는 작전 세력의 목표가 되기 십상이라, 가격이 엄청난 규모로 폭등한 후 또 그만큼 절망적인 폭락을 거듭하곤 합니다. 이 중 많은 코인이 지갑 해킹, 51% 공격 같은 재난에 시달리기도 했습니다. 일부는 명백한 사기극의 일환이거나, 투기꾼이의 도박 수단에 지나기 않기도 합니다. 또한 이 중 대부분이 구조상 고도로 중앙집중화 되어있기도 합니다. forkdrop.io/ 웹사이트에서 현재 74 개의 비트코인 아류를 확인할 수 있습니다.



소프트포크(soft-fork)에서 나온 코인은 이전 노드와 호환이 됩니다.
하드포크(hard-fork)는 하위호환이 되지 않는 UTXO 를 생성하며 이전 노드와 호환이 안됩니다.

또 다른 코인들은 라이트코인(Litecoin)이나 도지코인(Dogecoin)처럼 비트코인과 유사한 코드를 차용했지만 비트코인의 UTXO 를 이어받지 않고 애초에 독자적인 장부를 시작한 경우도 있습니다. 이런 경우는 비트코인과 동일한 코드를 사용함에도 불구하고 공유하는 거래기록이 없기 때문에 통상 엄밀한 의미에서 비트코인의 포크로 분류되지는 않습니다.

비트코인 포크의 존재는 비트코인 자체의 2,100 만개로 공급이 제한되어 있는 속성에는 영향을 미치지 않습니다. 포트녹스 요새(Fort Knox) 최고의 보안 시설에 전세계 금이 모두 저장되어 있다고 상상해보겠습니다. 이때, 누군가 허름한 판잣집을 세워 포트녹스 라이트(Fort Knox Lite)라고 이름 짓고 경비원 하나를 세운 다음 노랗게 색칠한 돌멩이를 한가득 집어넣습니다. 그리곤 세상에 "포크한 금"이라며 금을 보관하고 있는 모두에게 동일한 무게의 색칠한 돌멩이를 배분한다고 상상해보겠습니다.

비트코인의 보안을 유지하기 위해서는 51% 공격이 어렵도록 만들기 위해 많은 채굴자가 필요합니다. 채굴자가 많이 없는 비트코인 포크는 마치 경비원 한 명이 지키는 판잣집처럼 공격에 쉽게 노출됩니다. 몇 안되는 개발자들이 동료 심사도 충분히 거치지 못하고 배포한 코드는 역시나 판잣집처럼 구조적으로 부실할지 모릅니다. 포크 코인은 비트코인의 규칙을 따르지 않으므로, 기존 어떤 노드에서도 받아들여지지 않습니다. 마찬가지로, 화학적 테스트를 통해 금을 감별할 수 있는 사람이라면 색칠한 돌멩이를 금으로 받아들이는 경우는 없을 겁니다. 모든 보유자는 포크 코인과 색칠한 돌멩이를 공짜로 받았기 때문에 취득 원가는 영(0)에 불구합니다. 따라서 비트코인 포크에 대한 시장의 관심은 제한적일수 밖에 없습니다.

수천 가지 중 어느 것도 두드러지는 시가총액을 이루지 못한, 비트코인 복제품을 검토하면서 다음과 같은 역설을 떠올려 보시기 바랍니다. 비트코인 포크를 만드는 것은 돈도 들지 않고 쉽지만, 비트코인의 규칙을 바꾸거나 새로운 비트코인을 만드는 것은 매우 어렵다는 사실입니다. 다음에 비트코인에 대한 지식이 부족한 사람이 비트코인의 어떤 점이 특별한지 물어본다면 이 내용으로 답해주시기 바랍니다.

분산 시스템의 특성 상 비트코인 생태계는 현상 유지를 강하게 선호하는 경향을 띕니다. 커다란 변화가 적용되기까지는 대체로 짧게는 수개월에서 길게는 수년에 걸쳐 설계하고, 토론하고, 동료 심사를 거치게 됩니다. 이런 엄격한 과정은 글로벌 통화를 지향하는 시스템이

갖추어 마땅한 강점입니다. 비트코인은 때론 서로 상충되는, 각자의 이기적 동기를 바탕으로 행동하는, 수천명의 개별 참여자들간 섬세한 줄다리기입니다. 이야말로 어떤 관리자도 존재하지 않는 진정한 의미의 무정부주의적 완전경쟁시장이라고 할 것입니다.

9. 앞으로의 방향은? (WHAT'S NEXT?)

비트코인은 암호화폐계의 마이스페이스(MySpace)인가?

어째서 저는 암호화폐 생태계 전반에 대한 책을 쓰지 않고 비트코인에 대한 책을 쓰게 되었을까요? 비트코인 말고도 수천개의 암호화폐가 넘쳐나는데 말입니다. 최초 암호화폐라는 점 외에 비트코인의 어떤 면이 특별한 것일까요? 비트코인은 새로운 경쟁 코인에 비해 속도도 느리고 기능도 부족한 것은 아닐까요?

이는 비트코인을 처음 접하는 분들이 곧잘 던지는 질문입니다. 비트코인의 작동 원리를 이해한 후, 논리적으로 다음 질문은 이와 같을 것입니다. "블록체인 기술은 아주 흥미롭네요. 새로운 버전의 블록체인이 나타나 비트코인이 마이스페이스와 같은 길을 걷게 되지 않을까요?"

경영학에서 해자(moat)란 사업체가 경쟁사의 손쉬운 신규 진입을 막기위한 경쟁 우위를 뜻합니다. 마이스페이스에게 해자는 친구 관계를 통해 얽혀 있는 거대한 사용자 기반이었습니다. 다른 친구들이 이미 사용하고 있지 않은 이상 경쟁사의 서비스로 옮겨갈 이유가 없었습니다. 탄탄히 얽혀 있는 사회 관계망이라는 커다란 해자를 가졌던 마이스페이스도 페이스북에게 잠식되기까지 채 1 년이 걸리지 않았습니다.

비트코인의 해자는 마이스페이스의 경우보다 훨씬 큽니다. 비트코인의 해자를 이해하기 위해 경쟁자가 비트코인을 대체하려면 무엇이 필요할지 알아보도록 하겠습니다.

수요와 유동성이 더 높은 화폐가 될 것

첫번째로 이해해야 할 점은 마이스페이스와 페이스북의 사례 경우 사용자가 추가비용 없이 마이스페이스와 페이스북의 계정을 모두 가질 수 있기 때문에, 비트코인에 적용하기 적절하지 않다는 것입니다. 실제로, 사용자들이 마이스페이스에서 페이스북으로 넘어가던 시기에 많은 사람들이 두 서비스의 계정을 모두 만들어 놓는 양상은 보였기도 합니다. 일단 페이스북 사용자수가 임계치를 넘어간 순간부터 사람들은 마이스페이스를 더 이상 사용하지 않았습니다.

그러나, 화폐는 이와는 다른 방식으로 작동합니다. 여러분이 1 달러 어치의 비트코인을 보유하고 있다는 것은, 1 달러 어치만큼 다른 화폐를 보유하지 않고 있다는 의미이기도 하기 때문입니다. 따라서 특정 화폐를 보유하기 위해서는 다른 화폐를 매도해야 합니다. 두 화폐에 동시의 가치를 둘 수 없는 것입니다. 이제 다음 질문에 대해 생각해보아야 합니다. 그 누가 되었든, 가장 유동성이 높고 저변이 넓은 화폐를 두고 다른 화폐를 보유할 이유가 있을까요? 답은 결국 투기(speculation) 목적 뿐인 것입니다. 특정 화폐를 보유하도록 경제 전체를 바꿀 수 있는 것이 아니라면, 해당 화폐가 지배적 위치에 도달할 가능성은 사라집니다.

비트코인의 유동성은 어떤 경쟁자와도 비견할 수 없습니다. https://messari.io/onchainfx 에 따르면 오늘날, 비트코인의 시가총액은 약 1,600 억 달러에 달합니다. 그 다음으로 가장 큰 경쟁자인 이더리움의 시가총액은 약 300 억 달러에 불과합니다. 가격 하락에 영향을 주지 않고 얼마나 많은 물량을 매도할 수 있는 지로 판단할 수 있는 진정한 유동성의 관점이라면 비트코인과 경쟁자의 간극은 더 커질 것입니다.

유동성은 눈덩이처럼 불어나는 성질이 있습니다. 가장 유동성이 높은 화폐를 보유하면 다른 사람들도 해당 화폐를 원하게 되고 이는 다시 해당 화폐의 유동성을 증가시킵니다. 가장 유동성이 높은 화폐 외에 다른 화폐를 보유한다는 것은 다른 사람들이 뒤따르기 바라며 기다리는 동안 여러 손해를 감수하는 상황이 됩니다. 이러한 경제적 유인들로 인해 유동성의 전환은 하루아침에 일어나기 어렵습니다.

10 년간 1,000 억 달러 어치 수준 이상의 보안을 입증할 것

환경적으로, 비트코인은 아무도 신경 쓰지 않는 쓸모 없는 괴짜 인터넷 실험에서, 비트코인 10,000 개로 한판의 피자를 구매할 수 있게 되고, 비트코인 당 최고가 20 만 달러로 상승하기까지 성장할 수 있는 기회를 누렸습니다. 이런 성장은 어떤 강력한 기관의 감시나 간섭 없이 대체로 조용히 진행되었습니다. 이 시기동안 비트코인은 여러 공격 가능성에 대해 세계적 수준의 보안을 이룩하고, 세계 최대의 해시 파워를 갖춘 네트워크를 구축할 수 있었습니다. 10 년이 넘는 기간동안 1,000 억 달러가 넘는 거래금액을 처리하면서 단 한번도 해킹을 당하지 않은 것입니다.

오늘날 새로운 암호화폐 네트워크를 조용히 출시한다는 것은 불가능에 가깝습니다. 암호화폐에 대한 많은 비밀들이 이제는 공공연한 정보가 되었습니다. 출시 시점에 시가총액이 100 억 달러에 달했고 현재는 그 절반 수준의 가치를 가진 블록체인

이오스(EOS)를 살펴보겠습니다. 이오스는 코드 상의 버그로 인해 출시 이틀만에 네트워크 동결을 겪게 되었습니다. 이 버그는 최소한의 감시와 검토를 거쳐 불과 몇 시간만에 패치를 통해 수정되었습니다. 여러분이라면 이런 네트워크에 1,000 억 달러 어치의 거래를 넣으시겠습니까? 이오스가 10 년 후 여전히 존재할 수도 있겠지만, 그때가 오면 비트코인은 20 년이 넘는 기간동안 수조 달러 어치의 거래를 처리하고 있을 것입니다.

기존 해시파워로부터의 공격을 물리칠 것

수천개의 코인이 불과 수십 종에 불과한 해시 알고리즘을 채택하고 있어, 새로운 코인은 기존 해시파워의 51% 공격 위협에 놓이게 됩니다. 이 위험은 비트코인 골드(Bitcoin Gold)와 몇몇 코인에 실제 발생한 바 있습니다.

새로운 경쟁자는 기존 해시파워가 이끄는 공격에서 살아남거나, 전문화된 ASIC 장치를 활용하지 않는 알고리즘을 차용해야만 합니다. ASIC 을 활용하지 않는 시스템은 시중에서 손쉽게 구할 수 있는 GPU 를 대여하는 방식으로 공격당할 수 있습니다. 이오스의 경우처럼 출시 직후부터 커다란 금액을 처리하는 것도 바람직하지 않은데, 이는 무모한 동시에 쉽게 중앙집권식의 패치 형태에 손쉽게 빠지는 방식이기도 합니다. 따라서 자금을 모집하는 것도 바람직하지 못할 뿐 아니라, 보안 수준이 비례적으로 차차 성장할 수 있도록 비트코인 같은 방식의 공정한 출시(fair launch)를 통해 네트워크 가치가 점차적으로 성장해야 합니다. 그렇지만, 반대로 점진적 성장만으로는 시간이 지나면서 비트코인의 사용자 저변과 유동성은 영영 따라잡을 수 없게 됩니다.

고도로 분산화 될 것

비트코인 보안 모델의 많은 부분이 고도의 분산화에 기인합니다. 이는 비트코인 프로토콜이 바꾸기 어려우며, 고정된 공급량 등의 코드 상 약속된 성질이 준수될 것이라고 믿을 수 있습니다. 비트코인의 이런 특징은 많은 사업자와 채굴자가 담합하여 블록 용량에 관한 특정

변화를 몰아 부치려 했을 때 증명된 바 있습니다[8]. 해당 포크는 사용자의 지지를 받지 못하면서 대실패로 돌아갔습니다.

고도로 분산화된 네트워크가 되려면, 실패나 담합의 중심점이 될 수 있는, 잘 알려진 사람들이 설립한 회사나 팀이 존재하지 않아야 합니다. 또한, 중앙집권적 일수 밖에 없는, 실험적이고 빠르게 새로운 기능을 도입하고 업그레이드를 적용하는 방식도 적용할 수 없게 됩니다. 따라서 비트코인의 경쟁자는 빠르게 새로운 기능을 도입하기 위해 중앙집권화 되거나, 충분히 분산화를 이루는 대신 비트코인을 영영 따라잡지 못하게 됩니다.

세계 최고의 개발자들을 끌어들일 것

리눅스(Linux)가 개발자 사이에서 거대한 돌풍을 일으켜 다른 *Nix 시스템의 경쟁 가능성을 배제한 것처럼, 비트코인도 마찬가지 영향을 일으키고 있습니다. 이 개발자 커뮤니티는 매일매일 성장하고 있으며, 새로운 회사들의 바탕이 되고 있습니다. 비트코인의 경쟁자는 수십 개의 회사, 교육 프로그램, 컨퍼런스를 포함하는 기하급수적으로 성장하고 이 개발자 커뮤니티로부터 인지도를 경쟁해야만 합니다.

세계적 금융 네트워크를 키울 것

전세계 수백개에 달하는 거래소, CME 선물 거래소, CBOE 선물 거래소, 수백개의 헷지 펀드와 거래 부서들, 베네수엘라 볼리바 같이 실패한 화폐의 대안으로 이미 비트코인을 사용하고 있는 사용자 네트워크까지, 비트코인 경쟁자는 이 모든 것을 대체할 수 있는 기반을 이룩해야만 합니다.

CME(Chicago Mercantile Exchange, 시카고상품거래소)나 CBOE(Chicago Board Options Exchange, 시카고옵션거래소) 같은 기관이 기존 거래량이 충분하지 않은 경쟁 코인을 모두 상장시키지는 않을 것입니다. 비트코인 대신 새로운 경쟁 코인을 채택하도록 수백개에 달하는 사업체를 설득해야 하기도 할 것입니다. 대체로 보안이 더 취약하고, 유동성이 낮으며,

[8] 이면 합의를 통해 진행되다 종국에 무산된, 소위 세그윗 2X(Segwit2X) 라고 불리는 포크에 대해서 다음 자료를 통해 더 자세히 알아보시기 바랍니다. https://bitcoinmagazine.com/articles/now-segwit2x-hard-fork-has-really-failed-activate

개발자 저변이 좁고, 전세계적 대중화 수준도 낮을 경쟁 코인을 말입니다. 어려운 일이 아닐 수 없습니다.

좀 더 건전화폐(sound money)가 될 것

비트코인의 목적이 빠르고 저렴한 송금수단이라는 판단은 대단히 잘못된 이해입니다. 동일한 기록을 전세계에 무수히 많이 중첩적으로 관리하는 근본적인 특성에 기반한 점을 상기해본다면 이 점은 자명합니다. 오히려, 비트코인의 주된 실사용 방식으로써 검열할 수 없는 건전화폐(censorship resistant sound money)의 역할이 대두되고 있습니다.

저렴한 송금 같은 다른 모든 기능은 사실 금상첨화의 부가 요소에 지나지 않습니다. 비트코인 경쟁자의 대부분이 빠른 결제 기능을 제공해야만 한다고 생각하나, 이 기능은 전세계 수많은 기존 중앙집중화된 기업들이 이미 충분히 괜찮은 수준으로 제공하고 있는 서비스이기도 합니다. 여기에, 빠르게 성장하고 있는 비트코인 기반의 라이트닝 네트워크(Lightning Network)가 솔루션을 제공할 수 있는 기능이기도 합니다.

건전화폐로써 기능하기 위해서는 무엇보다도 분산화와 쉽게 변경하거나 공격할 수 없는 성질을 갖추는데 모든 최우선 순위를 두어야 합니다. 사이퍼펑크(cypherpunk) 생태계 상에서 우연히 점진적으로 성장해온 비트코인과 달리, 경쟁 코인들은 대부분 이윤을 추구하는 중앙집권화된 팀이 설계하였기 때문에 건전화폐의 특성을 달성하기 어렵습니다.

비트코인의 향후 개발 방향

지금까지 비트코인 프로토콜의 개발 과정을 살펴보았습니다. 이제 미래로 눈을 돌려 향후 도달할 비트코인의 개선 사항을 살펴보도록 하겠습니다.

비트코인은 프로그래밍이 가능한 화폐로, 이를 기반으로 무수한 서비스를 만들 수 있습니다. 이는 이전까지 없었던 완전히 새로운 컨셉트로, 아직 우리는 겨우 그 가능성을 옅본 것에 지나지 않습니다.

라이트닝 네트워크(Lightning Network)

비트코인은 블록 공간에 대한 수요가 높아지면서 높은 수수료의 문제점을 경험한바 있습니다. 오늘날, 비트코인은 블록에 포함된 거래 수에 따라 초당 3 개에서 7 개 정도의 거래를 처리할 수 있습니다. 이때 유념할 점은 각 거래가 실제로는 배칭(batching)을 통해

수백명에게 송금하는 거래일 수 있다는 것입니다. 어찌되었든, 이 정도 거래 처리량은 글로벌 결제 네트워크가 되기에는 부족한 것이 사실입니다.

이 문제에 대한 순진한 해결책은 블록 용량을 늘리는 것인데, 실제 비트코인 캐쉬(Bitcoin Cash)를 포함해 몇몇 경쟁 화폐는 이런 접근법을 택하기도 했습니다. 블록 용량을 늘리는 것은 노드의 개수나 지리적 분포 수준 등 분산화에 악영향을 미칠 수 있기에, 비트코인은 이런 방식을 취하지 않습니다. 하드웨어 기술의 발전 등으로 블록 용량의 증가가 가능하게 되더라도, 고도로 분산화된 비트코인의 특성으로 인해 블록 용량을 변경하는 하드포크가 많은 혼란을 야기하는 동시에 네트워크의 전면적 분할에 따른 새로운 코인의 생성으로 이어질 수 있습니다.

블록 용량의 증가는 비트코인을 전세계 결제 시스템으로 만드는 문제를 원천적으로 해결하지도 못합니다. 비트코인은 결국 이 방식으로는 확장에 한계가 있을 수밖에 없습니다. 여기에 라이트닝 네트워크(Lightning Network)가 활용됩니다. 라이트닝 네트워크는 네트워크 밖에서(off-chain) 거래를 기록한 후 일정 기간마다 정기적으로 비트코인 네트워크 상에서 일단의 소프트웨어로 구성된 별도의 프로토콜입니다. 라이트닝 네트워크는 그 자체로 책 한권 전체가 필요할 주제이므로, 간단히 다루도록 하겠습니다.

모든 거래가 블록체인에 기록될 필요는 없다는 개념이 라이트닝의 핵심입니다. 예를 들어, 저와 여러분이 바에 가서 술을 마신다면 술을 시킬 때마다 계산을 하지 않고 일단 장부에 올려놓은 뒤 마지막에 한번만 결제하면 됩니다. 술을 시킬 때마다 매번 결제하는 것은 시간 낭비입니다. 한 나라 수준의 에너지를 사용하는 비트코인 네트워크에 커피나 맥주 한잔의 구입내역을 올리고 전세계 수천개의 컴퓨터에 기록하는 것은 확장에 확장하기도 어렵고 프라이버시 측면에서도 좋은 방법이 아닙니다.

라이트닝 네트워크가 성공한다면 비트코인의 많은 단점을 보완할 것입니다.

- 사실상 무한정한 거래량 출력(transaction throughput). 수십만건의 소액 거래를 수행한 후 한번의 정산을 통해 비트코인 네트워크에 기록하는 방식으로 비트코인의 한정된 초당 거래량을 극복할 수 있습니다.
- 즉각적 거래확인(instant confirmations). 블록 채굴을 기다리지 않아도 거래가 확정될 수 있습니다.
- 소액 거래에 적합한 소액의 거래 수수료.

- 프라이버시 증대. 모든 거래가 전세계에 전송되는 비트코인 네트워크 상(on-chain) 거래와 달리 라이트닝 세부 거래내역은 거래 당사자들만 알 수 있습니다.

라이트닝은 비트코인 네트워크 상에서(on-chain) 일정량의 비트코인을 예치해 놓고 해당 비트코인을 라이트닝 네트워크가 즉각적이고 낮은 수수료의 거래에 활용하도록 하는, 송금 채널(Payment Channels)이라는 컨셉트를 활용합니다. 라이트닝 네트워크의 개발은 아직 초기 단계에 있으나, 이미 다양한 가능성을 보여주고 있습니다. 라이트닝에 기반한 소액 결제로 기고문을 읽을 수 있는 서비스를 https://yalls.org/ 에서 확인해 보시기 바랍니다.

우주 시대의 비트코인

비트코인은 (머리 속에 기억할 수 있기 때문에) 압수할 수 없고, (여러분이 직접 할 수도 있는) 단 하나의 정직한 채굴자만 거래내역을 네트워크로 받아들이면 되기 때문에 송금도 막을 수 없는, 검열이 불가능한 특성이 있습니다.

그럼에도 불구하고, 인터넷을 통해 송신되는 비트코인의 특성으로 인해 네트워크 전체 레벨에의 검열 가능성은 여전히 존재합니다. 비트코인을 단속하려는 권위주의적 정부가 나라 전체를 통하는 비트코인 트래픽을 막으려 할 수 있습니다.

블록스트림 위성(Blockstream Satelite)는 인터넷 접속이 불가능한 외딴 지역에서도 비트코인을 활용할 수 있도록 만드는 것과 더불어, 국가적 단위의 네트워크 검열 우회를 위한 첫 시도입니다. 곧 양방향 통신(bi-directional communication) 기능도 갖출 예정인 이 위성을 통해 위성 안테나와 상대적으로 저렴한 장비만 갖추면 비트코인 블록체인에 접속하고 다운로드 할 수 있습니다. 공공 인프라가 전혀 필요하지 않은(off-the-grid) 메쉬 네트워크(mesh networks)를 개발하는 TxTenna 와 같은 프로젝트도 있습니다. 위성 연결과 같이 사용하면, 이 방식을 사실상 누구도 막을 방법이 없습니다.

더 읽어볼 거리

자! 여기까지 우리는 비트코인의 발명을 되짚어 보았습니다. 부디 이전과 다른 새로운 시각을 얻고, 더 알아볼 준비가 되는 과정이셨기 바랍니다. 이제 무엇을 살펴보아야 할까요? 더 읽어볼 자료를 아래에 정리해보았습니다.

비트코인의 경제학 분야 추가 자료:

- *비트코인 스탠다드(The Bitcoin Standard)* - 사이프딘 아무스(Saifedean Ammous)
- *비트코인 투자 이론(Bitcoin Investment Theses) - 피에르 로챠드(Pierre Rochard)* *https://medium.com/@pierre_rochard/bitcoin-investment-theses-part-1-e97670b5389b*
- 비트코인 상승 시나리오(The Bullish Case for Bitcoin) – 비자이 보야파티(Vijay Boyapati) https://medium.com/@vijayboyapati/the-bullish-case-for-bitcoin-6ecc8bdecc1
- 아동 서적: 비트코인 머니(Bitcoin Money) – 마이클 카라스(Michael Caras)

컴퓨터공학 분야 추가 자료:

- 비트코인 백서(The Bitcoin Whitepaper) – 사토시 나카모토(Satoshi Nakamoto) https://bitcoin.org/bitcoin.pdf
- 비트코인, 공개 블록체인 프로그래밍(Mastering Bitcoin) – 안드레아스 안토노폴로스(Andreas Antonopoulos)
- 밑바닥부터 시작하는 비트코인(Programming Bitcoin) - 송재준(Jimmy Song)
- 비트코인 세미나 – 송재준 (Jimmy Song) https://programmingblockchain.com

비트코인의 역사와 철학 관련 추가 자료:

- 비트코인 심기(Planting Bitcoin) – 댄 헬드(Dan Held) https://medium.com/@danhedl/planting-bitcoin-sound-money-72e80e40ff62
- 비트코인 거버넌스(Bitcoin Governance) – 피에르 로챠드(Pierre Rochard) https://medium.com/@pierre_rochard/bitcoin-governance-37e86299470f
- 비트코인 과거와 미래(Bitcoin Past and Future) – 무라드 마무도프(Murad Mahmudov) https://blog.usejournal.com/bitcoin-past-and-future-45d92b3180f1
- 통화 전쟁(Currency Wars)과 불변성의 순간(The Moment of Immutability)를 비롯한 안드레아스 안토노폴로스(Andreas Antonopoulos)의 모든 영상

비트코인 생태계의 커다란 부분이 트위터(Twitter) 상에 존재합니다. 아래에 팔로우 추천 인물들을 순서와 상관없이 정리해보았습니다.

@lopp
@pwuille
@adam3us
@danheld
@TraceMayer
@pierre_rochard
@bitstein
@theonevortex
@AlenaSatoshi
@WhatBitcoinDid
@stephanlivera
@TheBlock__
@TheLTBNetwork
@real_vijay
@jimmysong
@Excellion
@starkness
@dickerson_des
@roasbeef
@saifedean
@Melt_Dem
@_jillruth
@giacomozucco
@Snyke
@aantonop
@MustStopMurad
@danheld
@peterktodd

@dergigi

@skwp (본 저자)

제 홈페이지 yanpritzker.com 에서 저의 다른 저작을 보실 수 있습니다. 다시 뵙기를 고대하겠습니다.

감사의 말씀

본 저작의 집필 과정에서 조언을 주신 많은 분들과 특히 Joe Levering, Phil Geiger, Yury Pritzker, Jonathan Wheeler, Walter Rosenberg, 그리고 Michael Santosuosso 에게 감사드립니다.

비트코인 프로그래밍 세미나를 통해 이 책의 탈고에 많은 자극을 주신 송재준(Jimmy Song)님에게 감사드립니다.

저자

저자 얀 프리츠커(Yan Pritzker)는 지난 20 년간 개발자이자 스타트업 기업가로 활동하였습니다. 가장 최근에는 Reverb.com 의 공동 창업자이자 CTO 로써 2012 년부터 2018 년까지 테크놀로지와 인프라스트럭쳐를 관장하였습니다. 현재는 초기 단계의 스타트업을 대상으로 비트코인 교육 및 컨설팅에 전념하고 있습니다.

현재 저자는 비트코인 및 관련 주제에 대해 웹사이트 yanpritzker.com 에 기고하고 있습니다.

저자의 트위터는 @skwp 입니다.

옮긴이

옮긴이 허성필은 한국공인회계사이며 안진회계법인에서 회계감사, 한국투자증권에서 크레딧 애널리스트 업무를 거쳐 현재 KTB 자산운용에서 대체투자 투자운용을 담당하고 있습니다.

huhsungpil@gmail.com

초안, 2021 년 2 월 27 일