

# 비트코인 디플로마

비트코인을 기반으로 한 금융 교육

학생 워크북

제3판 | 2022년 9월

한글번역 : ATOMIC BITCOIN

*Mi Primer Bitcoin* ha creado este trabajo y lo ha hecho disponible gratuitamente bajo **Creative Commons**.

Este trabajo tiene una licencia **Creative Commons**  
**Atribución-NoComercial-SinDerivadas**  
**4.0 Internacional (CC BY-NC-ND 4.0)**



# 비트코인 디플로마

비트코인을 기반으로 한 금융 교육

학생 워크북

제3판 | 2022년 9월

한글번역 : ATOMIC BITCOIN

PARA DONAR:



bc1qc0h5ddd4ln4z05u55l87cp4umg8eg0jjkhcgvf



## 감사인사

**비트코인 디플로마**는 대성공을 거두었으며 우리가 상상할 수 있었던 것보다 빠르게 성장했습니다. 우리를 여기까지 데려온 모든 훌륭한 사람들에게 공을 돌리고 싶습니다.

커리큘럼의 핵심 팀인 이 콘텐츠의 원동력은 Dalia Platt, Gloriana Solano, Raúl Guirola 및 Robert Malka입니다. 그들은 몇 달 동안 무대 뒤에서 지칠 줄 모르고 일했습니다. 처음에는 심각한 시간 위기로 이것을 만든 다음 계속 배우고 개선했습니다. 이 네명이 없었다면 이 모든 것이 불가능했을 것입니다. 그 과정에서 이 핵심 그룹은 Giacomo Zucco, Pedro Solimano, María Andrée Maegli, Alejandro Machado, Gerson Martínez 및 Vriti Saraf의 도움을 받았습니다. ACTIVA의 디자이너 Gerardo Apóstolo와 Enrique Jubis도 놀라운 일을 해냈습니다.

**비트코인 디플로마**의 이야기는 2022년 2월 엘살바도르 산마르코스에 있는 공립학교인 라 파체코(La Pacheco) 회의에서 시작됩니다. 우리는 400명이 넘는 개인 기부자들로부터 기금을 모아 4월에 수업을 시작하고 6월에 첫 번째 수업을 졸업하면서 빠르게 움직였습니다.

그 2월 모임의 빌더들 역시 이 이야기에서 빼놓을 수 없는 인물들입니다. La Pacheco의 이사인 Asael Rodríguez는 변화하는 세상을 위해 학생들을 준비시키는 데 전념했습니다. 이미 La Pacheco를 지원하고 있던 Rodrigo Ayala 대리인도 비트코인 교육의 필요성을 인식했습니다. IBEX Mercado의 커뮤니티 빌더인 Carlos Toriello는 저를 포함한 다른 비트코이너를 초대하여 학교를 방문하고 커리큘럼에 대해 배우도록 했습니다.

Carlos와 IBEX는 여기에서 자신만의 섹션을 가질 자격이 있습니다. 그들은 La Pacheco에 새 카페테리아를 짓기 위해 기금을 마련했고, 그 대의를 옹호했으며, 나머지 비용을 조달하는 데 도움을 주었습니다. **비트코인 디플로마**는 이제 다른 장소와 다른 스폰서와 함께 존재하지만 La Pacheco에서 파일럿 프로그램의 성공을 기반으로 구축되었으며 단순히 이들 없이는 일어나지 않았을 것입니다.

Mi Primer Bitcoin은 엘살바도르의 모든 사람과 전 세계의 모든 사람에게 비트코인에 대한 양질의 편견 없는 교육을 제공하는 단일 사명을 가진 비영리 조직입니다. 비트코인을 채택한 최초의 국가로서 우리는 엘살바도르가 풀뿌리 사례가 될 수 있다고 믿습니다. 우리의 비전은 국가를 가르치고 세상을 바꾸는 것입니다. 미친 소리로 들리겠지만, 우리가 가고 있고 **비트코인 디플로마**가 그 중 큰 부분을 차지한다고 생각합니다.

더 나은 세상을 위해

John Dennehy

설립자

Mi Primer Bitcoin

한글번역

ATOMIC BITCOIN

# 목차

## 제 1장

소개: 화폐시스템	9
✍ 1.1 수업 활동: 돈 소개	10
📖 1.2 오늘날 돈에 어떤 문제가 있을까요?	10
📖 • 발전결과	10
🔗 - 수요 vs. 수단	11
📖 • 현대화	11
📺 1.3 돈의 정의	13
✍ • 돈의 기능	13
🔗 • 돈의 특성	14
📖 • 기존 화폐 및 화폐 자산	15
✍ - 돈의 본질	15
✍ - 수업 활동: 건포도는 좋은 돈 일까요?	17

## 제 2장

돈의 역사, 진화 및 평가 절하	19
📖 2.1 돈의 역사	20
✍ 2.2 수업 활동: 물물교환 게임	20
📺 2.3 시간에 따른 화폐의 진화	22
📖 • 역사 속의 국제통화기준	22
📖 2.4 Fiat로의 갑작스러운 전환	23
📖 2.5 중앙 은행	24
✍ 2.6 수업 활동: 부분 준비금	25

## 제 3장

법정화폐와 중앙 집중화의 효과	27
✍ 3.1 수업 활동: 경매!	28
📺 3.2 인플레이션	28
📖 • 우리는 왜 인플레이션을 신경 써야 할까요?	29
📖 • 현대 경제학자들은 우리에게 어떻게 얘기할까요?	29
📺 • 인플레이션의 원인	30
🔗 • 시간 경과에 따른 인플레이션	32

☞	3.3 검열	33
☞	3.4 제한	33
☞	3.5 중앙화 vs. 탈중앙화	35
☞	3.6 결론	36

## 제 4장

	<b>비트코인</b>	<b>39</b>
☞	4.1 비트코인은 왜 만들어졌을까요?	40
☞	• 해결해야 할 문제는 무엇일까요?	40
⊗	• 이러한 문제는 어떻게 해결되었을까요?	40
☞	• 누가 해결했을까요?	40
☞	• 사토시는 어떤 어려움을 겪었을까요?	42
☞	• 비잔틴 장군 문제는 무엇일까요?	43
☞	• 이것이 비트코인과 어떤 관련이 있을까요?	44
☞	4.2 비트코인 소개	44
☞	4.3 비트코인과 법정화폐의 차이	48
☞	4.4 비트코인 구성요소	50

## 제 5장

	<b>비트코인의 구매, 보관 및 이동</b>	<b>53</b>
☞	5.1 입금 및 출금 통로	54
☞	• 비트코인 살 돈이 충분한가요?	54
☞	5.2 비트코인 보관	55
☞	• 지갑과 라이트닝	55
☞	• 사토시를 보내거나 받으려면 어떻게 해야 할까요?	56
☞	5.3 거래 주기(On-chain)	57
☞	• 비트코인 거래란 무엇일까요?	57
☞	• 거래와 저장을 위한 브릿지 및 정류장	57
⊗	• 거래는 어떻게 이루어지나요?	58
⊗	• UTXO - '사용하지 않은 동전'	60
☞	• 거래 확인	61



## 제 6장

<b>가치저장 및 지불 네트워크로서의 비트코인</b>	<b>63</b>
☞ 6.1 이중 지불 문제	64
☞ 6.2 메모리 그룹 및 멤풀	65
✎ 6.3 수업 활동: 거래가 확인되었지만 승인되지 않았습니다	67
☞ 6.4 비트코인 네트워크 (On-Chain)	68
☞ • 풀 노드	68
✎ • 수업 활동: 거래 상태	69
📺 6.5 라이트닝 네트워크 (Off-Chain)	70
☞ • 레이어 1(또는 기본 레이어)과 레이어 2의 차이점은 무엇일까요?	70
✎ • 수업 활동: 라이트닝 작동 방식	73

## 제 7장

<b>채굴자와 비트코인 채굴</b>	<b>77</b>
☞ 7.1 채굴 노드	78
☞ • 채굴자간 수학적 경쟁은 어떤 것일까요?	78
☞ 7.2 해시의 중요성 이해하기	79
☞ • 함수란 무엇일까요?	79
☞ • 해시란 무엇일까요?	80
☞ • SHA-256이란 무엇일까요?	80
✎ - 수업 활동: 해시 생성	80
☞ • 논스란 무엇일까요?	81
☞ • 머클 트리란 무엇일까요?	81
☞ 7.3 채굴	82
☞ • 신뢰하지 말고 검증하세요	84
☞ • 블록 해시	85
☞ • 블록 논스	86
✎ • 수업 활동: 실시간 블록 분석하기	86

## 제 8장

<b>최소성, 비용, 가격 및 변동성</b>	<b>89</b>
☞ 8.1 블록 보상의 중요성	90
☞ 8.2 반감기	90
📌 • 반감기 이벤트	90
☞ 8.3 시간 경과에 따른 비트코인의 가치	91
☞ • 중장기 요인	93
☞ 8.4 채굴자에 대한 보상	96
☞ • 채굴 난이도	96
☞ 8.5 무엇을 또는 누구를 조심해야 할까요?	97
☞ • 비트코인 공격	97
☞ • 51% 공격이란 무엇일까요?	98

## 제 9장

<b>비트코인의 현재와 미래</b>	<b>101</b>
☞ 9.1 사용되는 에너지	102
☞ 9.2 혁신	102
☞ • 소프트웨어 - 비트코인 코어	102
☞ • 세그윗, 탭루트 및 슈노르 서명	103
☞ • 타로	104
☞ 9.3 비트코인과 엘살바도르의 미래	104
✍ 9.4 수업 활동: 비트코인 시뮬레이터	107

## 제 10장

<b>최종 프로젝트</b>	<b>109</b>
✍ • 왜 비트코인 일까요?	110

## 추가

<b>디지털 서명의 마법</b>	<b>115</b>
☞ • 공개 키 및 개인 키	116
☞ • 디지털 서명	117
☞ • 유효한 거래	117









## 제 1장

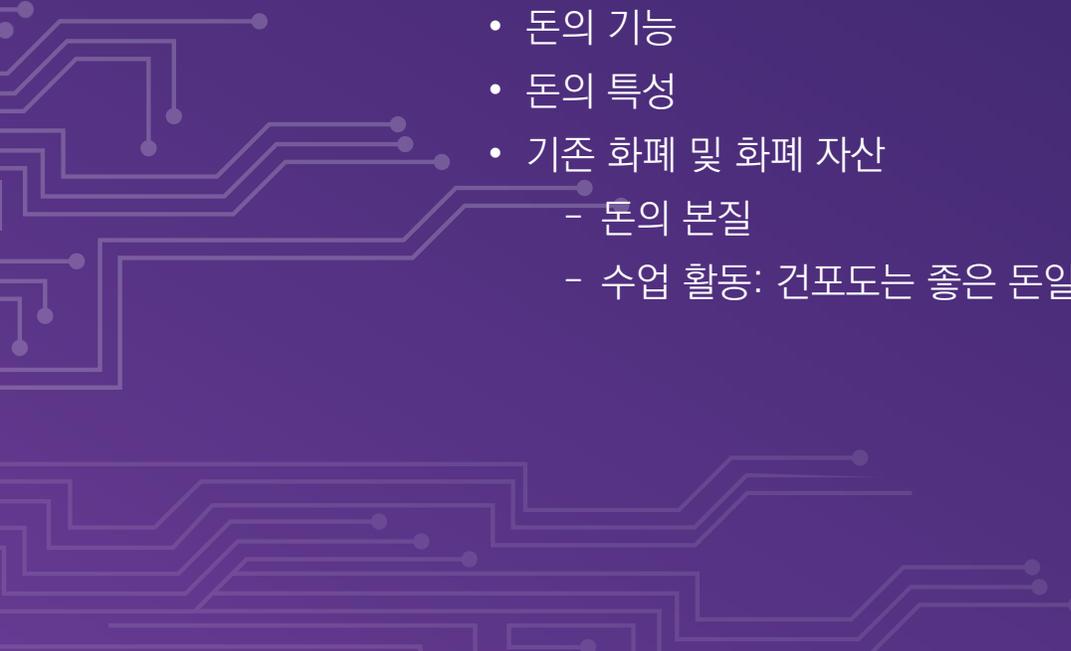
# 소개: 화폐시스템

1.1 수업 활동: 돈 소개

1.2 오늘날 돈에 어떤 문제가 있을까요?

- 발전결과
  - 수요 vs 수단
- 현대화

1.3 돈의 정의

- 돈의 기능
  - 돈의 특성
  - 기존 화폐 및 화폐 자산
    - 돈의 본질
    - 수업 활동: 건포도는 좋은 돈일까요?
- 

# 소개: 화폐 시스템

## 1.1 수업 활동: 돈 소개

**수업 활동.** 이 활동을 하기 위해 교사의 지시를 기다리세요.

## 1.2 오늘날 돈에 어떤 문제가 있을까요?

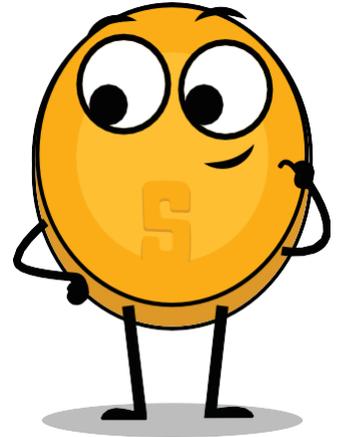
우리는 인생에서 위기를 극복하면서 살아오고 있습니다. 또한 자기계발과 생산적이고 창의적이며 가치 있는 삶을 살기를 원하는 것은 자연스러운 인간의 과정이지만 아래와 같은 문제가 있습니다.

- 소수를 위한 것은 많지만 다수를 위한 것은 거의 없는 세상에 살고 있습니다.
  - 경제력이 낮은 사람은 동일한 기회를 갖지 못합니다. 왜냐하면?
    - 그들과 같은 수준의 교육을 받을 수 없습니다.
    - 사업을 시작하는 데 필요한 자금을 확보할 수 없습니다.
- 빈곤을 줄이고 건강한 사회가 되려면 다음을 수행하는 것이 중요합니다.
  - 모두를 위한 금융 교육을 쉽게 해야 합니다.
  - 돈을 관리하는 능력을 키우는 것.
  - 새로운 기술을 책임감 있게 사용하는 방법을 배웁니다.
  - 미래를 위한 계획을 하세요.

우리는 **비트코인**이 도구이자 돈의 한 유형이라는 것을 알게 될 것입니다.

- 투명하고, 분산되고, 글로벌하고, 디지털이고, 저렴하고, 프로그래밍 가능하고, 쉽고 빠르게 접근할 수 있어 여러 문제를 해결할 수 있습니다.

## SATOSHI



저는 **비트코인 디플로마** 과정에서 여러분을 도와줄 대화형 조수인 **SATOSHI**입니다. **비트코인 공부를 같이 해볼까요?**

### 발전결과

- 사람들은 항상 미래를 위해 돈을 저축할 대상이 필요했습니다.
  - 가치 저장을 위해 임금, 시간, 에너지를 교환하는 방법.
- 우리가 진화하지 않았다면 물물교환 경제로 전락했을 것입니다.
  - 누군가가 사고 싶어하는 모든 것은 그 사람이 제공할 수 있는 것과 교환되어야 합니다.
- 기술 개발은 사회와 전세계 문명에 혁명을 일으켰습니다. 대부분 미래 삶의 질을 향상시키는 데 관심을 가지고 있습니다.
  - 기술이 발전하고 생산성이 향상됨에 따라 다음의 현상이 발생해야 합니다.
    - 자연스럽게 물건 가격이 낮아지는 것.
    - 통화의 구매력이 강화되는 것.
    - 더 적은 비용으로 더 많은 것을 살 수 있게 되는 것.
  - 그러나 반대 현상이 발생합니다.
    - 통화의 구매력이 약해지며 같은 물건을 구매하기 위해 더 많이 지출하게 됩니다.

- 어떻게 이렇게 되었나요?
- 어떻게, 왜, 무엇을 위해 더 많은 돈이 만들어지고 그 결과는 무엇인가요?
- 오늘날 금융 시스템 뒤에 숨겨진 것은 무엇일까요?
- 통화의 구매력이 내려가는 보이지 않는 위험은 무엇일까요?
- 저축에 추가적인 가치를 줄 수 있는 방법은 무엇일까요?

- 오늘날 은행과 정부만이 화폐를 발행할 수 있는 권한을 가지고 있습니다.

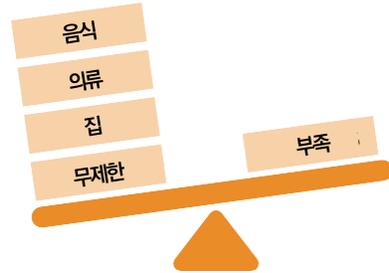
돈이 그냥 없어지지 않습니다. 정부는 공공 지출을 조달하는 데 필요한 금액을 인쇄하고 경제에 자원을 투입한 다음 세금 형태로 인출합니다.

- 우리가 버는 것보다 더 많이 쓴다는 것에 문제가 있습니다. 결과적으로 다음과 같은 일이 일어납니다.
  - 돈의 가치와 현대 은행 시스템에 대한 신뢰 상실.
  - 세계 경제 및 정치 불안정은 전쟁을 발생시키기도 합니다.

### 수요 vs 수단



우리의 수요는 끝이 없지만 자원은 부족합니다.



### 현대화

“은행은 우리 돈을 보관하고 전자적으로 이체한다고 믿어야 하지만, 준비금이 거의 없는 신용 거품의 물결에 그것을 빌려줍니다.”

-사토시 나카모토



정부, 기업, 많은 사람들이 돈이 필요하게 되고 은행에 요청합니다. 그들은 그 부채에 대해 이자를 지불합니다.



은행은 중개자입니다. 즉, 예금자로부터 돈을 사서 필요한 사람에게 더 높은 이율로 판매합니다.



많은 사람들 돈을 저축합니다. 그들은 은행에 돈을 예금하고 약간의 이자를 받습니다.

# 소개: 화폐 시스템

은행 업무는 다음으로 구성됩니다.

- 예금자로부터 예금 형태로 돈을 구매하고 필요한 사람들에게 대출을 통해 후속 판매합니다.
- 다른 비즈니스와 동일합니다.
  - 대출한 돈의 이자율은 예금자에게 지불하는 이자율보다 높습니다.
  - 핵심은 그 돈이 예금자의 소유가 아닌 채무자에게 판매할 수 있는 가능성에 있습니다.
- 정부는 통화 발행을 통제합니다. 그들은 골치 아픈 통화 사이클을 수정하려고 합니다.
- 경제 침체에 더 많은 돈을 인쇄합니다.
  - 단기적인 성장을 촉진합니다.
  - 단기적으로 실업을 줄입니다.
- 물리적 지폐의 필요성이 사라졌습니다.
  - 인터넷 뱅킹은 신용화폐 사용을 촉진했습니다.

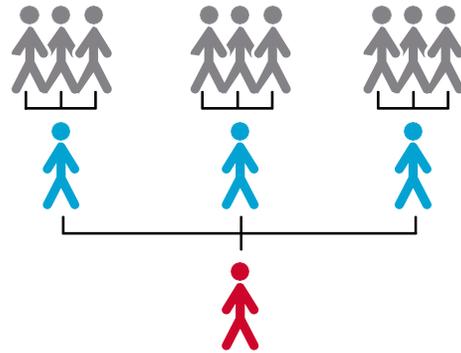
## 혜택

- 즉각적인 거래와 미래 계획을 용이하게 합니다.
- 은행은 중앙 데이터베이스에 저축자와 채무자의 모든 거래를 기록합니다.
- 은행은 지속적으로 사용자의 입금과 출금내역을 모니터링합니다.
- 은행은 계좌를 합법적으로 동결할 수 있습니다.

- 은행은 여러 가지 이유로 계좌에서 돈이 누락된 경우 복구할 수 있습니다.
- 은행은 강도를 대비한 보험에 가입되어 있습니다.

## 가격

- 은행 시스템은 단일 실패 지점을 가지고 있으며 중앙 집중 식이며 쉽게 조작할 수 있습니다.



- 정부(중앙은행)는 다음을 수행할 수 있습니다.
  - 화폐 공급을 자유롭게 확장 및 축소합니다.
  - 은행 계좌를 압류합니다.
  - 예고 없이 출금을 차단합니다.
  - 심각한 기술적 문제 또는 해킹 당한 경우 기본 서비스를 중단합니다.
  - 이자율과 세금을 조율합니다.
- 높은 인플레이션과 마이너스 금리는 화폐 가치를 떨어뜨립니다.

“은행은 날씨가 좋을 때 우산을 빌려주고 비가 내리기 시작하면 달라고 하는 곳이에요.”

-로버트 리 프루스트

## 1.3 돈의 정의

상품 또는 서비스 대가로 현금, 수표 및 신용 카드로 지불할 수 있습니다.

- 우리는 이 모든 교환 수단이 단지 지불 약속일 뿐이라고 생각합니다.

돈이 무엇인지 생각해 본 적이 있나요?

이 영상에서 우리의 돈에 대한 착각을 알 수 있습니다.

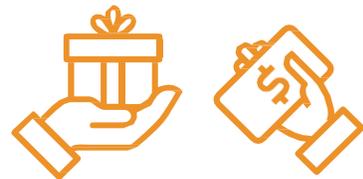
— SATOSHI



- **가치 척도.** 그것은 상품과 서비스의 가치를 표현하는 가격 체계의 보편적인 패턴을 허용합니다.

**복습 하기.** 화폐의 올바른 기능의 이름을 쓰세요.

\_\_\_\_\_. 돈은 모든 사람이 지불을 받아들이기 때문에 교환을 용이하게 합니다.



\_\_\_\_\_. 돈은 우리가 저축하고 미래에 쓸 수 있게 해주기 때문에 부를 유지하는데 도움이 됩니다.

### 돈의 기능

돈에는 3가지 기능이 있습니다.

1. 투자, 저축 또는 대출할 수 있는 가치 저장소.
2. 상품과 서비스에 대한 대가를 지불하기 위한 교환 매개체.
3. 제품 간의 가격을 비교할 수 있는 측정 단위.

- **가치 저장.** 시간이 지나도 그 가치를 유지하는 경향이 있습니다.

- **교환 매개체.** 복잡한 물물교환 시스템을 제거하여 보다 효율적으로 상품을 교환하고 부채를 상환할 수 있습니다.



\_\_\_\_\_. 화폐는 재화와 서비스의 가치를 측정하고 서로 다른 재화를 비교하는 것을 가능하게 합니다. 값비싼 가격표는 그 재화의 가치에 대해 우리에게 무엇인가 말해줍니다.

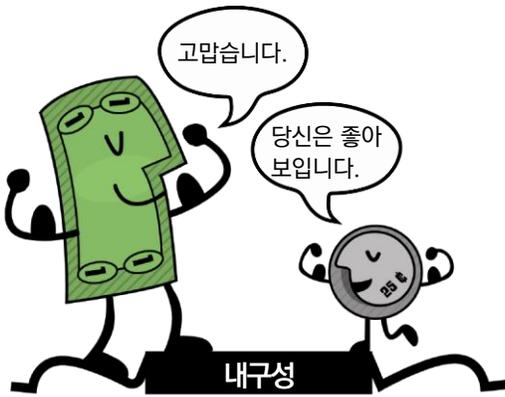


# 소개: 화폐 시스템

## 돈의 특성

돈은 다양한 형태를 취할 수 있습니다. 이러한 특성을 많이 나타낼수록 더 좋은 화폐입니다.

- **내구성.** 돈은 물리적인 소멸에 강해야 하고 시간이 지나도 지속되어야 합니다. 경제에서 수용 가능하고 인식 가능한 상태로 순환할 수 있어야 합니다.



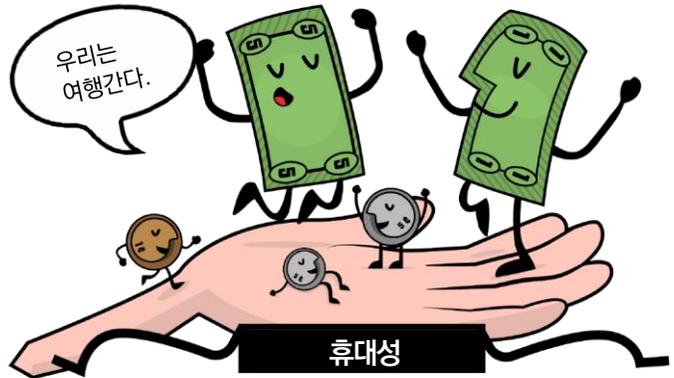
내구성

- **균일성 또는 대체 가능성.** 각 화폐 단위는 정확히 같아야 합니다.



균일성

- **휴대성.** 화폐를 쉽게 이동할 수 있어야 합니다. 작은 무게에 많은 가치를 담을 수 있어야 합니다.



휴대성

- **인식 가능성 또는 수용 가능성.** 사용된 재화는 모두가 화폐로 인식해야 합니다.



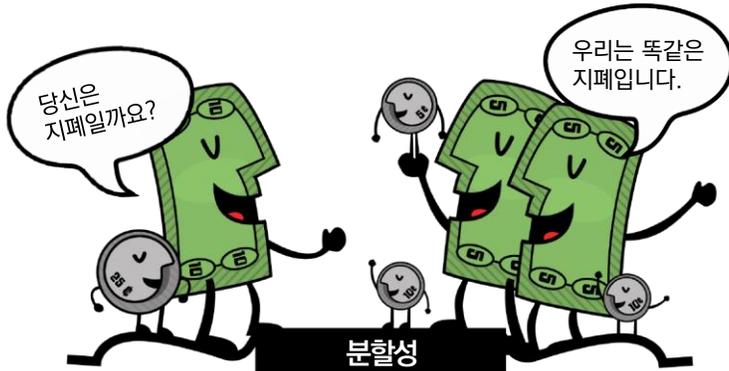
인식 가능성

- **희소성.** 화폐의 가치는 수요와 공급에 달려 있습니다. 더 많은 화폐가 발행되거나 덜 필요할수록 그 가치는 낮아질 것입니다.



희소성

- **분할성.** 물건을 구입하고 거스름돈을 돌려 받을 때 가치를 잃지 않고 똑같은 화폐로 받아서 사용 가능해야 합니다.



## 기존 화폐 및 화폐 자산

- **기존 화폐**는 특정 국가에서 일반적으로 사용되는 화폐입니다.
  - 유통 통화, 은행 예금 및 중앙 은행 준비금이 포함됩니다.
  - 대부분은 회계 장부의 대변 또는 전자 항목입니다.
  - 시간이 지나도 반드시 그 가치를 유지하는 것은 아닙니다.
- **화폐 자산**은 일반적으로 시간이 지남에 따라 가치를 유지합니다.

## 돈의 본질

### □ 상품성

- 추출이 어렵고 희소합니다.
- 가치를 보존하는 대상입니다.
- 금과 은은 수천 년 동안 좋은 돈으로 여겨졌습니다.
- [금전적 자산]

### □ 대표성

- 금 또는 은으로 된 지폐.
- 각 지폐는 동등한 가치의 금속으로 교환됩니다.
- 금본위제는 1971년까지 지속되었습니다.
- [화폐 자산이 화폐 공급이 증가하면서 일반 화폐가 되었습니다.]

### □ 법정화폐 또는 수탁화폐

- 정부 독점적이며 중앙은행에서 발행합니다.
- 물리적인 자산으로 보증하지 않습니다.
- 내재가치가 없으며 다음에 따라 달라집니다.
  - 수요와 공급의 관계.
  - 화폐를 발행하는 정부의 안정성.
- [디지털 화폐는 물리적인 화폐보다 더 많은 거래상대방 위험이 존재합니다]

### □ 비트코인

- 희소한 디지털 화폐입니다.
- 분산 방식으로 운영됩니다.
- 거래를 수행하기 위해 소프트웨어 및 암호학을 기반으로 합니다.
- [금전적 자산]



# 소개: 화폐 시스템

**수업 활동.** 물품이 표시된 특성을 충족하는 경우 X로 표시해보세요.

돈으로 어떤 항목을 선택 하시겠습니까?

\* 클래스 #4가 완료될 때까지 마지막 '비트코인' 열을 채우지 마세요.

특징	 사과	 조개	 1온스 골드	 1 달러	 비트코인
균일성 또는 대체가능성					
분할성					
휴대성					
희소성					
내구성					
인식성					

돈으로 어떤 항목을 선택 하시겠습니까?

---



---



---



---



---



---



---



---



---



---





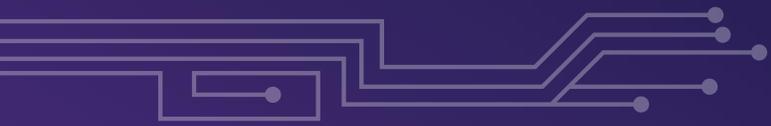


## 제 2장

# 돈의 역사, 진화 및 평가 절하

- 2.1 돈의 역사
  - 2.2 수업 활동: 물물교환 게임
  - 2.3 시간에 따른 화폐의 진화
    - 역사 속의 국제통화기준
  - 2.4 Fiat로의 갑작스러운 전환
  - 2.5 중앙 은행
  - 2.6 수업 활동: 부분 준비금
- 





3. 상품화폐란 무엇일까요?

---

---

---

---

---

---

---

---

4. 상품화폐를 사용할 때 어떤 문제가 발생할까요?

---

---

---

---

---

---

---

---

5. 돈이란 무엇일까요?

---

---

---

---

---

---

---

---

6. 사람들이 기꺼이 돈을 받는 이유는 무엇일까요?

---

---

---

---

---

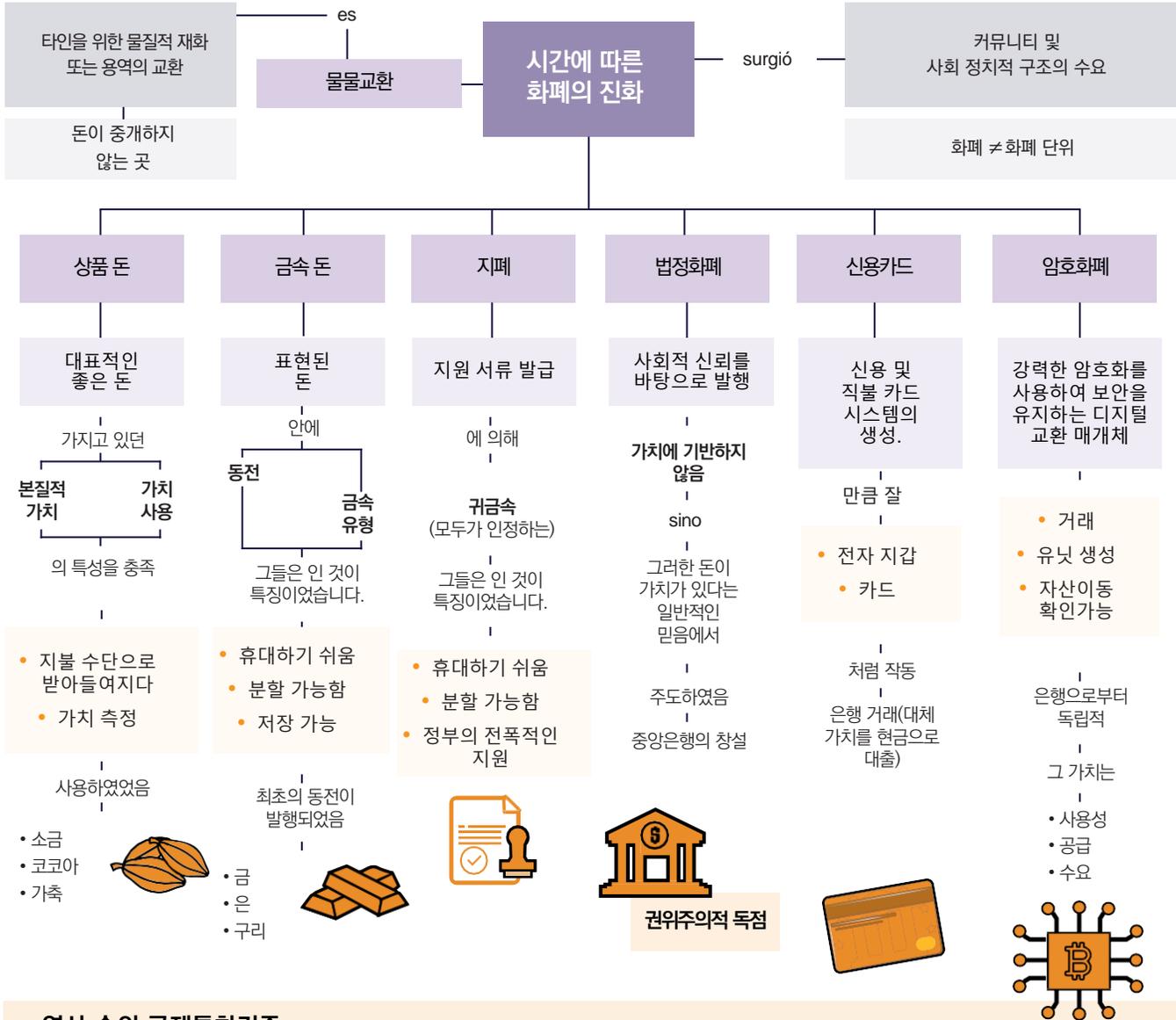
---

---

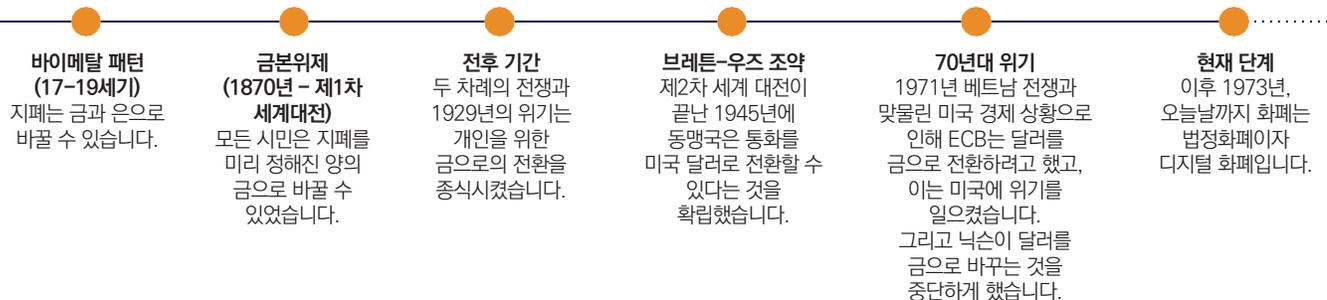
---

# 화폐의 역사, 진화 및 평가절하

## 2.3 시간에 따른 화폐의 진화



### 역사 속의 국제통화기준





- 화폐는 시대가 변화함에 따라 역사적으로 진화해 왔습니다.
  - 일반적으로 우수한 특성을 제공하는 화폐의 형태가 채택되었습니다.
  - 그러나 구매력이 절하되고 귀금속에서 종이 금속으로 전환되기 시작한 이후:
    - 최고의 성능을 가진 화폐의 형태를 자연스럽게 선택하는 방식에서 사용의 용이성, 뛰어난 휴대성 및 분할성으로 전환했습니다.
  - 중앙 집중화로의 전환이 있었습니다.

## 2.4 Fiat로의 갑작스러운 전환

산업화 시대는 중앙 집중화의 시작을 알렸습니다.

- 목적은 생산된 상품을 올바르게 분배하는 것이었습니다.
  - 중앙 은행이 만들어졌습니다.
  - 신용 및 직불 카드 시스템의 탄생하였습니다.

- 돈이 중앙 집중화되면 심각한 문제가 발생할 수 있습니다.
  - 정부는 시민들의 경제 활동을 모두 모니터링합니다.
  - 권력 남용은 다음과 같은 결과를 초래할 수 있습니다.
    - 경제적 보상 및 정부 개입.
    - 부채 폭발과 무책임한 소비.
    - 부의 불평등 증가.

1971년까지 대표화폐는 교환의 매개체이자 가치의 저장의 수단으로 사용되었습니다.

- 1971년부터 우리는 건전한 돈에서 벗어나 부채에 기반한 세상으로 옮겨왔습니다.
  - 리처드 닉슨(당시 미합중국 대통령)은 금본위제를 포기했습니다.
  - 현재의 실험인 **법정화폐**로 넘어옵니다.
  - 현대의 화폐는 합의에 의한 것이 아니라 법령에 의한 것입니다.
  - Fiat는 라틴어에서 유래했으며 법령에 의한 의미입니다: 법에 의해 선택되고 설정됩니다.

"어제 효과가 있었던 것이 오늘 반드시 효과가 있는 것은 아닙니다."

-조던 피터슨



# 화폐의 역사, 진화 및 평가절하

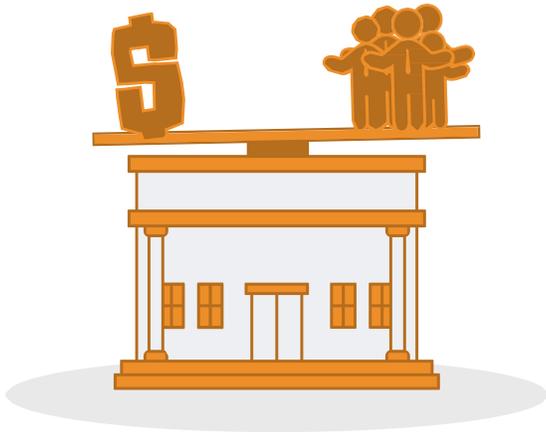
## 2.5 중앙은행

- 중앙은행의 목적과 기능:
  - 안정을 보장하기 위해 국가의 통화 정책을 통제합니다.
  - 주 기능은 은행을 위한 은행이 되는 것입니다.
  - 주요 업무: 유통 중인 화폐 공급을 조작합니다.
    - 경제 및 금융 정책을 통한 인플레이션 통제 및 고용 극대화.
  - 미국 중앙은행을 연방 준비 은행이라고 합니다.

연준은 다음과 같은 이중 권한을 부여 받았습니다:

물가안정

최대고용



- 누가 이러한 목표를 정의하고 누가 이익을 챙길까요?
  - 대형 은행 - 연방준비은행 및 글로벌 정책에 영향을 미칠 수 있습니다.

- 연방준비은행은 통화 공급을 어떻게 변경할까요?
  - 은행 시스템을 통한 **부분 지급준비금**.
  - 미국 내 은행들은 예금액의 10%만 준비금으로 보관합니다.
  - **부분 준비금은 은행이 갖고 있는 돈보다 많이 발행** 할 수 있습니다.
    - 한 국가의 경제에서 두 명 이상의 사람들이 동시에 같은 돈을 사용합니다.

은행은 은행에 있는 모든 예금의 일정 비율을 유지해야 합니다. 그 비율을 줄이면 더 많은 돈이 유통될 수 있고, 이 비율을 높이면 더 적은 돈이 유통될 수 있습니다.

- **부분 준비 은행**은 어떤 문제를 일으킬 수 있을까요?
  - 은행은 “예금자의 돈보다 많은 돈을 빌려준다”.
    - 예금 인출이 현금 준비금을 초과합니다.
    - 은행은 막대한 손실을 입습니다.
    - 최악의 경우 **뱅크런**이 발생합니다.
  - **이자율 또는 자본 비용의 변화가 위험에 영향을 미칩니다.**
    - 유통되는 돈이 많다는 것은 대출이 더 저렴하고 덜 필요하게 된다는 것을 의미합니다.
- **공개 시장 운영**(유통 화폐를 늘리거나 줄이기 위해).
  - 정부는 **화폐 증권(고 유동성 부채)**을 거래합니다.
    - 화폐량을 늘리고 싶으면 국고채를 삽니다.
    - 화폐량을 줄이려면 국고채를 팝니다.





## 제 3장

# 법정화폐와 중앙 집중화의 효과

3.1 수업 활동: 경매!

3.2 인플레이션

- 우리는 왜 인플레이션을 신경 써야 할까요?
- 현대 경제학자들은 우리에게 무엇을 얘기할까요?
- 인플레이션의 원인
- 시간 경과에 따른 인플레이션

3.3 검열

3.4 제한

3.5 중앙화 vs. 탈중앙화

3.6 결론

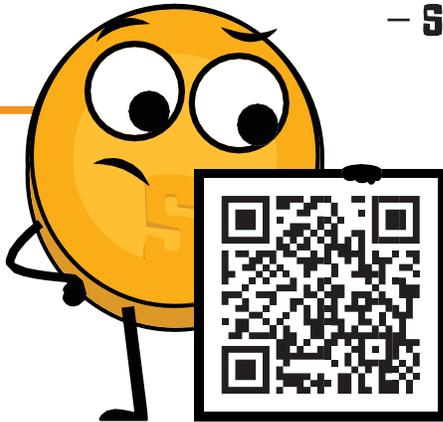


## 3.2 인플레이션

인플레이션이 무엇인지에 대한 다음 영상을 분석합니다.

집중!

— SATOSHI



- 원래 인플레이션이라는 용어는 다음을 나타내는 데 사용되었습니다.
  - 통화 가치의 손실,
  - 공급 증가로 인한 구매력 평가절하.
- 이러한 가치 손실은 일반적으로 다음을 유발합니다.
  - 모든 상품 및 서비스 가격의 지속적인 인상.
- 또한 ‘인플레이션’이라는 용어는 물가 상승을 나타내는 데 사용되었습니다.
  - 어떠한 원인에도 관계없음.

### 우리는 왜 인플레이션에 신경을 써야 할까요?

- 더 많은 돈이 같은 수량의 재화를 쫓을 때:
  - 가격이 상승합니다.
- 제품 가격이 임금 및 급여보다 빠르게 상승하는 경우:
  - 사람들은 가난해집니다.

### 1970년의 맥도날드 가격

	1/4 POUNDER w/cheese	.70	
	1/4 POUNDER	.60	
	BIG MAC	.65	
FILET-O- FISH	.48	LARGE Order Fries	.46
CHEESEBURGER	.33	FRENCH FRIES	.26
HAMBURGER	.28	HOT APPLE PIE	.28
MILK	.20	COFFEE (W/OUT SUGAR TAI 0%)	.15
	HOT CHOCOLATE	.15	
SHAKES CHOCOLATE STRAWBERRY VANILLA	COFFEE	.35	
COCA COLA - ROOTBEER - ORANGEADE	15 &	.20	
TRIPPLE RIPPLE ICE CREAM CONE		.20	

### 2020년의 맥도날드 가격

## McMENÚ DEL DÍA

LUNES	MARTES	MIÉRCOLES
<b>QUESOBURGUESA DOBLE</b> 	<b>POLLO FRITO McCRISPY™</b> 	<b>CUARTO DE LIBRA CON QUESO</b> 
<b>JUEVES SANDWICH McPOLLO™</b> 	<b>VIERNES McNÍFICA™</b> 	<div style="border: 2px solid red; border-radius: 50%; padding: 10px; text-align: center;"> <span style="font-size: 2em; font-weight: bold;">\$3.75</span>  <span style="font-size: 1.5em; font-weight: bold;">C/U</span>  <small>Desde las 11:00 a.m. en adelante. No aplica en servicio a domicilio.</small> </div>

### 현대 경제학자들은 우리에게 어떻게 얘기할까요?

- 국가를 효과적으로 운영하려면 인플레이션을 일으켜야 합니다.
- 지출 및 투자를 장려하지 않는 경우(통화 평가절하를 통해):
  - 수요 감소의 위험이 있습니다.
  - 생산량 감소를 유발합니다.
  - 최악의 경우 경기 침체로 이어집니다.
  - 이 모든 것은 저장하는 것이 어렵거나 불가능하거나 권장되지 않음을 의미합니다.

# 법정화폐와 중앙 집중화의 효과

- 현재 상황은 우리에게 지출을 장려합니다. 자기 파괴적인 이론입니다.
  - 우리는 며칠, 몇 주 또는 몇 달이 지난 미래를 생각하지 않습니다.
  - 우리는 자손의 미래를 준비할 수 있어야 합니다.
  - 인플레이션은 단순히 재정적 규율을 허용하지 않습니다.
- 우리의 결정에는 결과가 따라옵니다.
  - 이것을 '기회 비용'이라고 합니다.



공부하기.

- 좋은 직업을 얻을 수 있는 옵션.
- 미래를 위한 준비.
- 학위 취득을 위한 방법.

일하기.

- 급여를 받다.
- 직장생활 경험.
- 사회적 명성.

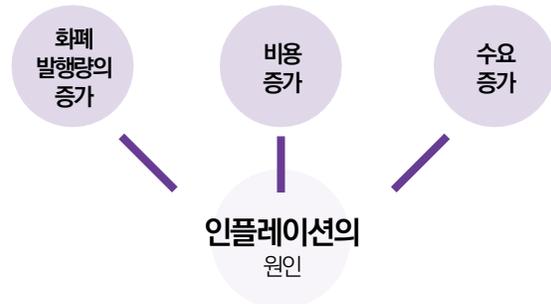


- 미래에 얻을 수 있는 것보다 지금 얻을 수 있는 것을 선호할 때 시간 선호도가 높다고 합니다.
- 미래에 더 나은 것을 얻기 위해 현재 얻을 수 있는 것을 포기하는 것을 선호하는 사람은 시간 선호도가 낮습니다.

- 인플레이션은 높은 시간 선호도를 부추기며, 이는 우리가 2년 후의 200달러보다 오늘 100달러를 선호한다는 것을 의미합니다.
- 우리의 목표는 낮은 시간 선호도를 만드는 것이어야 합니다.

높은 시간 선호	낮은 시간 선호
돈을 쓰기	돈 절약
패스트푸드	집에서 만든 음식
페이스북	책 읽기
TV시청	운동하기
콘텐츠 소비	콘텐츠 제작

## 인플레이션의 원인



다음 영상에서 인플레이션이 발생하는 세 가지 이유를 보여줍니다.



## □ 1. 비용 또는 공급 인플레이션

- 다음과 같은 이유로 가격이 상승합니다.
  - 정부 규정, 전쟁, 가뭄, 공급망 문제 등.
  - 세울의 인상은 원자재 비용을 증가시킵니다.
  - 전문 직업군의 임금은 더 올라갑니다.
    - 사회에서 기술이나 자원의 부족이 원인입니다.
  - 새로운 기술은 매우 비쌉니다.
    - 시간이 지남에 따라 상품 비용이 감소합니다.

## □ 2. 수요 인플레이션

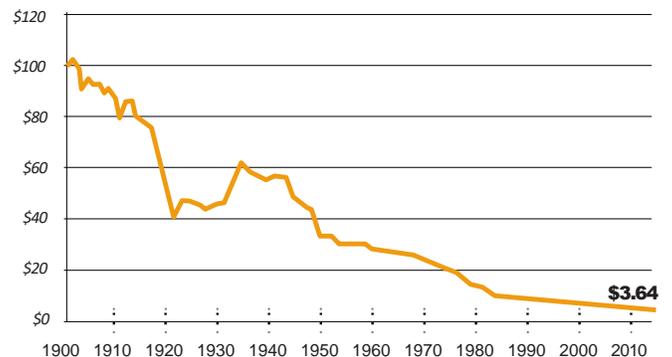
- 재화의 공급이 수요를 충족시키기에 충분하지 않습니다.
- 세금 감소(또는 대출 금리 인하)로 인해 가처분 소득이 증가합니다.
  - 넘치는 자금이 시장에 유통되기 시작합니다.
  - 더 많은 돈으로 같은 상품을 얻기 위한 경쟁이 발생합니다.
    - 이것은 상품 가격을 상승시킵니다.
- 결국 공급이 증가하고 가격은 다시 하락합니다.

## □ 3. 정부 정책에 의한 인플레이션

- 정부는 채권 발행으로 적자 자금을 조달합니다.
- 인플레이션을 통해 창출된 일자리/프로젝트는 진짜일까요?
- 사람들이 돈으로 물건을 사는 것이 정부에게 왜 중요할까요?
- 경제에 좋을 때 우리는 어떤 유형의 상품을 구매할까요? 생활 필수품인가요?
- 하나의 경제 단위에서 세율이 임금 상승률보다 빠르게 상승하면 어떻게 될까요?

- 인플레이션이란 당신이 얼마 전에 한 일이 오늘보다 가치가 떨어진다는 것을 의미합니다.
  - 당신이 지난해 10달러를 받았습니다. 1달러에 10개의 도시락을 살 수 있었습니다.
  - 당신은 그것들을 유지하기로 결정했습니다.
    - 그리고 오늘날 경제에는 더 많은 돈이 순환하고 있습니다.
    - 도시락을 사려는 사람들이 더 많아졌습니다.
    - 하지만 여전히 같은 수의 도시락을 판매합니다.
    - 점심 가격은 2달러가 되었습니다.
  - 시간이 지나 저축한 10달러로 도시락 5개만 살 수 있게 되었습니다.
  - 이론상 이것은 말이 되지 않습니다. 8시간 일하면 10년이 지나도 그 현실은 변하지 않습니다. 그 에너지가 당신과 함께할 수 있어야 합니다.
  - 인플레이션은 일종의 가치 절도라고 말할 수 있습니다.

- 다음 그래프는 달러(USD) 가치의 손실을 보여줍니다.



# 법정화폐와 중앙 집중화의 효과

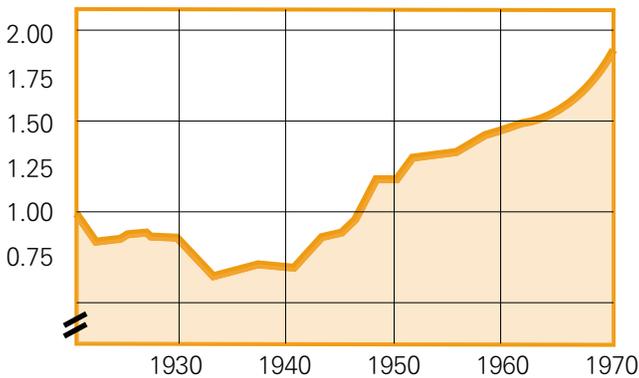
## 시간경과에 따른 인플레이션

- 1970년에서 2020년 사이의 인플레이션은 이전 50년 기간인 1920년에서 1970년보다 훨씬 높았습니다.
  - 우리가 같은 추세를 이어 간다면 어떻게 될까요?
  - 조부모 세대와 부모 세대 중 누가 더 큰 경제적 손실을 보았을까요?



다른 기간에 대해서 보려면 다음 영상을 참고하세요

1920년~ 1970년의 \$1

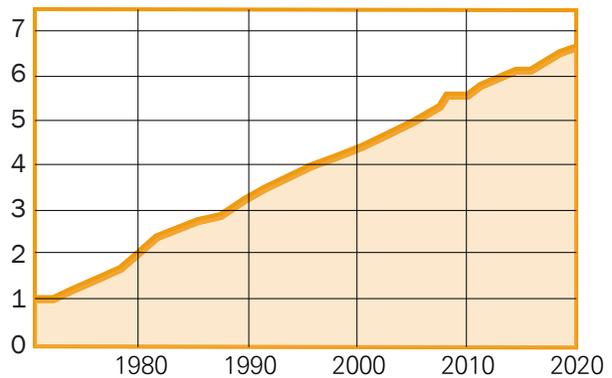


결과: \$1.94

평균 인플레이션율: 연간 1.33%

총 인플레이션 계수 증가율: 93.72%

1970년~ 2020년의 \$1

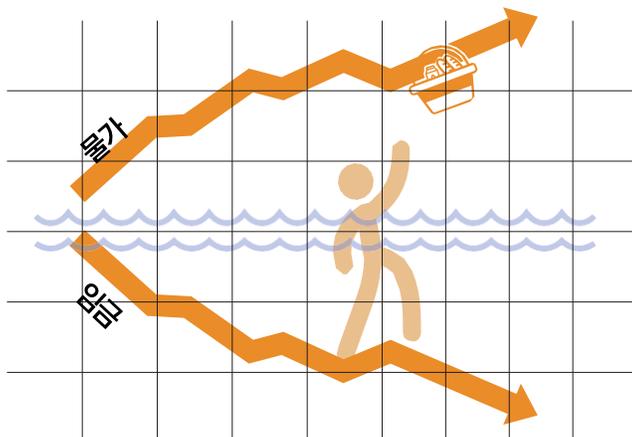


결과: \$6.67

평균 인플레이션율: 연간 3.87%

총 인플레이션 계수 증가율: 566.60%

- 물가와 함께 임금이 올랐을까요?

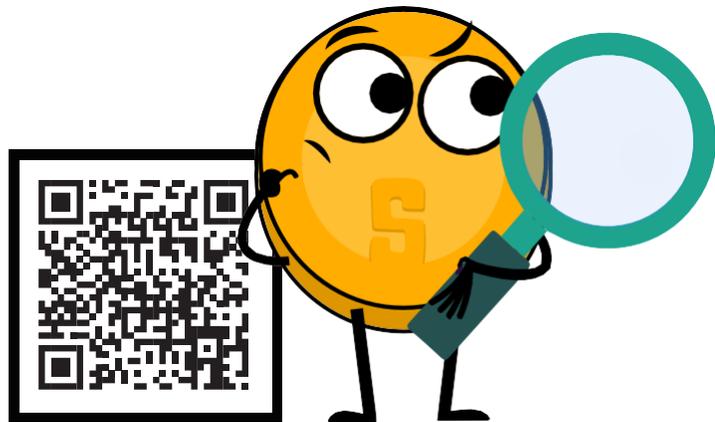


- 다른 관점에서 보면 2022년에 100달러로 구매할 수 있는 것을 1920년에는 약 7달러로 구매할 수 있었습니다.

- 인플레이션은 구매력 손실을 초래합니다.
  - 임금 인상 폭이 식품 가격 인상 폭보다 작습니다.
  - 개인은 소비를 줄여야만 합니다.
  - 구매력이 떨어집니다.

<p><b>인플레이션 수혜자</b></p>	<p><b>인플레이션 피해자</b></p>
<p><b>국가</b></p> <p>높은 물가와 월급으로 인해 세금으로 인한 수입은 증가하지만 비용은 훨씬 적게 증가합니다.</p>	<p><b>예금자</b></p> <p>저축의 가치가 점점 낮아집니다.</p>
<p><b>채무자</b></p> <p>인플레이션으로 인해 부채가 고정된 상태에서 돈을 상환하는 것이 더 쉬울 것입니다.</p>	<p><b>채권자</b></p> <p>채무자가 돈을 상환할 때는 구매력이 더 떨어져 있을 것입니다</p> <p><b>연금 수급자와 근로자</b></p> <p>연금과 임금이 물가보다 덜 오릅니다.</p>

- 결과는 다음과 같습니다.
  - 디지털 사기, 온라인 괴롭힘, 갈취, 신분 도용 및 사용자의 개인 정보와 보안을 위협하는 기타 문제가 발생합니다.
  - 우리의 카드 구매내역은 기록, 분석 및 모니터링됩니다.
    - 현금으로 상품과 서비스를 구매하지 않는 한 모니터링 됩니다.
  - 누군가 당신의 인터넷 뱅킹 비밀번호를 알아내거나 중앙 집중식 서버를 해킹하면 모든 정보에 접근할 수 있습니다.



우리는 개인 정보를 보호하고 모든 개인 정보를 정부 및 민간 기업과 공유하지 않는 돈이 필요합니다.

### 3.3 검열

- 정부는 돈을 세탁하거나 다른 유형의 불법 거래를 하는 사람들을 검열 합니다.
  - 감시는 양날의 검입니다.
  - 사기가 더 많이 발생할수록 국가 및 민간 기업의 더 많은 감시가 이루어집니다.
    - 그들은 기술 발전을 이용해서 우리의 사생활을 침해합니다.
    - 그들은 사회적, 경제적 네트워크에서 우리의 움직임을 통제합니다.
    - 특정 서비스를 즐기는 대가로 개인정보 데이터를 요구합니다.

### 3.4 제한

- 국가간 자금이동이 어렵고 비용이 많이 든다는 점입니다.
- 정부는 일반인 사이의 환전도 통제합니다.

다음은 이러한 상황이 발생할 수 있는 정책 및 방법들입니다:

# 법정화폐와 중앙 집중화의 효과

## 정부정책

- 자본 통제: 시민들이 해외로 송금, 변경 또는 가져갈 수 있는 금액이 제한됩니다.

### • 예시:

- 아르헨티나, 러시아, 인도네시아, 쿠바 및 중국.
- 중국 시민은 연간 최대 50,000달러 인민폐(약 8,000 달러)만 환전할 수 있습니다.

*“쿠바에서 우리가 찾은 유일한 해결책은 비트코인입니다. 지금 우리는 다른 어떤 나라와도 평등하게 경쟁할 가능성이 있습니다. 제재나 금지 없이 우리가 창조하고 성장하고 연결할 수 있는 기술에 완전히 무료로 접근할 수 있기 때문입니다.”*

### -에릭 가르시아 크루즈

(쿠바 기업가이자 비트코인 애호가)

## 은행 정책

- 계좌에서 인출할 수 있는 현금 금액에 제한이 있거나 이체할 수 있는 최대 금액이 존재합니다.

- 이러한 거래의 대부분에는 수수료가 있습니다.

### • 예시:

- 그리스는 2015년 위기 이후, 시민들은 하루에 60달러만 인출할 수 있었습니다.
- 이것은 누가 당신의 돈을 실제로 통제하는지에 대한 분명한 신호입니다.
  - 엘살바도르에서 송금은 국내총생산(GDP)의 23%를 차지합니다.
- 2020년에는 거의 60억 달러에 달합니다. 약 60%는 송금 회사에서, 38%는 은행 기관에서 발생합니다.
- Western Union과 같은 회사는 수수료가 높습니다.
- 특히 1,000달러 미만인 경우 수수료가 높습니다.

## 커미션 또는 수수료

- 이러한 수수료는 은행을 부유하게 할 뿐입니다.

- 또한 부자와 가난한 사람 사이의 격차를 증가시킵니다.

- 10달러와 같은 소액의 경우 수수료는 최대 3달러 또는 33%가 될 수 있습니다.
- 100달러의 경우 수수료 범위는 12%에서 15%입니다.

## 시간

- 돈 보내기/돈 받기

- 보내는 사람과 받는 사람 모두 가까운 지점으로 가야 합니다.
- 이것은 물론 영업 시간 동안이어야 합니다.

## 보안

- Western Union 사무소에 가는 것은 다음과 같은 추가 위험을 수반합니다.

- 사람들은 돈을 현금으로 가지고 다녀야 하므로 강도를 당할 가능성이 높아집니다.
- 중앙 집중식 서버에 장애가 발생하면(자주 발생) 모든 고객의 자금을 대한 접근이 거부될 수 있습니다.

## 3.5 중앙화 vs. 탈중앙화

- 현대 경제의 중앙 집중화는 다음을 생산합니다.
  - 검열, 권력 남용, 부패, 기회의 불평등, 부의 불평등, 단일 실패점 등.
- 은행은 중앙 집중식 서버를 통해 운영됩니다.
  - 그들은 사용자의 모든 금융 활동에 접근할 수 있습니다.

은행은 고객에 대해 무엇을 알고 있을까요?

- 당신이 얼마를 지불하는지.
- 당신이 무엇에 돈을 쓰는지.
- 당신이 누구에게 돈을 송금하는지.
- 계좌와 관련된 모든 것.

## 중앙 집중식 시스템의 특징

- 중앙 집중식 조직이 데이터를 안전하게 보호할 것이라고 믿어야만 합니다.
- 그들은 시스템과 데이터를 완벽하게 제어합니다.
- 주 서버가 손상되면 데이터가 위험에 노출됩니다.

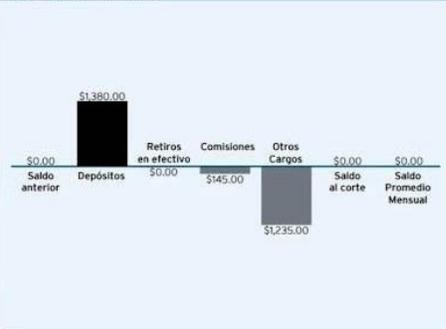
중앙 은행 디지털 통화는 현재 시스템의 연속이지만 디지털 형식입니다. 즉, 변경 가능, 검열 가능, 폐쇄형, 중앙 집중식, 배타적, 경계성입니다.

Carlos Pérez Pérez.  
Av. Independencia # 543 interior 2.  
Col central C.P 34004

## BANCO

Contrato: 25687451  
Sucursal 1  
Cuenta: 123321  
Clave Interbancaria: 00000123321  
Cliente: 963258  
RFC: PEPC920212R47

### Comportamiento

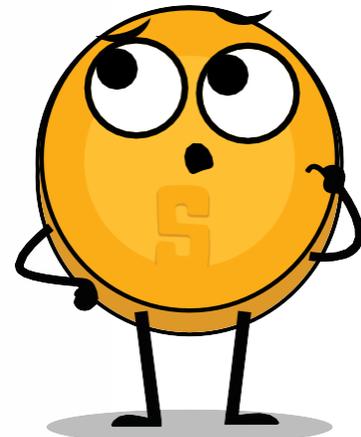


### Resumen En Pesos Moneda Nacional

Saldo anterior	0.00
Depósitos	1,380.00
Retiros en efectivo	0.00
Otros cargos	1,235.00
Saldo al corte	0.00
Saldo promedio mensual	0.00

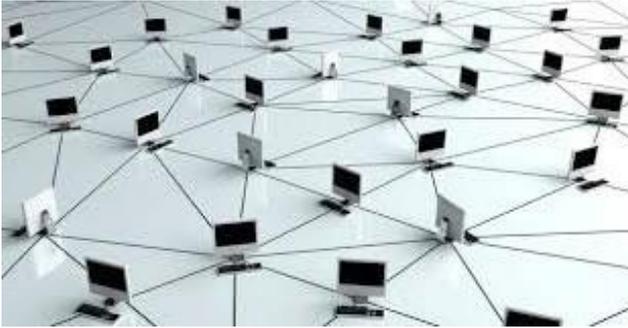
### Detalle de Operaciones En pesos Moneda Nacional

FECHA	CONCEPTO	RETIROS	DEPÓSITOS	SALDO
25 DIC	SALDO ANTERIOR			0.00
11 ENE	PAGO RECIBIDO DE BBVA BANCOMER POR ORDEN DE MAURICIO DEL MORAL DURAN REF.0000001 ARTICULOS RASTREO: BNET0100160110002067854		1,380.00	1,380.00
11 ENE	IVA POR COMISION MANEJO DE CUENTA	23.20		1,356.80
11 ENE	COMISION PENDIENTE MANEJO DE CUENTA 8110401166	145.00		1,211.80
11 ENE	COBRO DE 600501077330 MAS910614BR6 Domi Asistencia Familiar 10	89.00		1,122.80
11 ENE	RETIRO POR TRASPASO	1,122.80		0.00
22 ENE	COMISION MANEJO DE CUENTA PENDIENTE POR: 145.00 MAS I.V.A.			0.00



# 법정화폐와 중앙 집중화의 효과

잘못된 정부 정책으로 인해 발생하는 이러한 현상에 어떻게 대처해야 할까요?



## 탈중앙화 시스템의 특징

다음은 P2P 시스템의 특징입니다.

- 사람들은 인터넷을 통해 상호 작용하고 상호 연결하기 위해 자신을 식별할 필요가 없습니다.
- 모든 사람은 자신의 장치에 대한 권한이 있지만 리소스를 빌려주고 공유합니다.
- 네트워크 공격이 있는 경우 해커가 대부분의 컴퓨터를 제어해야 합니다. 이는 거의 불가능합니다.
- 한 서버에 오류가 발생하더라도 나머지는 영향을 받지 않습니다.
- 더 공정한 사회를 달성합니다 - 강력한 기업으로부터 통제권을 가져옵니다.

## 3.6 결론

다시 한 번 자문해 보겠습니다. 현재의 화폐 문제에 대한 해결책이 있을까요?

이것은

돈이었다



=



금과 은으로  
보증합니다

이것은

종이다



=



'정부의 선의와 신용'이  
보증합니다

이것은 미래다  
기술을 사용하여  
세계 시민의  
지원을 받습니다.

=









## 제 4장

# 비트코인

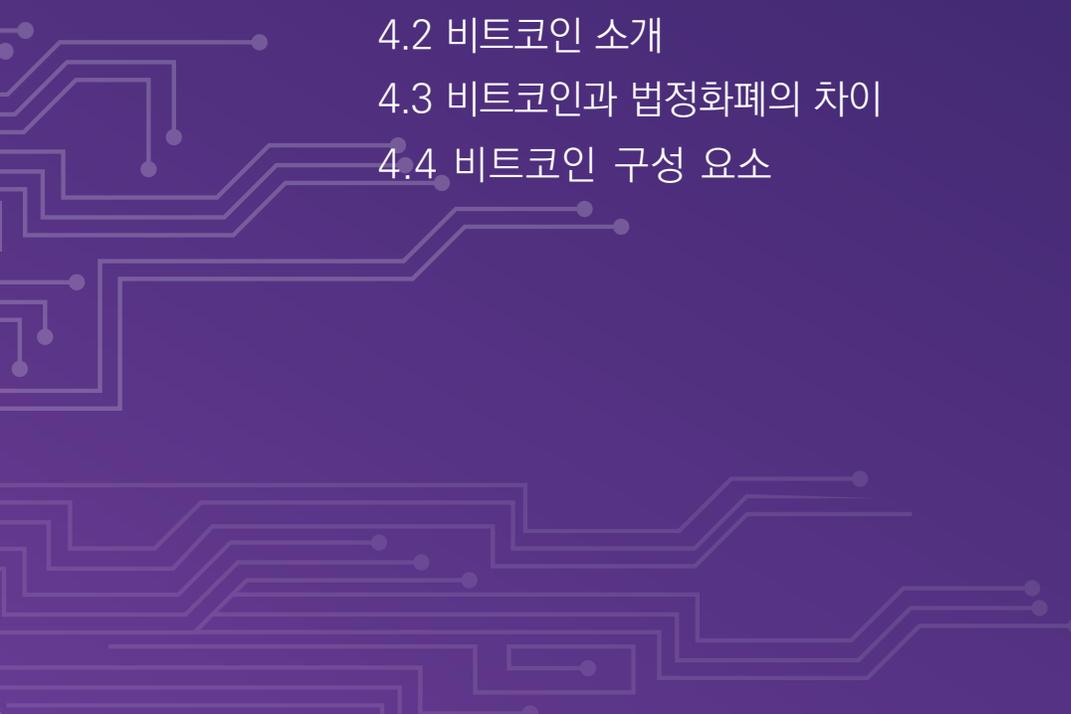
### 4.1 비트코인은 왜 만들어졌을까요?

- 해결해야 할 문제는 무엇일까요?
- 이러한 문제는 어떻게 해결되었을까요?
- 누가 문제를 해결했을까요?
- 사토시는 어떤 어려움을 겪었을까요?
- 비잔틴 장군 문제는 무엇일까요?
- 이것이 비트코인과 어떤 관련이 있을까요?

### 4.2 비트코인 소개

### 4.3 비트코인과 법정화폐의 차이

### 4.4 비트코인 구성 요소



## 4.1 비트코인은 왜 만들어졌을까요?

2001년 뉴욕의 쌍둥이 빌딩에 대한 공격은 세계 경제에 심각한 타격을 입혔습니다. 그 결과, 미국은 민생 경제 지원과 저소득층을 위한 모기지 대출 금리 완화라는 목표로 이전에 볼 수 없었던 수준으로 빠르게 금리를 낮추기 시작했습니다.

금리가 낮아지면서 소득, 자산 또는 직업이 없는 사람들에게도 신용혜택이 주어졌습니다. 위기의 여파는 오늘날에도 여전히 살아 있습니다. 해당 사건은 2008년 9월 15일 투자은행 리먼브러더스가 파산을 선언하면서 발생했습니다. 그 순간부터 미국은 경제 붕괴를 겪었고 나머지 국가들 또한 마찬가지로였습니다. 결과적으로 과도한 위험을 감수하고 규제가 미비한 은행에 대한 불신이 나날이 커지는 결과를 낳았습니다.



### 해결해야 하는 문제는 무엇일까요?

- 부족한 개인 주권
- 은행의 중앙 집중화.
- 인플레이션.
- 검열.
- 중개인의 부재.
- 접근성이 나쁜 은행 서비스.
- 높은 국제 송금 비용.
- 기타 등등

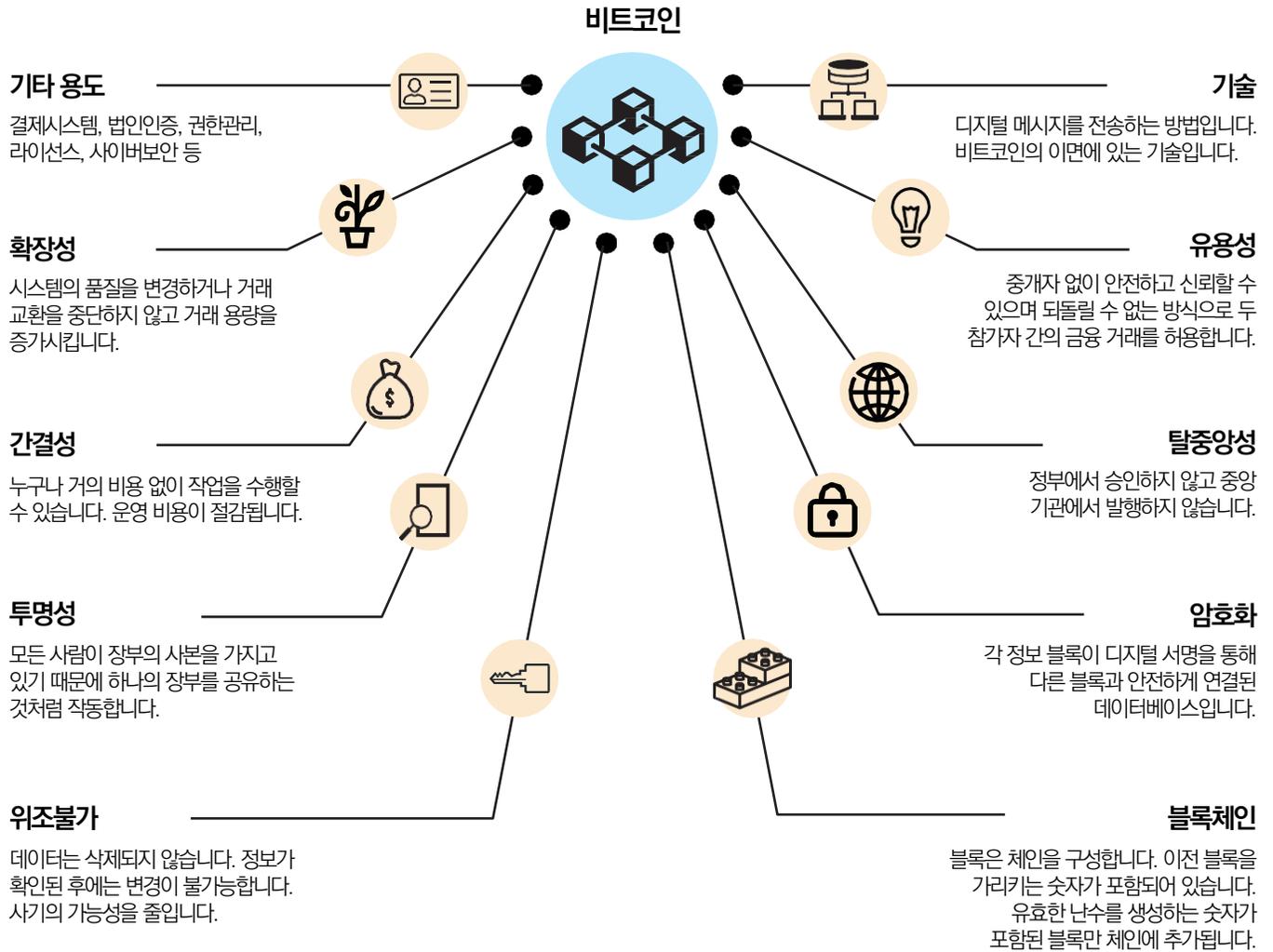
## 이러한 문제는 어떻게 해결되었을까요?

- 1991년에 개발된 기술을 사용하여 해결했습니다 (Blockchain).

Blockchain(또는 Chain of Blocks)은 유명한 디지털 통화인 **비트코인**을 이루는 기술입니다. 블록체인은 거래 장부 역할을 하는 공개 온라인 데이터베이스입니다. P2P 분산형 지불(Payment) 네트워크입니다. 암호화 키를 사용하고 여러 컴퓨터에 배포 및 공유되므로 사기 및 위조의 위험이 현저히 줄어듭니다.

## 누가 해결했을까요?

- 사토시 나카모토는 2008년 10월에 등장했으며 그의 정체는 여전히 수수께끼입니다.
- 그는 새로운 전자 화폐 시스템에 대한 아이디어를 제안했습니다. 이 돈을 **비트코인**이라고 합니다.
- 그는 다음과 같은 새로운 지불 방법을 설명하는 가이드 문서를 만드는 데 시간을 보냈습니다.
  - 가치를 저렴한 비용으로 신속하게 이전할 수 있는 방법입니다.
  - 정부나 금융 기관이 통제하거나 조작할 수 없게 하는 방법입니다.
- 이 사람 또는 특정 그룹(알려지지 않음) 덕분에 '이중 지불' 문제에 대한 해결책이 나왔습니다.
  - 이제 누군가가 다른 두 곳에서 동일한 화폐를 사용하는 것은 불가능합니다.
- 백서(White Paper)라고 하는 9페이지 문서입니다.



- 그는 그것을 사이퍼펑크(Cypherpunks)와 메일링 리스트에 공유했습니다.
  - 기술 토론이 있는 매우 활동적인 그룹입니다.
  - 그들은 수학, 암호학, 컴퓨터 과학, 정치 및 철학 토론, 심지어 개인적인 논쟁까지 다루었습니다.
- 사토시는 전통적인 화폐와 은행 시스템에 대해 냉소적이었습니다.
  - 제네시스 블록에서 그가 다음과 같은 메시지를 기록한 것을 볼 수 있습니다.

**여기에서 사토시나카모토의 백서를 다운로드할 수 있습니다.**

“2009년 1월 3일: 더 타임스, 은행들의 두 번째  
구제금융을 앞두고 있는 영국 재무장관”

-사토시 나카모토, 제네시스 블록

- 그는 “두 번째 은행 구제 금융 위기에 처한  
재무장관”이라는 제목의 타임즈 신문 기사를  
기록하였습니다.
  - 영국 재무장관은 은행 구제금융을 위해 수조  
영국 파운드화를 경제에 투입할지 여부를  
결정해야 했습니다.
- 다음은 **비트코인** 백서에 담겨있는 내용입니다.

1. 9페이지만 있습니다.



2. 중개자가 없는 ‘전자화폐’ 시스템을  
찾았습니다.



3. 책에는 블록체인이라는 단어가 나오지  
않습니다.



4. 디지털 통화를 일련의 서명으로  
정의합니다.



5. 채굴은 이해를 돕기 위한 용어  
입니다.



6. 더 빠른 거래가 아니라 더 안전한  
거래를 추구합니다.



7. 체인 크기의 증가는 4.2MB/년으로  
계산되었습니다.

- 최초의 비트코인 거래는 사토시와 할피니 엮습니다.

- 사토시의 마지막 ‘생명의 신호’는 소프트웨어 개발자  
개빈 안드레아센과 함께했습니다.

“...나는 개빈 안드레아센과 모든 사람들과 좋은 손을  
잡고 다른 일들로 넘어갑니다.”

- 공개 메시지와 나중에 게시된 비공개 메시지에서  
사토시는 개인적인 이야기를 한 적이 없습니다. 모두  
비트코인과 그 코드에 관한 것만 있었습니다.
- 많은 사람들이 본인이 사토시라고 주장하고  
있지만, 우리는 여전히 그가 누구인지 모릅니다.
- 사토시는 약 980,000 비트코인을 보유한 것으로  
추정됩니다.

## 사토시는 어떤 어려움을 겪었을까요?

- 같은 돈을 두 사람에게 동시에 보낼 수 있을까요?
- 누가 인터넷에서 상대방을 믿을 수 있을까요?
- 누군가의 계정(또는 지갑)에 제품을 구매할 만큼  
충분한 돈이 있는지 어떻게 알 수 있을까요?
- 탈중앙화 네트워크의 일부 노드가 비정상이라  
올바른 결정을 내릴 수 있도록 하려면 어떻게 해야  
할까요?
- 참가자가 윤리적으로 행동하고 그룹의 이익을 위해  
일할 것이라고 당연히 가정하지 않는 분산되고  
안정적인 시스템을 만들 수 있을까요?
- 돈을 보내는 사람입장에서 돈을 받고 싶어하는  
사람이 그 자신인지 어떻게 알 수 있을까요?

‘이중 지불 문제’ = ‘비잔틴 장군 문제’

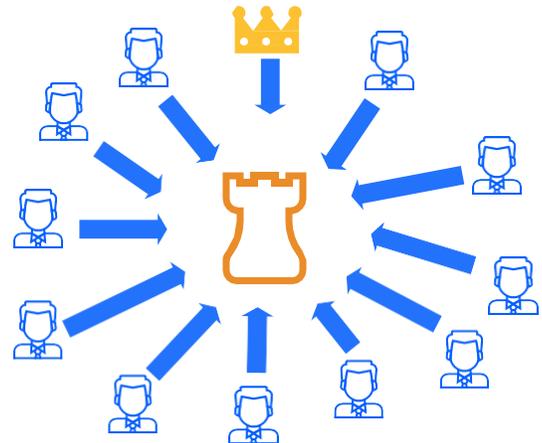
메시지를 보낸 사람이 반역자이고 군대를 배신할 계획이라면 어떻게 될까요? 장군 자신이 부패하여 다른 장군들 사이에 불화를 일으키려고 하면 어떻게 될까요?

### 비잔틴 장군의 문제는 무엇일까요?

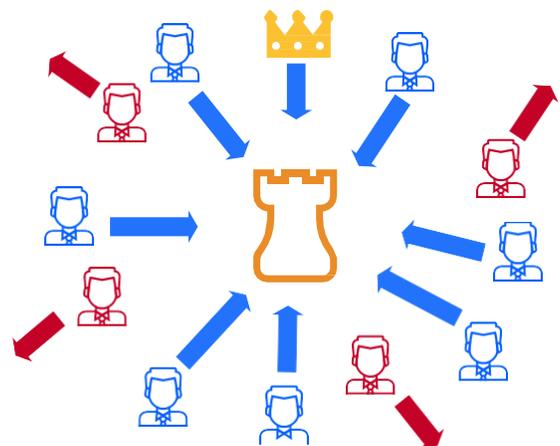
- 비잔틴 장군의 문제는 신뢰할 수 있는 중앙 통제자의 개입 없이 신뢰할 수 있는 정보를 전송하는 어려움을 은유적으로 설명합니다.

비잔틴 장군의 어원은 무엇일까요?

- 페르시아에는 매우 튼튼한 성이 있습니다.
- 비잔틴 장군들은 성을 포위하고 공격을 계획하고 있습니다.
- 군대가 너무 분산되어 있기 때문에 중앙 통제자가 없습니다.
- 장군들은 메신저를 통해 서로 통신합니다.
- 두 가지 가능한 명령은 ‘공격’과 ‘후퇴’입니다.
- 그들은 페르시아 군대를 공격하는 데 동의해야 하며 동시에 해야 합니다.
- 그들 중 하나가 동의하지 않으면 전투에서 패배합니다.
- 배신자가 있으면 충성파가 동의하지 않을 수 있습니다.
  - 예를 들어, 한 장군에게는 공격하고 다른 장군에게는 퇴각하라고 말할 수 있습니다.
- 어느 날 아침, 장군은 다음과 같은 메시지를 받습니다. “공격은 화요일에 일어날 것입니다.” 중앙 기관의 서명이 없습니다.



합동공격이 승리를 이룹니다



협력하지 않은 공격은 패배로 이어집니다.

군의 전략에 어긋나는 정보를 전달하려는 적의 속임수가 아닌 정상적인 명령임을 장군이 어떻게 확신할 수 있을까요?

이 문제에 대한 해결책은 원래 이메일 스팸을 방지하는 방법으로 사용되었습니다.

## 이것이 비트코인과 무슨 관련이 있을까요?

비잔틴 장군 문제는 다음을 설명합니다.

- 분산 시스템을 구성하는 구성원들이 하나의 진실에 동의하는 데 어려움이 있습니다.
- 믿을 수 있는 중개자 없이 송금하는 것과 같습니다.
  - 메시지가 수정되지 않았는지 확인하는 방법이 필요합니다. 이는 합의 메커니즘을 갖춘 **비트코인**이 등장할 때까지 달성되지 못했습니다.
- 이 과정에서 암호화의 사용은 필수인데, 암호란 무엇일까요?
  - 비밀 키로 암호화된 메시지를 생성하여 키를 가진 사람이 아니면 복호화 할 수 없도록 하는 기술입니다.
- 또한 **비트코인**은 작업 증명 메커니즘과 블록체인을 사용하여 '이중 지불' 문제를 해결합니다.
- **비트코인**은 다음을 달성합니다.
  - 1) 인터넷을 통해 다른 사용자에게 디지털 자산(또는 돈)을 전송합니다.
  - 2) 키 소유자만 전송할 수 있도록 합니다.
  - 3) 중간에 가로챌 수 없습니다.
  - 4) 누구나 송금을 확인할 수 있습니다.
  - 5) 그리고 모든 참가자가 그것을 인정합니다.
  - 6) 되돌리거나 지우는 것이 불가능합니다.
  - 7) 이 모든 것이 완전히 분산된 탈중앙화 방식으로 수행됩니다.

- 비트코인을 구성하는 주체는 노드입니다.
  - 노드는 공유 원장의 현재 상태를 결정하기 위해 합의에 도달해야 합니다.

## 4.2 비트코인 소개



### **비트코인**이란? **비트코인**이란?

- 여기 자세한 설명이 있습니다.
- **돈.** 전통적인 화폐의 세 가지 기능인 가치의 척도, 가치의 저장 및 교환의 매개체를 수행합니다.
- **소프트웨어.** 모든 컴퓨터에서 다운로드하여 실행할 수 있는 프로그램입니다.
- **네트워크(Network).** 장애 없이 작동하기 위해 합의를 통해 작동하는 프로그램과 컴퓨터의 집합입니다.



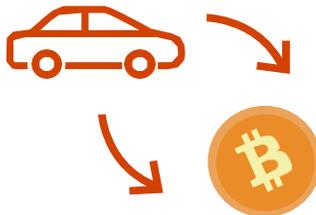
다른 화폐들과 마찬가지로 화폐입니다.

하지만 디지털입니다.



중앙 기관의 통제 없이.

재화 또는 용역으로 교환할 수 있습니다.



휴대가 간편하고 안전합니다.

수천 개의 매장에서 사용할 수 있으며 전 세계적으로 동일한 가치를 가지고 있습니다.

## 비트코인(Bitcoin)과 비트코인(bitcoin)의 차이점은 무엇일까요?

대문자 'B'가 붙은 **비트코인(Bitcoin)**은 동일한 프로그램으로 작동하는 컴퓨터 네트워크를 의미하며, 소문자 'b'가 붙은 **비트코인(bitcoin)**은 네트워크 내에서 관리되는 디지털 자산(\$)을 의미합니다. 즉, **비트코인(bitcoin)**은 암호학의 암호화된 가상 화폐 단위로 **비트코인(Bitcoin)** 네트워크 내에서 가치를 교환하는 데 사용됩니다.

### 주요기능은 무엇일까요?

- 중개자 없이, 경제적으로, 국제적 장벽 없이 개인 간 지불(P2P) 이체를 가능하게 하고 가치를 저장합니다.

### 어떤 기술적 발전을 이루었나요? 왜 은행 업무에 혁명을 가져올까요?

- 이중 지불을 방지합니다.
- 거래를 감독하는 중앙 기관이 필요하지 않습니다.

### 무엇이 그것을 가치 있게 만들까요?

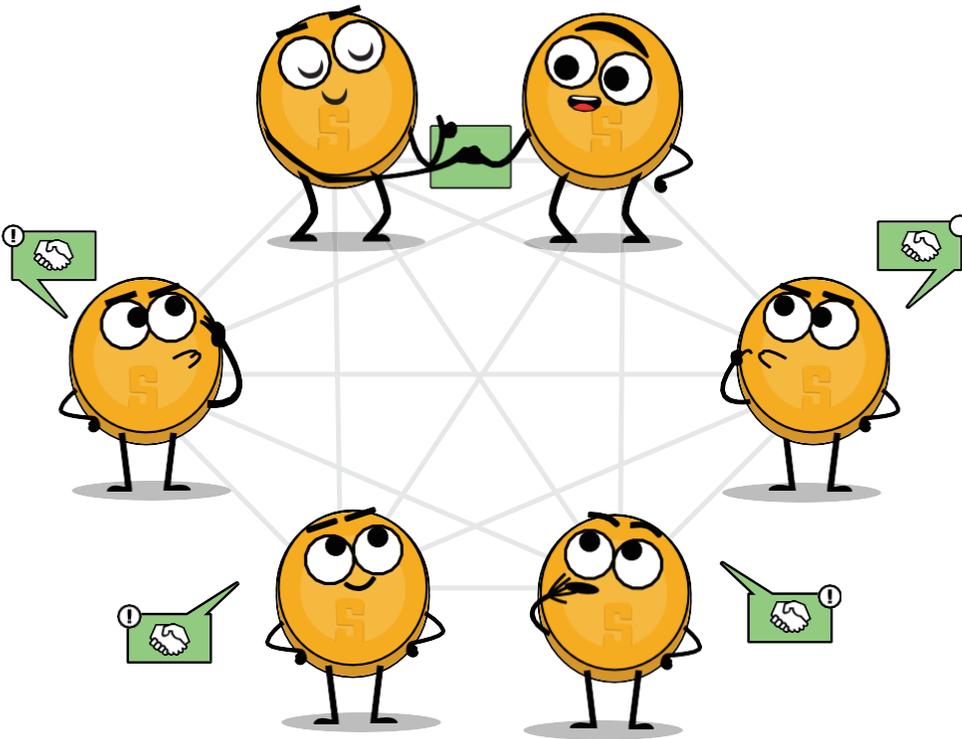


블록체인과 **비트코인**의 관계는 어떻게 될까요?

- 블록체인은 가장 중요한 **비트코인** 거래가 영구적으로 기록되는 공개 장부입니다.
- **비트코인**은 **비트코인** 통화로 이루어진 거래를 기록하는 유일한 블록체인입니다.

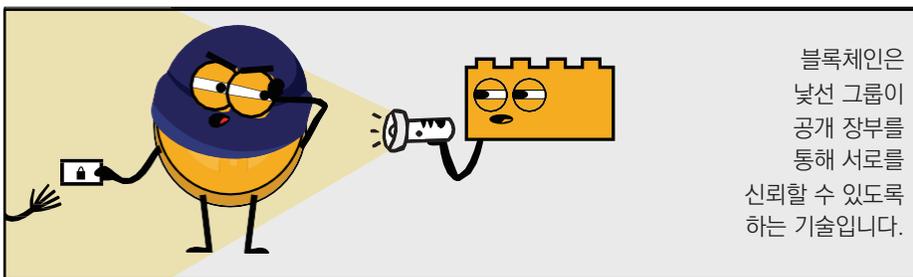
**비트코인**은 무엇으로 만들어졌나요?

- 지폐와 같이 물리적으로 만질 수 있는 것은 없습니다.
- 그들은 단지 디지털 숫자와 문자의 나열입니다.
- 고유한 ID(지문으로 ID를 제공하는 것처럼)입니다.



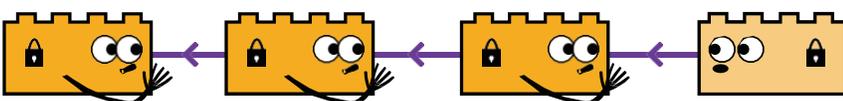
블록체인은 네트워크 구성원 간에 분산되어 있기 때문에 안전한 거래 기록입니다.

각 거래는 모든 사람에게 대해 영구적으로 기록되며 이러한 방식으로 어떤 거래도 숨길 수 없습니다.



블록체인은 낯선 그룹이 공개 장부를 통해 서로를 신뢰할 수 있도록 하는 기술입니다.

데이터는 암호화되어 순차적으로 연결된 블록(블록)에 저장되며, 전체 네트워크의 합의 없이는 정보를 수정하기 어렵습니다.



## 비트코인은 익명인가요?

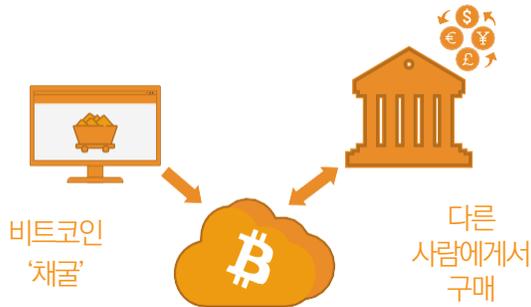
- 아니요, 가명입니다. 거래는 누구나 볼 수 있고 접근 가능하며 투명합니다.
- 사람들은 이름과 성이 아니라 일련의 문자와 숫자로 자신을 식별합니다.

## 누가 비트코인을 사용할 수 있을까요?

- 기존의 은행 시스템과 달리 인터넷에 접속할 수 있는 모든 사람입니다.

## 비트코인은 어떻게 얻을 수 있나요?

- 거래소를 통해 온라인으로 구매합니다.
- 새로운 비트코인은 채굴이라는 작업을 통해 생성됩니다.



## 비트코인의 어떻게 접근할까요?

- 비트코인으로 거래하려면 인터넷 접속이 필요합니다.
- 일부 국가에서는 입금을 금지하지만 교환을 금지하는 것은 불가능합니다.

## 비트코인은 어디에 저장되나요?

- 비트코인은 블록체인에 기록되어 있으며 개인 키로 제어할 수 있습니다.

물리적 세계에 존재하지 않고 그 어떤 것도, 그 누구도 뒷받침하지 않는 통화가 어떻게 가치를 가질 수 있을까요?

- 가치는 신뢰성, 희소성, 유용성, 수요 정도 등의 요인에 따라 증가합니다.

## 비트코인은 안전한가요?

- 채굴의 목적은 악의적인 행위자를 저지하고 이중 지불이나 스팸과 같은 원치 않는 행동을 저지하는 것입니다.

- 암호화하여 매우 안전하게 정보를 보호합니다.

사용 예시:

- **공개 키**(은행 계좌번호와 유사하지만 각 거래에서 고유).
- **개인 키**(은행 계좌에 속한 비밀번호와 유사).

거래가 실패 없이 실행되도록 누가 그리고 어떻게 보장할까요?

- 채굴자와 채굴을 통해 보장합니다.
- 나쁜 행위자를 저지하고 원치 않는 행동을 막는 것이 목표입니다.

법정화폐에 비해 **비트코인**의 장점은 무엇일까요?

- 비트코인의 가격은 전 세계 모든 국가에서 동일합니다.
- 국경이 없습니다.
- 인플레이션이 통제되고 발행량이 사전에 정의됩니다.
- 지배구조에 대한 의사결정 권한이 없습니다.

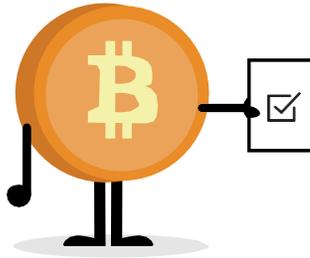
## 4.3 비트코인과 법정화폐의 차이

	비트코인	법정화폐
사용	암호화폐이며 디지털로만 사용할 수 있습니다.	물리적(동전 및 지폐)과 디지털(예: 수표, 앱) 모두에서 사용할 수 있습니다.
규제	채굴을 통해 생성되며 분산 컴퓨터 시스템에 의해 제어됩니다.	중앙 은행에 의해 생성되고 통제됩니다.
지배구조	자발적인 합의 메커니즘이며 높은 수준의 합의가 필요합니다.	중앙 정부가 관리합니다.
가치	채굴자가 많을수록 더 안정적입니다.	수요와 공급에 의해 결정되며 인플레이션에 취약합니다.
발행량	2100만개로 제한됩니다.	제한이 없습니다.
거래 검증	암호학을 통해 검증합니다.	은행이나 중개자를 통해 검증합니다.
거래비용	매우 저렴합니다.	중개자가 있기 때문에 비쌉니다.
거래시간과 속도	평균 10분(비트코인) 및 즉시(라이트닝 네트워크) 전송됩니다.	즉시(현금), 며칠 또는 몇 개월(은행 거래) 소요됩니다.
보안	암호학(수학의 한 분야). 노드의 51%에서 공격을 방지합니다.	은행의 내부 보안, 정부 정책의 변동으로 인해 부정적인 영향을 받을 수 있습니다.
변경사항	비트코인 거래는 변경 또는 취소할 수 없습니다.	거래에서 분쟁이 발생하거나 변경 또는 취소가 발생하는 것이 일반적입니다.

## 비트코인 vs 법정화폐



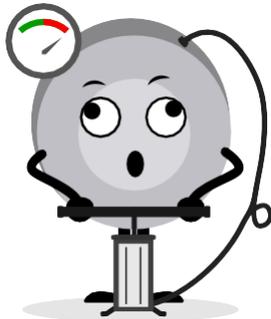
통제된 인플레이션,  
예측 가능하고  
사전 정의된 발행량.



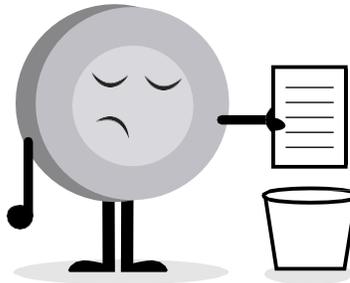
사용자가 수락한  
경우에만 변경 사항을  
적용할 수 있습니다.



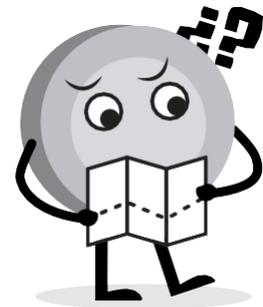
국경이 없으며  
전 세계 모든 사람이  
받아들일 수 있습니다.



원하는 만큼 화폐를 발행하여  
인플레이션을 일으키고  
가치를 평가절하할 수  
있습니다.



국민들의 동의없이  
지도자들의 결정에 따라  
일어납니다.



국내에서만  
사용 가능하며 해외에서는  
사용할 수 없습니다.

**수업 활동.** 16페이지의 클래스 #1에 대한 연습을 완료하세요.

'비트코인' 열에서 항목이 표시된 특성을 충족하는 경우 X로 표시해보세요.

돈으로 어떤 항목을 선택 하시겠습니까?

---

---

---

---

---

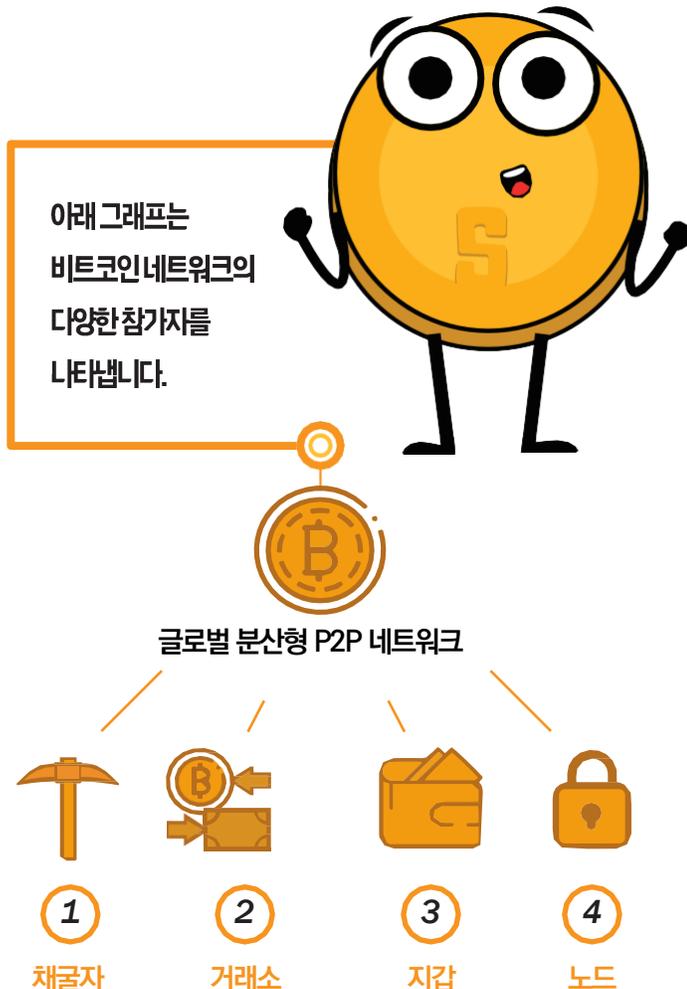
---

---

## 4.4 비트코인 구성요소

누군가 또는 시스템이 **비트코인** 네트워크에 참여하는 방식을 이해하려면 다음과 같이 자문해야 합니다.

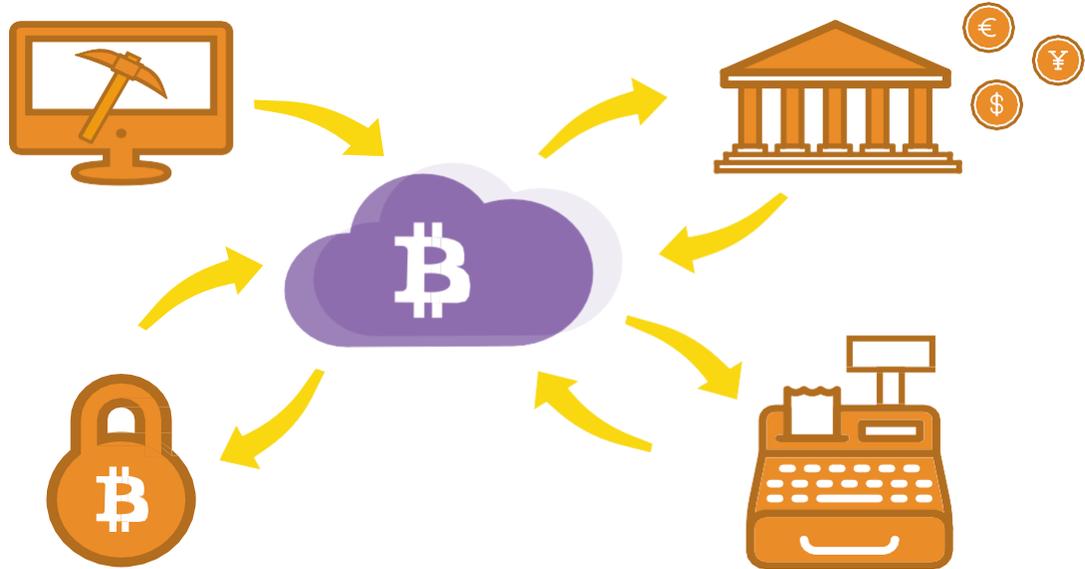
- 그들이 참여하는 거래만 볼 수 있을까요?
- 더 많은 정보에 접근할 수 있을까요?
- 어떤 거래를 할 수 있을까요?
- 네트워크에 어떤 권한이 있을까요?
- 네트워크와 어떻게 상호 작용할까요?
- 전체 블록체인의 사본에 접근할 수 있을까요?



- 1. 채굴자. 전문 컴퓨터 장비:
  - 그들은 새로운 **비트코인**을 만들기 위해 서로 암호 퍼즐을 풀기 위해 경쟁합니다.
  - 그들은 거래를 확인하고 네트워크 보안을 유지합니다.
  - 은행 직원과 동일합니다. 그들은 일을 한 대가로 돈을 받습니다.
- 2. 거래소. 그들은 **비트코인** 및 기타 유형의 암호화폐로 법정화폐를 교환합니다.
  - 그들은 채굴자가 아닌 사람들을 위해 시장에 들어오고 나가는 길을 제공합니다.
  - 은행과 유사합니다. 사용자에게 서비스를 제공합니다.
- 3. 지갑. **비트코인**을 저장, 전송 및 수신하는 데 사용되는 응용 프로그램입니다.
  - 이것은 은행 계좌 또는 온라인으로 돈을 이체하는 앱과 유사합니다.
- 4. 노드. 비트코인 거래를 검증, 전송, 처리 및 저장하는 디지털 네트워크에 연결된 장치입니다. (지갑 외에도 많은 기능을 가지고 있습니다.)
  - 하드웨어와 소프트웨어의 두 가지로 구성됩니다.
  - 모바일 웹 및 앱과 유사합니다.
  - 하드웨어는 소프트웨어를 실행하는 데 필요한 물리적 기반입니다.
- 5. 개발자. 코드 개선 사항을 제안하고 유지보수합니다.

채굴자는 컴퓨터를 사용하여 이전에 발생한 거래를 검증하고 **비트코인**을 생성하기 위한 암호문제를 푼다.

거래소는 기존 통화와 **비트코인** 간의 환전을 수행하여 비 채굴자가 시장에 진입할 수 있는 방법과 법정화폐를 인출할 수 있는 방법을 제공합니다.



사용자는 이메일 주소처럼 작동하는 **지갑**을 다운로드하여 비트코인을 보내고 받는 방법을 제공합니다. 웹 브라우저나 스마트폰 앱을 사용하여 한 지갑에서 다른 지갑으로 **비트코인**을 전송할 수 있습니다.

온라인 비즈니스를 하는 기업은 그들의 웹사이트에 **비트코인** 결제를 활성화하는 방식으로 개인 사용자와 동일하게 **지갑**을 생성합니다. 오프라인 비즈니스를 하는 경우 QR 코드 등을 사용하여 빠르고 쉽게 결제할 수 있습니다.



## 제 5장

# 비트코인의 구매, 보관 및 이동

### 5.1 입금 및 출금 통로

- 비트코인 살 돈이 충분한가요?

### 5.2 비트코인 보관

- 지갑과 라이트닝
- 사토시를 보내거나 받으려면 어떻게 해야 할까요?

### 5.3 거래 주기(on-chain)

- 비트코인 거래란 무엇일까요?
- 거래와 저장을 위한 브릿지 및 정류장
- 거래는 어떻게 이루어지나요?
- UTXO - '사용하지 않은 동전'
- 거래 확인

# 비트코인의 구매, 보관 및 이동

## 5.1 입금 및 출금 통로

- **비트코인**을 얻는 첫 번째 단계는 비트코인을 구매하는 것입니다. 다양한 방법이 있습니다.
  - 환전소, 브로커, ATM, 핀테크 기업, 상품권 등.
- 법정 화폐(유로, 달러 등)에 상응하는 **비트코인**으로 교환됩니다.
- 이러한 기능을 제공하는 서비스는 ‘출입구’입니다.
- 정부는 입금 및 출금 통로를 규제할 수 있습니다.
  - 은행이 **비트코인** 거래소로 돈을 보내거나 받는 것을 금지할 수 있습니다.
    - **비트코인**을 사고팔 수 있는 기능에 제한을 할 수 있지만 **비트코인**을 보내고 받는 것을 막는 것은 불가능합니다.

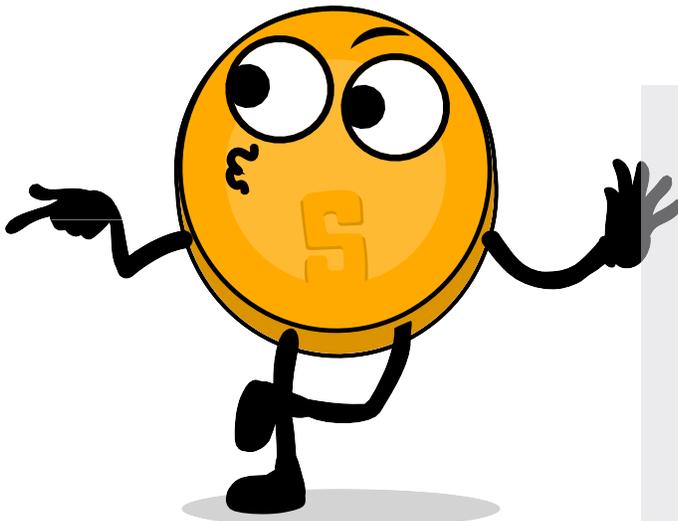
- 기호 ₿ 는 (USD) 또는 \$ 가 미국 달러에 사용되는 것처럼 **비트코인**을 나타내는 데 사용합니다.
- **비트코인**은 동시에 하나의 가격을 가집니다.
  - 예를 들면:  
1 ₿ = \$ 20,000 및 1 ₿ = KRW 28,800,000
- 비트코인은 \$1보다 훨씬 작은 단위로 나눌 수 있습니다,  
\$1 = 100 cents. 1/2 cents나 1/10 cents는 없습니다.
- Satoshi(또는 줄여서 Sat)는 **비트코인** 통화에서 가장 낮은 액면가입니다.
  - 1 BTC = 100,000,000 sats ≈ 0.0003 USD
  - 하나의 **비트코인**을 1억 개로 나눌 수 있음을 의미합니다.
- **단위 편향**: 잘못된 편견...
  - **비트코인** 1개를 모두 구매할 필요는 없으며 원하는 만큼 Sats를 구매할 수 있습니다.

### 비트코인을 살 돈이 충분한가요?

- BTC는 **비트코인** 통화의 공통 단위입니다.

“조금씩 더해서 자주 하다 보면 금세 많아지겠죠.”

-해시오도스



사토시(Satoshi)	비트코인
1	0.00000001
10	0.00000010
100	0.00000100
1,000	0.00001000
10,000	0.00010000
100,000	0.00100000
1,000,000	0.01000000
10,000,000	0.10000000
100,000,000	1.00000000

## 5.2 비트코인 보관

비트코인은 어떻게 보관되나요?

- Sats를 웹사이트에서 구매하면.
  - 돈이 이체될 때 은행 계좌로 받는 것과 유사합니다.
- 자신의 **비트코인**을 소유하고 있는 것처럼 보일 수 있지만 실제로는 그 돈이 제3자가 소유하고 있습니다.
- 따라서 **비트코인** 투자의 위험을 이해하고 다음부터 시작하는 것이 중요합니다.
  - **비트코인**을 보유하는 가장 좋은 방법을 알아 두세요.
  - 지갑이 무엇인지 알아보세요.
    - 각자의 취향에 따라 다양한 선택 방법이 있습니다.
  - 우리가 선택한 지갑의 장단점을 분석해보세요.
    - 모든 요구를 만족시키는 이상적인 지갑은 없다는 것을 이해해야 합니다.

### 지갑과 라이트닝

누가 내 **비트코인**을 통제할까요?

#### □ 자체 보관 지갑(Self Custody)

- 장점:
  - 구매한 **비트코인**의 진정한 소유자가 되는 유일한 방법입니다.
  - 서비스를 사용하기 위해 권한을 요청할 필요가 없습니다.
  - 계정 승인 절차가 없습니다.

- 전 세계 누구나 앱을 다운로드하여 바로 사용할 수 있습니다.
- 돈을 은행에 맡기지 않고 집에 보관해 두는 것과 같습니다.
- 도난을 방지하려면 **비트코인**을 자체 보관하는 것이 좋습니다.
- 어떤 회사/정부도 거래를 통제하거나 제한할 수 없습니다.
- 제3자가 임의로 압수할 수 없습니다.
- 외부의 압력을 받더라도 **비트코인**이 안전하다고 확신합니다.

#### • 위험요소:

- **개인 키** 분실 시 자금을 회수할 수 있는 방법이 없습니다.
- 상대적으로 불편합니다.
- 분실 책임이 개인에게 있습니다.

#### □ 제3자 보관 지갑 (Custody)

- 제3자가 당신의 **비트코인**을 보관하고 있습니다.
- 자금(**개인 키**)은 지갑 공급자의 통제 하에 있습니다.
- 장점:
  - 계정에 대한 액세스 권한을 잃거나 잊어버리더라도 자금을 쉽게 회수할 수 있습니다.
- 위험요소:
  - 항상 인터넷에 연결되어 있어 보안이 더 취약합니다.



# 비트코인의 구매, 보관 및 이동

가장 편리한 지갑은 무엇일까요?

## □ 하드웨어 지갑

- 인터넷에 연결되지 않은 지갑으로 인터넷이 작동하지 않아도 됩니다.
- 현존하는 가장 안전한 지갑입니다.
- 많은 양의 **비트코인**을 저장하는 데 이상적입니다.
- 개인 키는 하드웨어 장치에 저장됩니다.  
[예: 콜드카드 MK3.]
- 개인 키 백업 없이 지갑을 분실하면 자금을 복구할 수 없습니다.

## □ 종이 지갑 (콜드월렛)

- 개인 키를 보관하는 형태로 종이에 복사됩니다.
- 개인 키를 보관하기에 가장 안전하지만 비효율적인 방법 중 하나입니다.
- 보안을 위해서 거래가 이루어질 때마다 새로운 **개인 키**를 사용해야 합니다.

## □ 소프트웨어 지갑 (핫월렛)

- 인터넷에 연결되어 있습니다.
- 모바일 앱 설치 또는 웹을 통해 접속할 수 있습니다.

## ■ 모바일 지갑

- 휴대가 간편하고 편리합니다
- 대면 거래를 할 때 이상적입니다.
- 앱은 예고 없이 제거될 수 있습니다.
- 기기가 훼손되거나 분실된 경우, 자금 회수가 어려울 수 있습니다.  
- QR 코드와 함께 사용하기에 적합합니다.

## ■ 데스크탑 지갑

- 사용자는 자금을 완전히 제어할 수 있습니다.
- 일부는 콜드월렛을 지원합니다.
- 거래 시 QR코드 사용이 어렵습니다.
- **비트코인**을 훔치는 바이러스에 취약합니다.

비트코인 지갑의 구조

개인	미연계	콜드월렛	자체보관 콜드월렛
	연계	핫월렛	자체보관 핫월렛
		쉬움	어려움
사용성			

사토시를 보내거나 받으려면 어떻게 해야 할까요?

## □ 온체인 (on-chain)

- '메인' 네트워크에 연결된 지갑을 통합니다..
- 평균 10분에 한번씩 거래가 승인됩니다.
- 각 거래의 수수료는 금액이 아니라 거래에 필요한 데이터의 크기에 비례합니다.  
- 1달러의 가치를 체인으로 보내고 1달러가 수수료로 지불되는 경우 수수료율은 100%입니다.  
- 10,000달러를 체인으로 보내고 1달러가 수수료로 지불되면 수수료율은 0.01%입니다.

### □ 라이트닝 네트워크 (off-chain)

- ‘레이어 2’ 솔루션: **비트코인**을 보내고 받을 수 있습니다.
  - 수수료가 매우 낮거나 수수료 없이 매우 빠르게 지불합니다.
- 다음과 같은 국가에서 사용됩니다.
  - 지역 제한 및 규제는 대량 채택을 유도합니다.
  - 빠르고, 개인적이며, 경제적이고 효율적인 거래가 필요한 곳.

## 5.3 거래 주기(on-chain)

### 비트코인 거래란 무엇일까요?

**비트코인** 프로토콜을 통해 전송되고 저장되는 것은 **비트코인**이며 페소나 달러가 아닙니다.

- 이 돈의 이동을 **거래**라고 합니다.
- 블록체인(**비트코인**)에 기록되는 두 지갑 간의 가치 이동입니다.

새로운 거래가 네트워크에 전파될 때:

- 노드가 승인하려면 검증 과정을 통과해야 합니다.
  - **유효한 거래:**
    - 노드 모두가 사본을 가질 때까지 한 컴퓨터에서 다른 컴퓨터로 전송됩니다.
    - 약 10분마다 수천 개의 거래와 함께 그룹화됩니다.
    - 채굴을 통해 새 블록이 생성됩니다.
    - 새로운 거래는 블록에 영원히 기록됩니다.
    - 정보를 수정, 삭제 또는 추가하는 것은 불가능합니다.
  - **잘못된 거래:**
    - 거부되며 네트워크를 통해 확산되지 않습니다.

### 거래와 저장을 위한 브릿지 및 정류장

지갑을 통한 거래는 다음 과정과 유사합니다.

- 존재하는 모든 **비트코인**이 금고에 보관되어 있다고 상상해 보세요.
  - 모두 다른 양의 비트코인을 사용하지만 완전히 투명합니다.
  - 누구나 각 상자에 얼마나 많은 **비트코인**이 있고 어떻게 들어왔는지 알 수 있습니다.
- 각 상자에는 단일 소유자의 **주소**가 있습니다.
- 이 주소는 두 개의 다른 키가 필요한 보안 지물쇠로 보호됩니다.
  - 키 중 하나인 **개인 키**는 잠금 장치를 **해제**하고 내부의 비트코인에 접근할 수 있도록 합니다.
  - 그리고 또 다른 열쇠인 **공개 키**는 지물쇠를 **잠그고** 비트코인을 **보호**합니다.
- 네트워크의 각 **참가자**는 **개인 키**를 매우 안전한 장소에 보관해야 합니다.

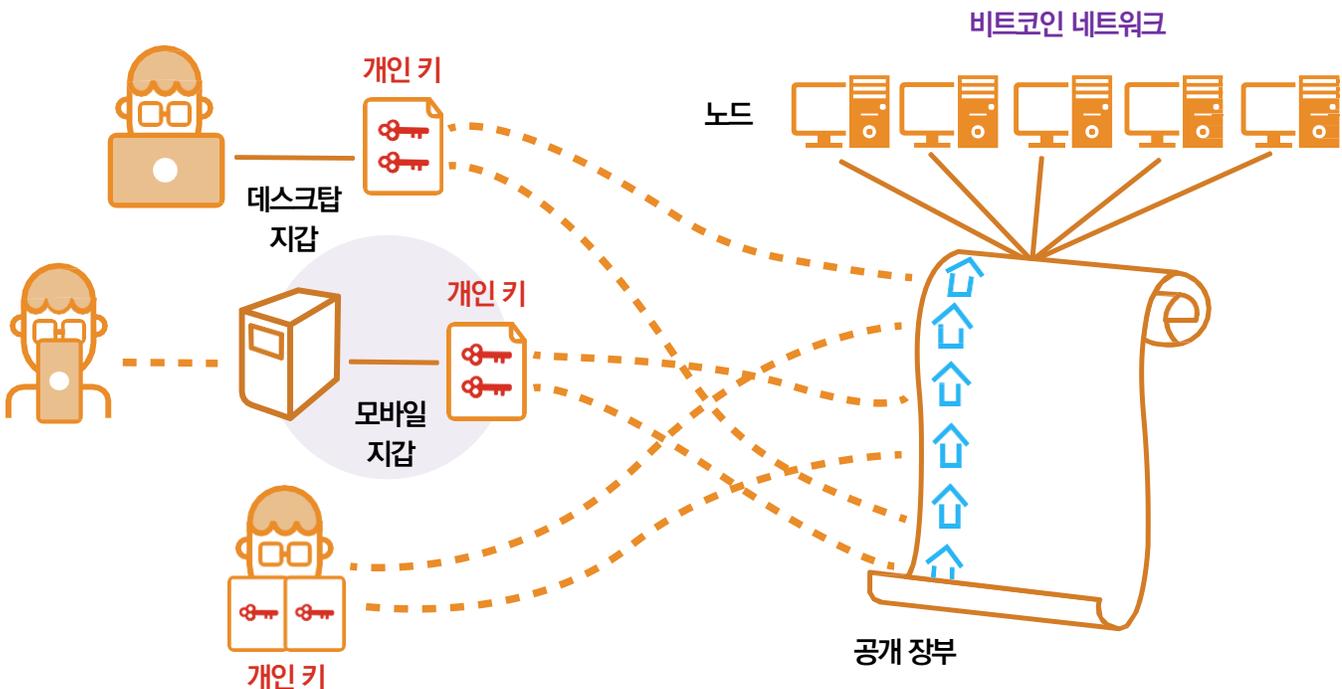
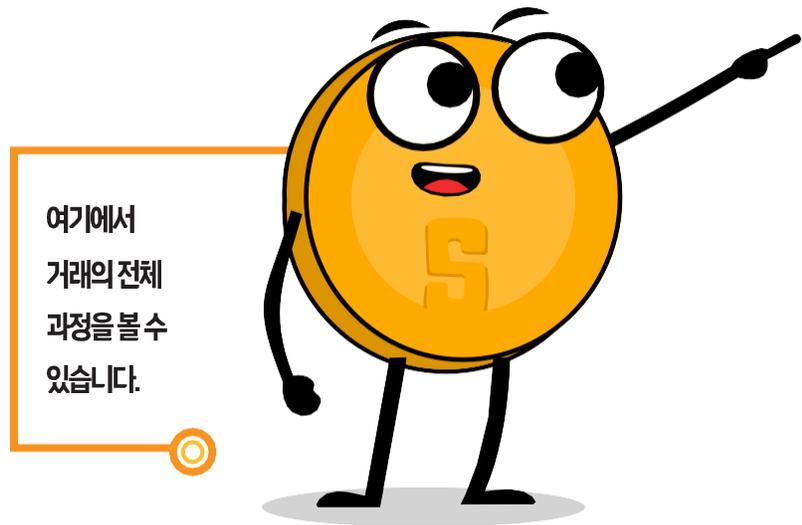
# 비트코인의 구매, 보관 및 이동

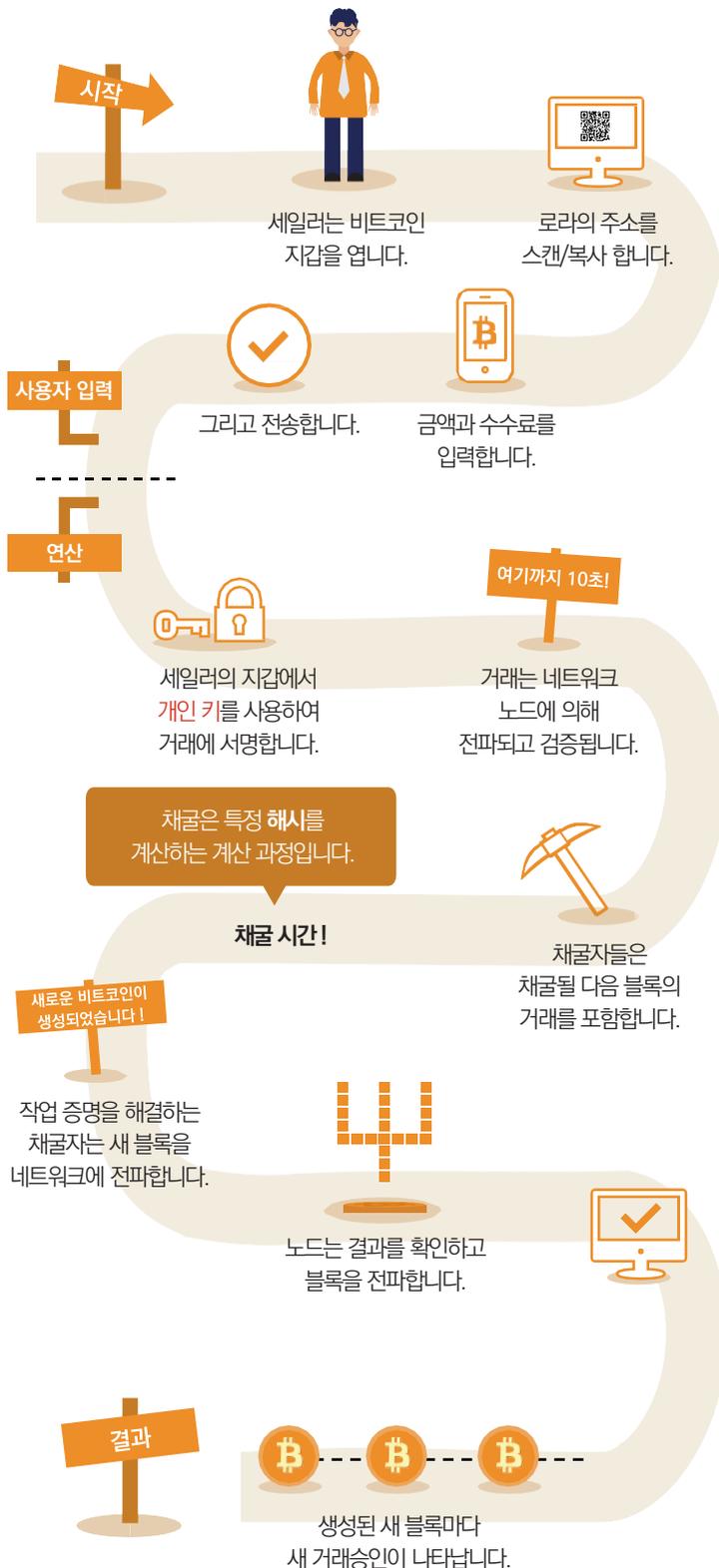


## 거래는 어떻게 이루어지나요?

분산 네트워크에서 성공적인 송금은 각 거래가 고유하고 인식 가능하다는 전제 하에 이루어집니다.

- 상자에 **비트코인**이 있는 경우 소유자는 언제든지 상자를 열어 다음을 수행할 수 있습니다.
  - 원하는 금액의 다른 주소로 이체할 수 있습니다.
  - 송금되기를 원하지 않는 수천 개의 주소가 있다는 점을 생각해야 합니다.
    - 비트코인이 올바른 주소에 입금되도록 정확한 주소를 입력해야 합니다.
  - 마지막으로 금고의 자물쇠는 **공개 키**로 잠가야 합니다.
    - 수취인 이외의 누구도 **비트코인**에 접근할 수 없도록 합니다.
  - 앞으로는 비트코인을 받은 사람의 **개인 키**로만 상자를 열 수 있습니다.





- 세일러가 여동생 로라에게 0.5 비트코인을 보낼 것이라고 가정합니다. 둘 다 지갑이 있습니다.
  - **고유하고 반복될 수 없는 거래의 식별자를 생성해서 전달해야 합니다.**
    - 이 식별자는 각 거래 **고유**의 식별자입니다.
    - 서로 다른 두 거래가 구분 되도록 하기 위한 것입니다.
    - 이것은 또한 검증 과정을 쉽게 만듭니다.
    - 이 과정이 안전하고 효율적으로 이루어지기 위해서는 암호화와 전자서명이 이루어져야 합니다.

- **암호화:** 세일러는 누구도 가로채지 않고 안전한 채널을 통해 **비트코인**을 보내야 합니다.
- **복호화:** 로라는 돈을 받고 다른 사람이 접근할 수 없도록 해야 하며 사용할 수 있어야 합니다.
- **서명:** 세일러는 로라에게 그가 보낸 돈이 원래 자신의 것이었으며 정확한 금액을 보내고 있음을 증명해야 합니다.
- **확인:** 네트워크의 사용자는 세일러의 계정에 지출할 돈이 있는지 확인해야 하고 세일러의 계정에서 공제하고 로라의 계정에 추가해야 합니다.

과정을 상세히 볼까요?

- 1. 세일러는 휴대폰에서 지갑을 열고 로라에게 전송 주소(**공개 키**)를 요청합니다.
- 2. 로라는 이를 세일러와 공유합니다(QR 코드, 이메일 또는 기타 방법의 형태로).
- 3. 이 거래에서 세일러는 QR 코드를 스캔하여 보낼 금액으로 거래를 생성합니다.
  - **채굴자들이 그것을 선택하도록 보상으로 수수료를 추가합니다.**

# 비트코인의 구매, 보관 및 이동

- 4. 한 번의 클릭으로 세일러의 지갑에 충분한 자금이 있는지 확인됩니다.
- 5. 세일러의 지갑은 **개인 키**로 거래에 서명합니다.
  - 그 **비트코인**은 로라에게 전송됩니다.
- 6. 거래가 네트워크를 통해 **노드**로 전송되어 승인되었는지 확인합니다.
  - 확인 될 때 까지 잠시 기다리세요.
- 7. 채굴자 **노드**는 수천 개의 거래를 선택하고 잘못된 거래는 거부합니다.
  - 아직 확인되지 않은 새로운 '후보 블록'에 추가합니다.
  - 그들은 모든 정보를 압축하고 각각은 블록 식별자를 생성합니다.
- 8. 채굴자 간 경쟁을 시작합니다(블록 식별자 간의 추첨과 유사).
  - 자신의 블록을 블록체인에 추가할 다음 사람이 누구인지 확인합니다.
- 9. 승리 블록은 세일러-로라 거래를 포함하고 이를 다른 노드로 전파합니다.
- 10. 노드는 승리한 블록의 식별자를 확인하고 블록체인에 추가합니다.
  - 블록체인에서 **확인된** 해당 블록의 모든 거래를 포함합니다.
  - 수정하거나 삭제할 수 있는 방법은 없습니다. 그것은 그 자리에 영원히 기록될 것입니다.

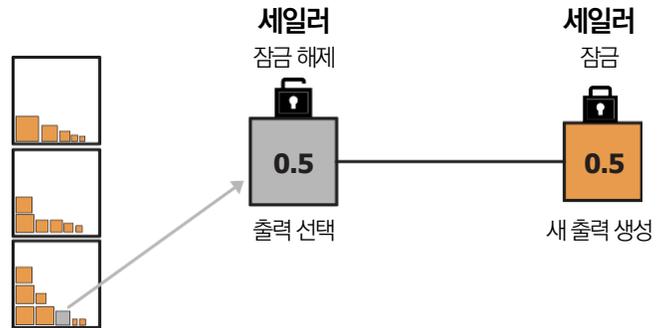
- 11. 로라는 해당 **비트코인**의 소유자가 됩니다.
  - 약 10분 안에 0.5 비트코인을 받게 됩니다.
  - 세일러는 지갑 잔액에서 공제된 금액을 확인할 수 있습니다.
- 12. 거래가 성공적으로 완료됩니다.

## UTXO - '사용하지 않은 동전'

거래는 단순히 한 지갑에서 다른 지갑으로 **비트코인**이 입금되고 출금되는 것입니다.

- 아직 사용되지 않은 비트코인은 UTXO, 미사용 거래 출력 또는 미사용 코인으로 간주됩니다.
- 블록체인의 **현재 상태**는 UTXO의 상태를 보여주는 데이터베이스라고 할 수 있습니다.
- **입력 값**은 거래를 생성하는 데 사용되는 돈을 나타냅니다.
- **출력 값**은 일반적으로 **거래의 결과가 전달되는 주소와 돈을 나타냅니다.**
  - 출력은 지분을 받은 사람에게 전달됩니다.
- 사용자가 다른 사람에게 보내기 위해 자신의 개인 키로 UTXO를 잠금 해제할 때.
  - 안전 금고가 열려 있으므로 잔액이 위험할 수 있습니다.
  - 이러한 이유로 잔액은 항상 새 지갑으로 보내는 것이 좋습니다.

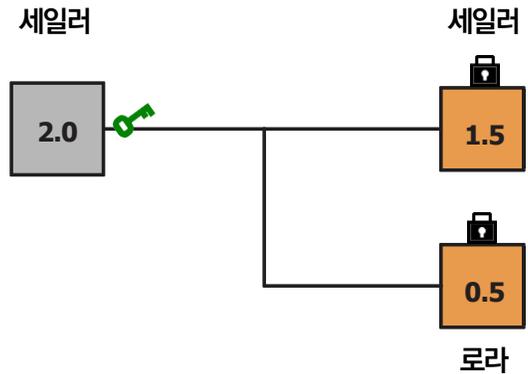
- 원래 지갑에 잔액이 있는 경우:
  - 다른 출력은 변경 사항을 수신하기 위해 생성된 새 주소로 이동합니다.
    - 이 금액을 새로운 입력 UTXO로 변환합니다.
- 네트워크 노드의 경우 다음과 같은 이유로 합의에 쉽게 도달할 수 있습니다.
  - 모든 사람이 동일한 데이터베이스의 복사본을 유지합니다.
  - 각 주소의 잔액을 확인할 수 있습니다.



- 노드는 거래를 실행하기 위해 원래 주소(세일러의 지갑에 있는 0.5 비트코인)를 가리키는 **비트코인**이 충분한지 확인합니다.
- 거래가 확인되면 일정량의 **비트코인**이 두 개의 다른 주소로 분배됩니다.
- 로라의 상자에는 **비트코인**이 늘어나고 세일러의 상자에는 **비트코인**이 줄어듭니다.

## 거래 확인

- 지갑에서 **비트코인** 출력을 승인하고 보내려면,
  - 거래는 **개인 키**로 서명해야 합니다.
  - 이 단계는 자신의 자금을 소유하고 있음을 증명하는 데 필요합니다.
- 지갑 항목을 수신하려면:
  - 사용자는 자신의 주소를 보내는 사람과 공유해야 합니다.
- 다음과 같은 경우 전송이 **확인**됩니다.
  - **비트코인**은 새 주소로 입금된 **비트코인**의 수량을 기록했습니다.
  - 그리고 그는 **보낸 사람**의 지갑에서 그것을 **뺏**니다.



- 송금 확인 후 블록체인은 입금된 지갑, 1.5 비트코인 지갑, 0.5 비트코인 지갑만 모니터링합니다.

거래가 승인되는 방법을 살펴보겠습니다.

- 노란색 상자는 UTXO를 나타냅니다.
- 회색 상자는 더 이상 **비트코인**이 없는 지갑을 나타냅니다(완전히 비어 있음).

- 이것은 이제 사용되지 않은 비트코인 또는 UTXO입니다.



## 제 6장

# 가치 저장 및 지불 네트워크로서의 비트코인

6.1 이중 지불 문제

6.2 메모리 그룹 또는 멤풀

6.3 수업 활동: 거래가 확인되었지만 승인되지 않았습니다.

6.4 비트코인 네트워크 (On-Chain)

- 풀 노드
- 수업 활동: 거래 상태

6.5 '라이트닝 네트워크 (Off-Chain)

- 레이어 1(또는 기본 레이어)과 레이어 2의 차이점은 무엇일까요?
- 수업 활동: 라이트닝 작동 방식

# 가치 저장 및 지불 네트워크로서의 비트코인

## 6.1 이중 지불 문제

자세히 알아보기 전에 다음 사항을 생각해 보겠습니다.

- 비트코인은 디지털 화폐입니다. 다음과 같은 특징이 있습니다.
  - 다른 유형의 디지털 파일(사진, 동영상 등)처럼 복제할 수 없으며,
  - 복제, 위조 하거나 여러 사람에게 동시에 보낼 수 없습니다.
  - 신용카드를 통해 이중으로 지불할 수 없습니다.

*이 비트코인 기능은 어떤 이점을 제공할까요? 예를 들어 설명하겠습니다.*

- 일반적으로 사람들이 영수증을 저장하고 지출을 관리합니다.
  - 주기적으로 자신의 계좌와 은행 잔고를 비교하고 지출의 불일치가 없다는 것을 확인합니다.
- 예를 들어, 식당에서 신용카드 결제가 두 번 청구됐다는 사실을 알게 될 수 있습니다.
  - 2022년 1월 26일 수요일에 5.08달러의 결제가 두 번 발생했습니다.
  - 동일한 점심에 대해 이중 지불된 것입니다.
  - 둘 중 하나를 취소하려고 은행에 가거나 전화를 겁니다.
    - 최선의 경우, 은행이 당신의 주장을 인정하면 몇 달 안에 돈을 돌려받을 수 있습니다.
    - 최악의 경우 식당이 두 번 점심을 먹었다고 주장하며 돈을 돌려주지 않는 것입니다.
- '이중 지불'의 개념을 설명하기 위해 일상적인 예를 계속 살펴보겠습니다.

■ **첫째 날:** 로라가 맥도날드에서 10달러에 점심을 주문한다고 가정해 봅시다.

- 5달러 지폐 두 장으로 점심을 주문합니다.
- 주문은 즉시 확인됩니다.
- 로라와 직원 모두 그 과정을 눈으로 목격했습니다.
- 단순히 돈과 햄버거의 교환이었습니다.

■ **둘째 날:** 로라가 같은 점심메뉴를 주문하기 위한 5달러 지폐 두 장을 가지고 있습니다.

- 그러나 하나는 정상이고 하나는 위조(똑같은 사본)입니다. 그녀는 위조된 지폐로 주문합니다.
- 일련 번호가 동일하기 때문에 직원은 그 중 하나가 위조임을 쉽게 알 수 있습니다.
- 또는 단순히 전날과 같이 지불을 수락할 수도 있습니다.
- 직원이 바빴기 때문에 일련 번호를 보지 않고 지불을 수락합니다.

■ **셋째 날:** 로라는 즐거운 시간을 보냈지만 맥도날드에 다시 가는 것을 두려워했습니다.

- 이제 맥도날드에서 지폐를 복제한 것처럼 비트코인을 복제하려고 합니다.
- 그녀는 세일러와 페페 모두에게 0.2 비트코인을 빚지고 있지만 그녀의 지갑에는 0.2 비트코인만 있습니다.
- 로라는 자신의 휴대폰과 어머니의 휴대폰에서 시드 문구와 함께 지갑을 엽니다.
- 그녀는 자신의 전화에서 0.2 비트코인을 세일러에게 보냅니다.
- 그녀의 어머니의 전화로 0.2 비트코인을 페페에게 보냅니다.
- 두 비트코인을 정확히 동시에 보내도록 합니다.

- 두 개의 다른 노드가 두 개의 거래를 수신합니다.
- 로라는 지갑에 0.2 비트코인만 사용할 수 있음을 기억합니다.



- 수천 건이 전송되었지만 승인되지 않은 거래가 있는 공간입니다.
- 서로 다른 노드끼리 공유하는 전체 메모리 풀은 없습니다. 각 노드는 다음을 수행해야 합니다.
  - 뱀풀에 거래를 포함하기 전에 거래의 유효성을 확인합니다.
  - 검증된 거래를 인접 노드로 전파합니다.
  - 유효하지 않은 거래를 거부합니다.

- 네트워크 노드가 이를 인지하고 두 거래 중 하나가 거부됩니다!
- 어떻게 거부된 것 일까요? 어떤 거래가 거부되고 어떤 거래가 승인되는지 결정하는 방법은 무엇일까요?
- 이것을 달성하기 위해 사토시 나카모토는 다음과 같은 메커니즘을 찾았습니다.
  - 블록체인에 추가하기 전에 네트워크의 모든 참여자가 합의한 방식으로 거래가 유효한지를 확인합니다.
  - 위에서 언급한 이중 지불문제에 대한 훌륭한 해결책입니다.

**여기에서 유효한 거래가 노드에서 노드로 얼마나 빨리 전파되는지 확인할 수 있습니다.**

## 6.2 메모리 그룹 또는 뱀풀

- 거래가 실행되고 블록에 설정되기 전에.
  - ‘뱀풀’ 또는 메모리 그룹이라는 대기 공간에 들어갑니다.

그것은 무엇이며 여기에 입력되는 거래는 어떻게 될까요?

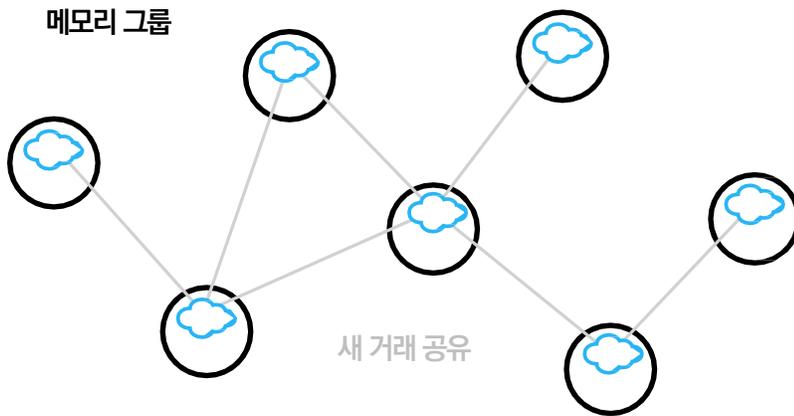
- 노드는 거래의 유효 여부를 판단해야 합니다.
  - 유효하다고 승인한 경우:
    - 채굴자가 거래를 선택하고 다음 블록에 추가하기를 기다립니다.
    - 그리고 공개 데이터베이스에 영구적으로 기록됩니다.
  - 다음과 같은 경우 거부될 수 있습니다:
    - 다른 거래와 충돌이 있는 경우.
    - 송금할 자금이 충분하지 않은 경우.
    - 서명이 유효하지 않고 해당 비트코인을 사용할 수 있는지 확인할 수 없는 경우.

- 일부 거래는 대기 공간에 있습니다.

- 금전적 보상을 추가하지 않으면 최종 거부될 때까지 최대 72시간 동안 머물러 있습니다.

- **멤플**은 DDoS 공격에 대한 추가 보안 및 저항 계층 역할을 합니다.

- 네트워크가 작은 거래들로 넘쳐날 때.
  - 관리할 수 없는 혼잡을 유발합니다.



멤플은 거래가 블록에서 승인되기를 기다리는 곳입니다.

-  tx hsh 6053b699...  
fee rate: 3 sat/vB
-  tx hsh bb3b8clfc...  
fee rate: 1 sat/vB
-  tx hsh d7c2532a9...  
fee rate: 15 sat/vB
-  tx hsh 0ecdd9c6...  
fee rate: 2 sat/vB



멤플의 주요 목적은 다음과 같습니다.

1 승인되지 않은 거래를 보관합니다.



2 채굴자가 블록에 포함 될 수 있도록 거래를 제공합니다.



노드가 피어로부터 처음 거래를 수신할 때 거래가 유효한 것인지 **확인**해야 합니다. 어느 누구도 거래의 오류가 있거나 오해의 소지가 있는 거래를 원하지 않습니다.

## 6.3 수업 활동: 거래가 확인되었지만 승인되지 않았습니다.



**수업 활동.** 이 활동에 대한 교사의 지시를 따르세요.  
시작하려면 QR 코드가 있는 링크를 스캔하세요.

- 아래에서 승인되지 않은 실제 거래를 볼 수 있습니다.
  - 고유 식별자(거래의 디지털 기록).
  - 차지하는 메모리 공간.
  - 지급되는 수수료.
  - 이체 금액.

TxID: **a434948b2de9de18398294f84e42436ec59fb86faf34a21052bd640a97cd94b7d**

\_\_\_\_\_ input → \_\_\_\_\_ outputs

**Size:** \_\_\_\_\_ vbytes (점유하는 메모리 공간)

**Fee Rate:** 27.01 sats/vbyte (수수료율 / 현재 vbyte)

**Fee:** \_\_\_\_\_ sats (거래 수수료)

**Total Value** \$ \_\_\_\_\_ BTC ≈ \$ \_\_\_\_\_ USD (총 거래 금액)

- 거래를 분석해볼까요?
  - 입력 값과 출력 값의 크기를 비교해보세요.
  - 참가자가 더 많거나 더 작은 수수료를 지불했나요?
  - 다음 블록에서 어떤 거래 발견될까요? 왜 일까요?
  - 블록이 뎀플에 들어있다는 것은 무엇을 의미할까요?
  - 거래가 승인되었다는 것은 무엇을 의미할까요?

---



---



---



---



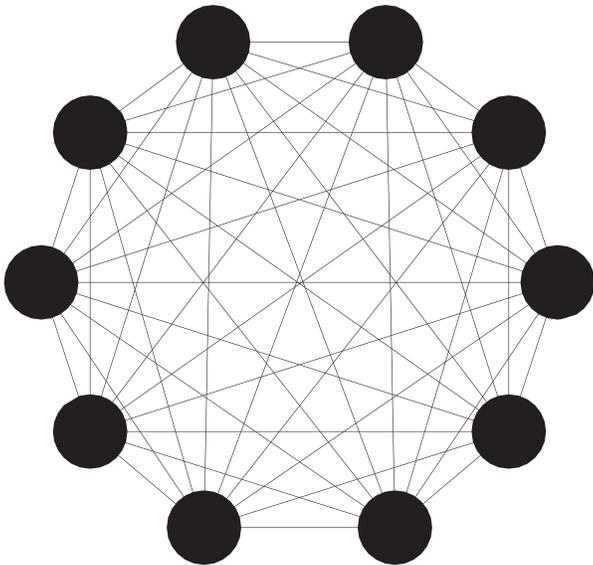
---

# 가치 저장 및 지불 네트워크로서의 비트코인

## 6.4 비트코인 네트워크 (On-Chain)

- **비트코인** 노드로 구성됩니다.
  - 규칙을 준수하는 소프트웨어(Bitcoin Core).
    - 그들은 네트워크로 연결된 사이버 공간에서 서로 통신합니다.
    - 각자가 실행하는 **비트코인** 소프트웨어는 버전이 다를 수 있습니다.

비트코인 네트워크 노드는  
공통 규칙 세트에 따라  
연결됩니다.

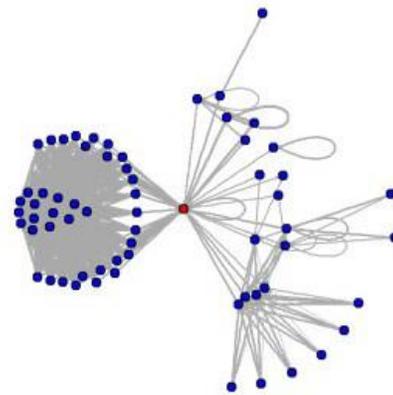


- 이러한 연결 지점에서 정보(즉, 거래)를 생성, 전송 및 수신할 수 있습니다.
  - 다양한 유형의 노드가 있습니다. 각각은 네트워크에서 다른 역할을 합니다.

## 풀 노드

- 그들은 **비트코인** 소프트웨어를 실행합니다.
  - 풀 노드는 합의에 도달하기 위해 자율성을 가지고 스스로 결정 할 수 있습니다.
    - 동일한 결정을 내림으로써 신뢰할 수 있고 안전한 탈중앙화 네트워크를 만듭니다.
    - 풀 노드에는 세 가지 기능이 있습니다.

### □ 1. 인접 노드에 정보를 전파합니다

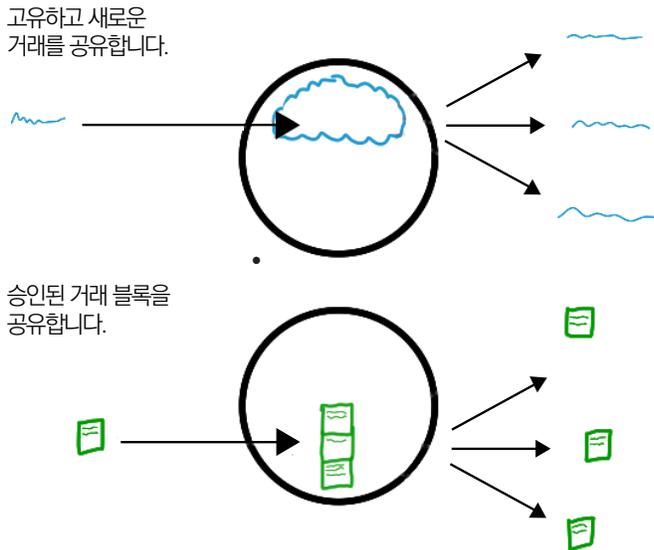


이 다이어그램은 거래의  
전파를 나타냅니다.

- 노드가 전파하는 두 가지 유형의 거래.
  - A. 신규 거래
    - 이들은 메모로 곧바로 이동합니다.
    - 노드는 이러한 거래를 승인하거나 거부하는 역할을 합니다.
      - 블록체인의 기록과 소프트웨어의 규칙 목록을 기반으로 합니다.
    - 그들은 유효한 거래를 이웃 노드로 전파합니다.
      - 아무도 잘못되거나 악의적인 거래를 받고 싶어하지 않습니다.

## — B. 승인된 거래

- '승인'되고 블록에 기록된 거래입니다.
- 이들은 그룹화되어 블록을 생성합니다. 개별적으로 공유되지 않습니다.



## □ 2. 승인된 거래의 사본을 보관하세요.

- 그것은 블록체인에 있는 모든 블록의 완전한 사본을 유지하고,
- '승인'은 거래가 취소될 위험을 기하급수적으로 줄입니다.



## □ 3. 블록을 검증하고 다른 노드와 합의에 도달하세요.

- 모든 참여 노드는 블록체인에 포함시키기 전에 전체 블록에 포함된 정보와 비교하고 확인해야 합니다.
  - 블록체인의 다른 노드와 공유합니다.
- 새로 승인된 거래의 상태는 온라인으로 추적할 수 있습니다. 어떻게 할까요?
    - 블록 탐색기는 모든 비트코인 거래를 볼 수 있는 도구입니다.
    - 각 주소의 잔액을 확인하고 각 거래의 세부 정보를 보는 등의 작업을 수행할 수 있습니다.

### 수업 활동: 거래 상태

**수업 활동.** 거래의 다양한 속성을 관찰할 수 있는 다음 링크로 이동합니다.

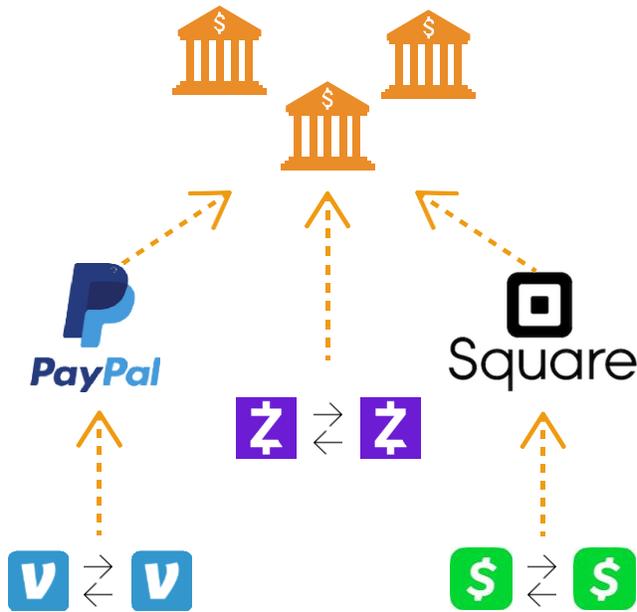
<https://www.blockchain.com/explorer?view=btc>



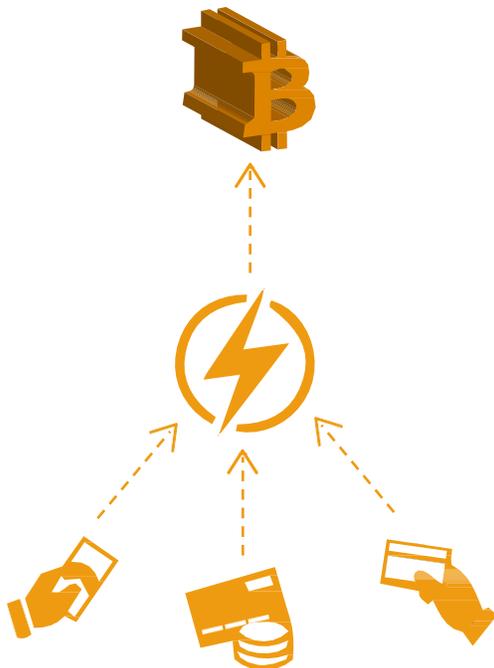
다음 페이지에서 질문에 대한 답변을 마칩니다.



현대 통화 시스템 = 폐쇄 네트워크  
은행을 생존하기 위해 유지합니다



비트코인 화폐 시스템 = 개방형 네트워크  
비트코인은 최종성을 유지합니다



라이트닝 네트워크에 구축된  
모든 앱은 상호 운용 가능합니다

● 라이트닝은 **비트코인** 위에 구축된 일련의 규칙(스마트 계약)입니다.

- 즉시 전송이 가능합니다.
- 높은 거래량이 존재합니다.
- 메인 네트워크와 연결은 끊어졌습니다.
- 네트워크상의 모든 거래를 기록할 필요는 없습니다.
  - 하지만 더 효율적인 대체 네트워크입니다.
  - **비트코인**의 모든 보안을 제공합니다.
  - 하지만 보상의 종류가 다릅니다.
- 더 많은 프라이버시를 제공합니다.
- **라이트닝**은 **비트코인**의 확장성 문제를 해결합니다.

● 다음 예시를 생각해 봅시다.

- 손님이 호텔에 체크인합니다. 그들은 당신의 신용 카드를 요구합니다.
  - 숙박에 대한 객실 요금 및 부대 비용을 충당하기 위함.
- 비용이 발생할 때마다 신용 카드로 결제하는 것보다 효율적이고 저렴합니다.
- 호텔은 고객이 이용한 모든 비용을 기록합니다.
- 호텔 내에 약국과 미용실이 있습니다.
  - 손님은 제품을 구입하고 서비스를 이용하며 객실 번호를 불러줍니다.
  - 호텔은 고객과 비즈니스 간의 결제 중개 수수료를 부과합니다.
- 손님에게 추가적으로 이용하거나 시설을 망가트렸을 경우 필요한 금액을 예치금에서 차감합니다.
- 체크아웃 이후에 손님이 요금 및 잔액이 정확한지 확인하고 동의한 경우에만 카드 값이 청구됩니다.

# 가치 저장 및 지불 네트워크로서의 비트코인

라이트닝네트워크와그이점에대해자세히  
알아보겠습니다.



라이트닝 네트워크는 유사하지만 다르게 작동합니다.

- 라이트닝 네트워크는 거래 당사자간의 신뢰가 없어도 거래가 가능합니다.
  - 오해입니다. 이것은 신용 시스템이 아닙니다.
  - 라이트닝 트랜잭션은 IOU(차용증)가 아닙니다.
    - 실제 UTXO를 움직이는 유효한 **비트코인** 거래입니다.
- 누군가에게 신용 카드를 주고 계좌를 열어 두는 대신.
  - 두 개의 노드는 지불 채널 또는 전송 경로를 열 수 있습니다.
  - 당사자는 원하는 금액 만큼 거래할 수 있습니다.
    - 잔액을 항상 최신 상태로 유지합니다.
  - 채널에 예치된 금액이 클수록.
    - 양방향으로 서로 전송할 수 있는 **비트코인**의 양이 증가합니다.

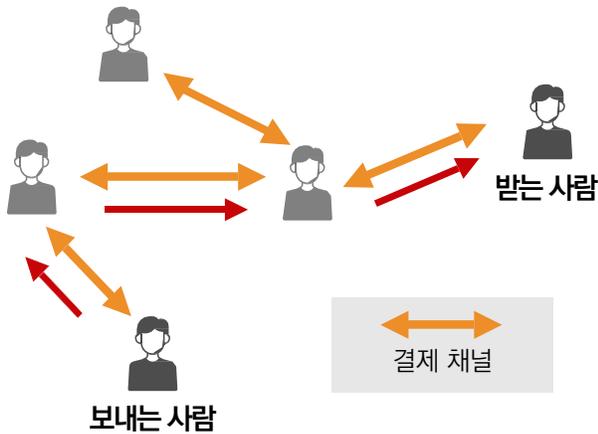
- 거래하는 모든 사람과 경로를 만들 수 있습니다.
- 채널이 많을수록.
  - 목적지까지 더 빠른 경로를 찾을 가능성이 커집니다.
- 직접 연결 가능한 경로가 있는 경우.
  - 모든 것이 간단하게 채널의 크기에 따라 거래가 이루어집니다.
- 제3자(브릿지)를 통해 연결하는 경우.
  - 통행료를 지불합니다.
- 새 채널을 열기 위해 두 노드 모두 채굴자에게 약간의 수수료를 지불합니다.
- 네트워크의 모든 거래를 업데이트하고 확인할 필요가 없습니다.
  - 이것은 비용과 시간이 많이 소요될 것입니다.
- 어느 한쪽이 채널을 폐쇄하기로 결정하면.
  - 최근 상태를 **비트코인** 네트워크로 전송합니다.



다음 링크에서 시각화 자료를 참조하세요.

<https://lnrouter.app/graph/zero-base-fee>

- A가 B와 열린 채널을 가지고 있고 B가 C와 열린 채널을 가지고 있다면 A는 B를 신뢰하거나 알 필요 없이 B를 통해 C에게 비트코인을 보낼 수 있습니다.



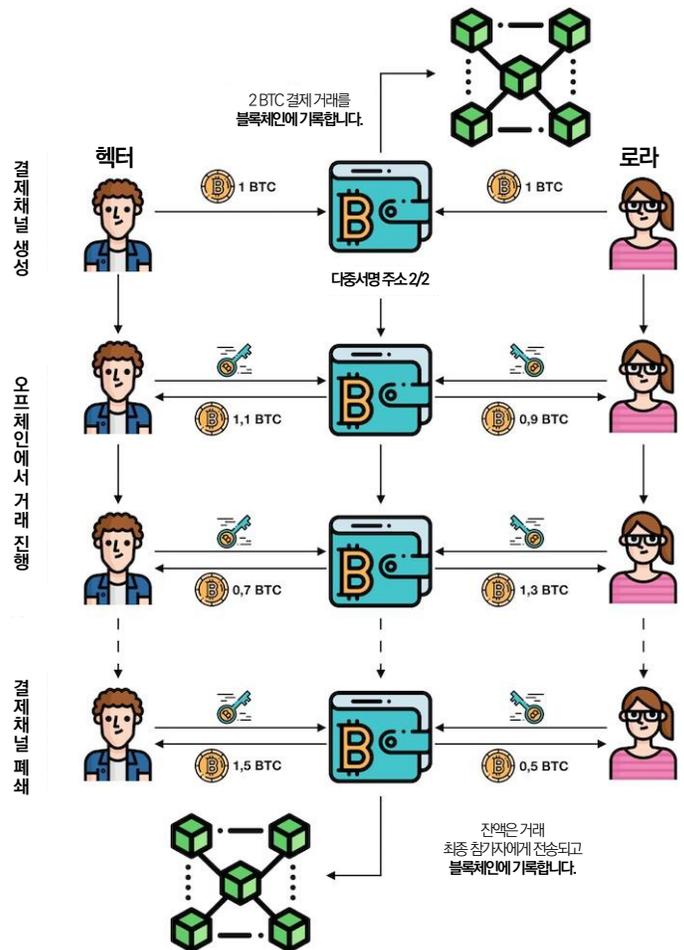
### 수업 활동: 라이트닝 작동 방식

수업 활동. 시뮬레이터를 봅시다. 이 활동을 완료하려면 교사의 지시를 기다리세요.

<https://www.robtex.com/lnemulator.html?conf=A5-5B,B5-5C&send=A2C>



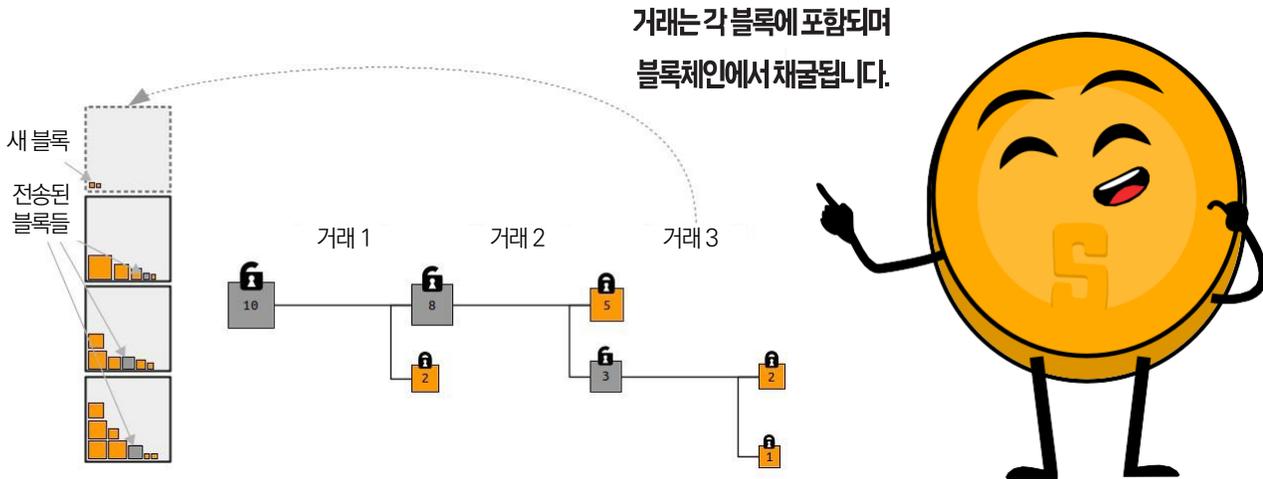
- 라이트닝을 사용하는 것은 이메일을 보내는 것만큼 저렴하고 빠릅니다.
  - 비트코인의 안전하고 무신뢰 기반 특성의 이점을 이용합니다.
  - 열린 채널에서 돈을 들고 있는 두 사람만이 그 돈이 얼마나, 얼마나 자주, 언제 움직이는지 알 수 있습니다.



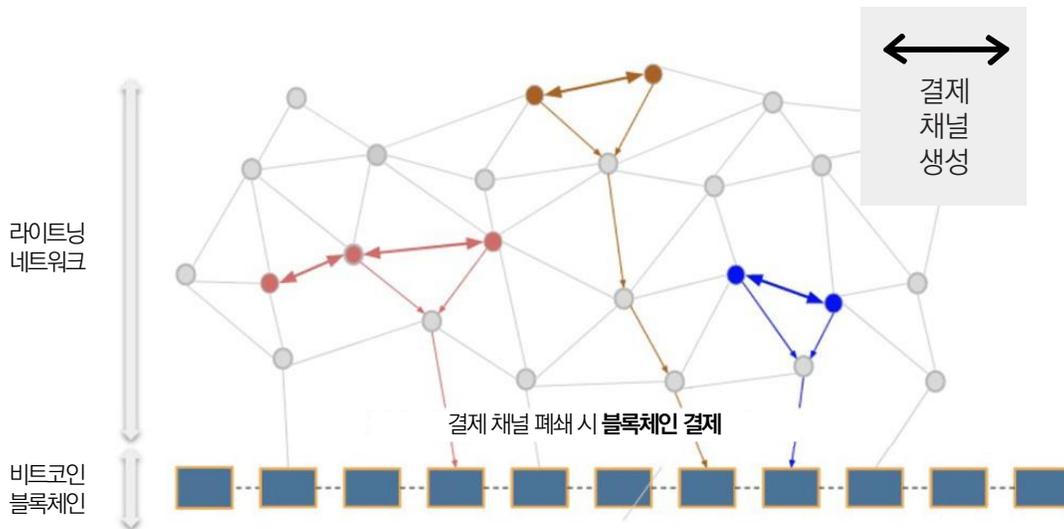
- 이에 비해 3개의 거래가 메인 네트워크로 이루어진 경우, 즉 기본 레이어에 남아 있는 경우.
  - 거래는 훨씬 오래 걸리고 비용이 많이 들었을 것입니다.

# 가치 저장 및 지불 네트워크로서의 비트코인

- 이러한 각 거래에는 모든 네트워크 참가자가 확인해야 합니다.



## 라이트닝 네트워크 작동 방식







## 제 7장

# 채굴자와 비트코인 채굴

### 7.1 채굴 노드

- 채굴자 간의 수학적 경쟁은 어떤 것일까요?

### 7.2 해시의 중요성 이해하기

- 함수란 무엇일까요?
- 해시란 무엇일까요?
- SHA-256이란 무엇일까요?
  - 수업 활동: 해시 생성
- 논스란 무엇일까요?
- 머클 트리란 무엇일까요?

### 7.3 채굴

- 신뢰하지 말고 검증하세요
- 블록 해시
- 블록 논스
- 수업 활동: 실시간 블록 분석하기

## 7.1 채굴 노드

- 채굴자들은 암호 퍼즐 문제를 먼저 풀고 새로운 블록을 만들기 위해 노력합니다.
  - 금전적 보상을 목적으로 채굴합니다.
  - 새로운 보상은 그들이 수학 문제를 풀기위해 들인 노력의 증거입니다.
  - 따라서 네트워크 보안을 유지하는 데 도움이 됩니다.
- 채굴자는 항상 풀 노드를 참고하여 다음을 수행합니다.
  - 유효한 거래들을 그룹으로 묶어 블록을 생성하고 네트워크에 제안합니다.
    - 작업 증명. PoW(Proof of Work)라는 합의된 규칙을 통해 네트워크의 보안을 강화합니다.
    - 사기를 방지하고 누구도 믿을 필요 없는 신뢰를 가능하게 합니다.
- 각 블록의 보상은 다음으로 구성됩니다.
  - **비트코인** 소프트웨어로 만든 새로운 **비트코인**.
  - 그리고 해당 블록에 포함된 거래의 수수료.
- 풀 노드와 채굴 노드의 주요 차이점:
  - 채굴 노드는 **비트코인** 네트워크에 새로운 블록을 제안할 수 있습니다.
    - 그들은 '채굴'이라는 과정에서 수학 문제를 해결하려고 노력 합니다.
    - 그들은 그 수학 문제를 올바르게 풀었다는 것을 증명해야 합니다.
    - 그리하여 블록에 대한 보상을 받을 수 있습니다.
  - 풀 노드는 새 블록을 제안할 수 없습니다.
    - 따라서 보상을 받을 수 없습니다.

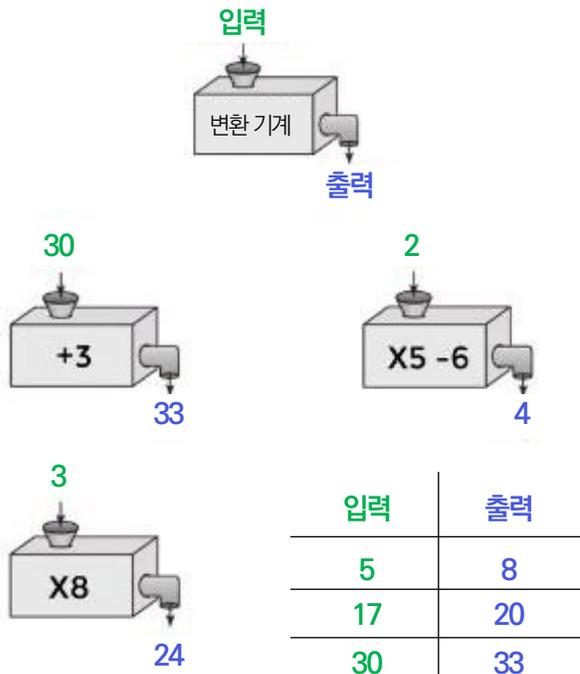
## 채굴자 간의 수학적 경쟁은 어떤 것일까요?

- 다시 예시로 돌아가서.
  - 각 채굴자에게는 1에서 1000까지의 숫자가 표시된 특수 주사위가 있습니다.
  - 채굴자들은 우승을 가리기 위해 대회에 등록하며, 우승자는 상금으로 6.25 **비트코인**이 조금 넘는 보상을 받습니다.
  - **비트코인**은 1~1000중에서 목표 숫자를 선택하고 모든 사람이 볼 수 있도록 게시합니다. 목표 숫자로 8이 선택되었다고 가정해 보겠습니다. 대회를 시작합니다.
  - 우승 조건은 주사위를 굴려 8보다 작은 숫자를 뽑는 것입니다.
    - 일부 채굴자들은 더 높은 승률을 가지고 있습니다. 왜냐하면?
    - 그들은 더 많은 자금으로 주사위를 몇 개 더 샀습니다.
    - 어떤 채굴자는 다른 채굴자보다 더 빠른 속도로 주사위를 던집니다.
  - 대회 시작.
    - 채굴자들은 피곤하더라도 우승하기 위해 주사위를 수백 번 굴려야 합니다.
    - 운이 좋은 채굴자가 굴린 주사위에서 8보다 작은 숫자가 뽑혔고 그 채굴자는 손을 들고 "내가 이겼어!"라고 말합니다.
    - 다른 채굴자들은 주사위 굴리기를 멈추고 자신이 던진 주사위를 봅니다.
    - 이렇게 하면 모든 채굴자가 그것이 사실인지 아닌지 확인할 수 있습니다.
    - 손을 든 채굴자가 승자라는 데 다수가 동의하면 그에게 보상이 주어집니다.
    - 대회를 다시 이어갑니다.
  - 더 많은 채굴자가 대회에 참가하면 **비트코인**은 목표 숫자를 더 작게 낮추어 누군가가 승리하는 데 항상 약 10분이 걸리도록 조절 합니다.

## 7.2 해시의 중요성 이해하기

### 함수란 무엇일까요?

- 변환 기계:
  - 어떤 값이 입력되고 특정 연산규칙에 의해 변환되며 완전히 다른 결과값이 나타납니다.
  - 즉, 입력 값  $x$ 를 변환 기계에 넣습니다.
  - 미리 정의된 연산규칙(더하기, 빼기, 곱하기 등)이 적용됩니다.
    - 결과는 출력 값  $y$  또는  $f(x)$ 로 나타냅니다.



- 예:  $f(x)=3x+4$ 는 다음과 같습니다.
  - 입력 값  $x$ 에 3을 곱하고 4를 더한 다음 출력  $f(x)$  또는  $y$ 를 얻습니다.
  - $f(2)$ 의 답은 무엇일까요? 즉,  $x=2$ 일 때  $y$ 의 값은 무엇일까요?
  - 그렇다면  $f(x)=15$ 를 만족하는  $x$ 는 어떻게 찾을 수 있을까요?

$$f(x)=3x+4=15 \quad 3x+4=15.. \quad x=?$$

- 어떤 함수는 단방향입니다.
  - 계산하기는 쉽지만 역산하기는 어려운 특성이 있습니다.
  - 결과 값을 알더라도 입력 값을 추론할 수 없습니다.
- 수학이 지루하다면 더 쉬운 예시를 들어 보겠습니다.
- 우리는 빨간 과일 주스를 만들 것입니다.
  - 다음은 입력 값입니다.
  - 물 1컵, 얼음 3개, 라즈베리 18개, 딸기 8개, 블랙베리 15개, 설탕 1/5컵.
  - 함수 실행:
    - 블렌더에 모두 함께 넣고 섞습니다.
  - 출력 값의 결과:
    - 맛있는 주스가 나옵니다.
  - 다른 사람이 당신이 만든 주스의 정확한 재료와 분량을 알아내는 것은 거의 불가능합니다.
  - 이것은 단방향 함수를 의미합니다.
  - 주스를 입력 값으로 다시 변환할 수 없습니다.

# 채굴자와 비트코인 채굴

## 해시란 무엇일까요?

- **비트코인**은 수학의 한 분야인 암호학을 사용합니다.
  - 입력 및 출력 과정은 매우 유사합니다.
  - 암호화 해시 함수:
    - 모든 값에 필요로 하는 암호화 과정입니다.
    - 고유하고 반복할 수 없는 결정적이며 쇄도 효과를 가지는 식별자(해시 값)을 반환합니다.

비트코인  
디플로마

해시 함수

F62D623DE  
61AB4A14C  
7862D00937  
44F55FEDA  
E409A76FF8  
6E40FE5F4A  
AA43B65

- 입력 값에는 제한이 없습니다.
  - 해시는 항상 동일한 길이의 문자를 생성합니다.
  - 해시는 또한 입력 값의 식별자(해시 값)로 간주됩니다.

### 💡 용어 사전

**결정적:** 동일한 입력 값은 항상 동일한 출력 결과 값을 생성합니다.

**쇄도 효과:** 약간 값이 약간만 변하더라도 완전히 다른 출력 값을 생성합니다.

## SHA-256이란 무엇일까요?

- **비트코인**이 사용하는 특정 해시 함수를 SHA-256이라고 합니다
  - 결과 값 또는 해시는 항상 16진수(0에서 9 사이의 숫자와 A와 F 사이의 문자)입니다.
    - SHA-256(입력) = 해시
- 해시를 생성해 보겠습니다. 다음 예시를 살펴보겠습니다.

SHA-256(로라) =

96F22B173D8926CB49E48C672B449F9DB2FDAF2E  
536FE55D5215FB5777763C5F

SHA-256(로라P) =

AC70214B72D22C2649F599B3E9B757883C6E25296  
41889BE38C302E797BAE077

SHA-256(안녕하세요. 제 이름은 로라입니다.) =

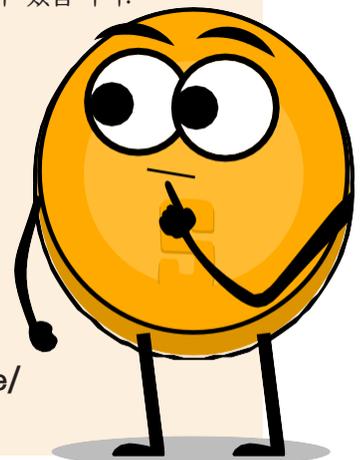
554517BA7AA49B840156EBE158B96275E242A6BB  
DFE45B13EEB07B7B5CA2C03B

수업 활동: 해시 생성

**수업 활동.** 해시 값 생성을  
다음 웹 사이트에서 연습할 수 있습니다.



<https://hashgenerator.de/>



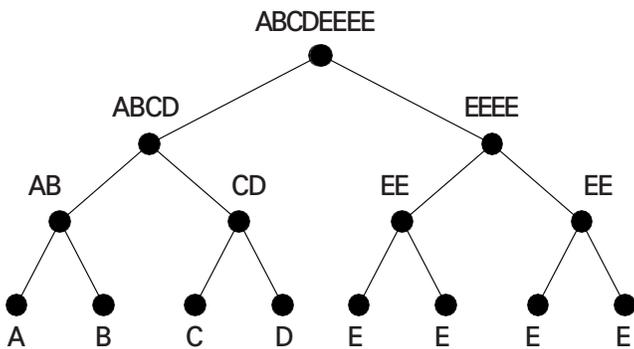


# 채굴자와 비트코인 채굴

- 데이터 구조를 전체적으로 확인할 수 있는 주요 식별자입니다.

- 블록이 포함하는 모든 거래정보를 나타내는 최종 데이터입니다.

- 머클 루트 또는 머클 트리라고 합니다.



- 메모에 거래들이 많을수록 네트워크는 더 혼잡해 집니다.
  - 금전적 보상은 일반적으로 트래픽이 많을 때 더 커집니다.
  - 트래픽이 많은 동안 채굴자는 수수료가 더 높은 거래를 선택합니다.
  - 트래픽이 감소하면 수수료가 낮은 거래들이 추가됩니다.

## 7.3 채굴

이제 **비트코인** 과정으로 돌아갑니다.

- 채굴자는 다음 블록에 포함할 거래들을 자유롭게 선택할 수 있습니다.
  - 그들은 검증할 새로운 거래를 선택하고 '후보 블록'으로 그룹화합니다.

*후보 블록'에 포함될 거래는 어떻게 선택해야 할까요?*

- 채굴자는 더 큰 금전적 보상을 갖고 더 작은 공간을 차지하는 것을 선택합니다
  - 전송자는 채굴자에게 보상을 제공하기 위해 수수료를 추가합니다.
  - 채굴자들이 정직하게 일할 동기가 생깁니다.

*각 후보 블록은 무엇으로 구성되어 있을까요?*

- 블록의 크기는 약 2.5MB입니다.
- 하나의 블록은 거래를 처리할 수 있는 제한 용량(수천개 가량)을 가지고 있으므로 효율적으로 선택하는 것이 중요합니다.
  - 블록 헤더를 포함합니다.
    - 이 블록 헤더는 해시 됩니다.

SHA-256 (헤더) = 결과

## 이 결과는 무엇에 사용될까요?

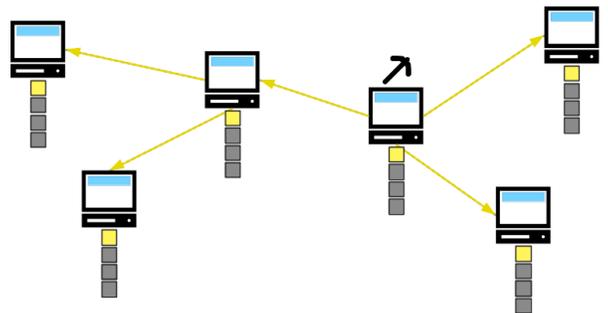
- 목표는 기존 체인의 마지막 블록 뒤에 위치할 조건에 맞는 새 블록의 유효한 해시 값을 생성하는 것입니다.
  - 이를 위해 채굴자는 '승리 해시'를 생성해야 합니다.
    - 특정 '목표 값' 미만이어야 합니다.
  - '결과 값'이 원하는 해시보다 크면.
    - 채굴자는 nonce를 1증가시키고 다시 시도합니다.
    - 채굴자들은 이것을 초당 수천 번 반복합니다.
    - 블록 보상을 얻기 위해 이렇게 합니다.
    - 그리고 해당 블록의 '기록' 또는 고유 해시를 생성합니다.
  - 다른 채굴자보다 '승리 해시'를 먼저 달성할 때까지 nonce를 수천 번 증가시키고 가능한 많은 결과 값을 생성하기 위해 노력합니다.
  - 목표 값보다 작은 결과 값으로 승리할 때까지 주사위를 여러 번 굴리는 앞에서 본 예시와 매우 유사합니다.
- 이는 네트워크의 모든 채굴 노드가 새 블록을 채굴할 수 있음을 의미합니다.
  - 하지만 그렇게 하려면 에너지를 소비해야 합니다.

ID 블록은 무엇일까요?  
알아 봅시다!

전문 채굴팀이 수학적 문제를 해결하여 블록을 채굴합니다.

## '승리 해시'가 발견되면 어떻게 될까요?

- 운이 좋은 채굴자가 마침내 승리 해시를 생성합니다.
  - 전체 네트워크에 승리를 알립니다.
    - 해당 해시는 '블록 해시' 또는 고유 식별자가 됩니다.
- 나머지 채굴자에게 블록의 유효성 검증은 간단한 과정입니다.
  - 모든 거래가 정상적인지 확인하기만 하면 됩니다.
  - 그리고 블록의 해시가 '목표 값'보다 작은 지 확인합니다.



- 블록이 검증되면 다른 노드가 채굴된 블록을 기존 체인에 추가합니다.
  - 해당 블록에 포함된 모든 거래는 블록체인에 영구적으로 기록됩니다.
- 해당 과정은 약 10분마다 반복됩니다.
  - 채굴자들은 그 뒤에 새로운 블록을 채굴하기 시작할 것입니다.

# 채굴자와 비트코인 채굴

그리고 목표 값을 찾은 채굴자는 어떻게 보상을 받나요?

- 모든 후보 블록은 보상을 포함하는 첫 번째 거래를 생성합니다.

- 여기에는 블록이 생성될 때 발행될 새로운 **비트코인**이 포함됩니다.

- 그리고 선택된 거래에 의해 생성된 모든 거래 수수료를 포함합니다.

- 승리한 채굴자만이 보상을 받을 수 있습니다.

- 엄청난 노력이 필요한 계산: PoW 또는 작업 증명.

- PoW는 성공적인 방법입니다.

- 해시를 찾는 것은 매우 어렵지만 검증하는 것은 매우 쉽기 때문입니다.

- 이 거래를 코인베이스 또는 기본 통화라고 합니다.

- 블록체인의 각 블록에서 첫 번째에 위치하고 있습니다.

신뢰하지 말고 검증하세요. (Don't Trust, Verify.)

이것은 무엇을 의미 할까요?

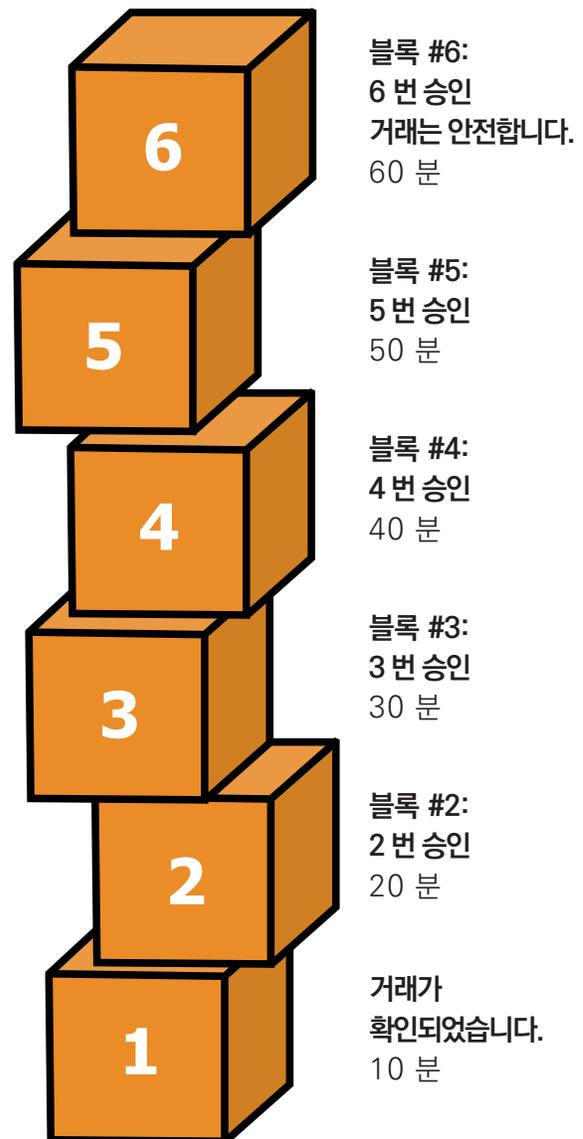
- 거래는 블록에 포함될 때 확인을 받고 각 후속 블록이 검증된 후에 승인됩니다.

- 이러한 블록이 블록체인에 포함되기 위해서는 네트워크에서 생성된 마지막 블록 뒤에 제대로 연결되어야 합니다.

- 블록체인의 승인은 “거래가 네트워크에서 처리 및 검증되었으며 취소될 가능성이 매우 낮음”을 나타냅니다.

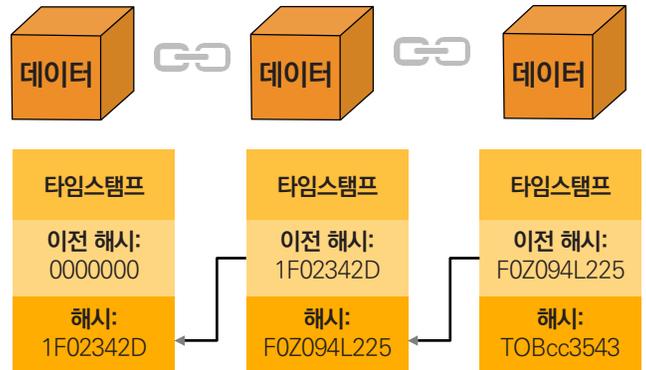
- 자금이 이체되었는지 확인하려면 최소 6번의 승인을 기다리는 것이 좋습니다.

- 비트코인은 현존하는 가장 안전하고 투명한 블록체인입니다.



## 블록 해시

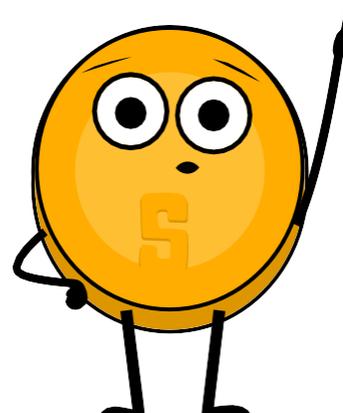
- 각 블록은 이전 블록을 참조합니다.
  - 블록 헤더의 '이전 블록' 필드를 통하여 확인합니다.
- 각 블록을 이전 블록에 연결하는 일련의 해시는 생성된 첫 번째 블록으로 돌아가는 체인을 생성합니다.
  - 첫 번째 블록은 제네시스 블록으로 불립니다.
- 기록한 거래를 조금만 바꾸더라도 블록의 해시가 크게 바뀌고 블록체인이 끊기에 됩니다.
- 해커가 거래의 심표라도 조작하려고 하면 후속 블록을 검증하는 데 연속적인 오류가 발생합니다.
- 각 블록에는 이전 블록에 대한 정보가 있기 때문입니다.
- 각 블록의 해시 값을 따라가다 보면 제네시스 블록에 도달합니다.
  - 헤더에는 다음이 포함됩니다.
    - 1. 블록 내의 데이터 요약, 즉 **머클 루트**로 압축된 모든 거래입니다.
    - 2. 블록체인에서 이전 블록의 해시입니다.
    - 3. **논스**는 '목표 값'을 찾기 위해 필요한 만큼 변경할 수 있습니다.
- SHA-256 해시를 사용하여 블록에 포함된 모든 정보가 압축됩니다.
  - 이 결과는 '**블록 해시**' 또는 '기록'을 나타냅니다.



버전	02000000
이전 블록 해시 (reversed)	17975b97c18ed1f7e255adf297599b55330edab87803c817010000000000000
머클 루트 (reversed)	8a97295a2747b4f1a0b3948df3990344c0e19fa6b2b92b3a19c8e6badc141787
타임스탬프	358b0553
목표 값	535f0119
논스	48750833
거래 개수	63
코인베이스 거래 (채굴된)	
거래	
...	

블록해시

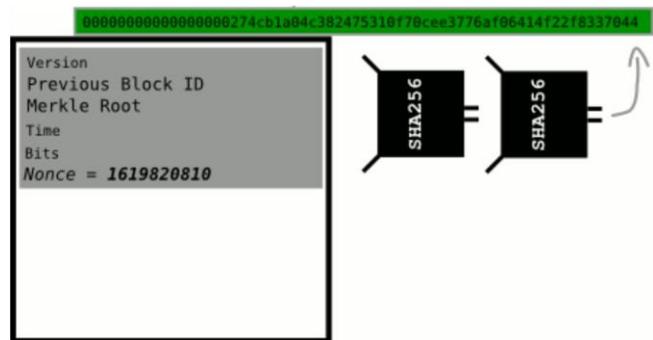
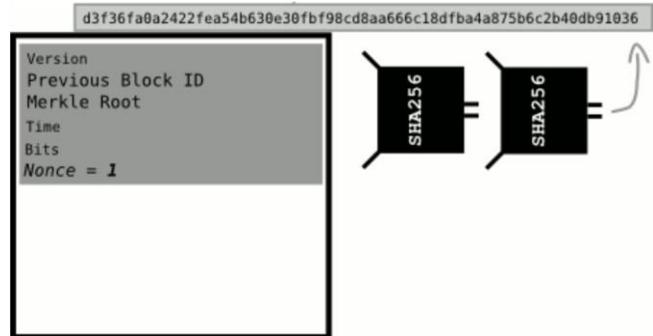
```
0000000000000000
e067a478024addfe
cdc93628978aa52d
91fabd4292982a50
```



# 채굴자와 비트코인 채굴

## 블록 논스

- 필드의 논스는 헤더 내부의 숫자입니다.
  - 채굴자는 헤더 해시가 목표 난이도 또는 목표 값이 될 때까지 증가시킵니다.
- 목표 난이도는 여러 개의 연속한 0으로 시작합니다.
  - 0의 개수는 가변적입니다.
  - 얼마나 많은 채굴자가 블록을 채굴하려고 하는지에 달려 있습니다.
- 채굴자는 헤더 해시에 추가되어 난이도 목표를 충족하는 논스를 찾으면 새 블록의 헤더에 추가하고 네트워크로 전송하여 나머지 채굴자가 유효한 블록인지 확인할 수 있도록 합니다.



## 수업 활동: 실시간 블록 분석하기

**수업 활동.** 다음 링크에서 실시간으로 블록 체인을 분석할 수 있습니다. 웹사이트의 정보를 바탕으로 질문에 답해보세요.



1. 마지막으로 채굴된 블록은 무엇일까요?

---



---

2. 그 블록에 얼마나 많은 거래가 포함되었나요?

---



---

3. 비트코인에서 거래되는 총 가치는 얼마일까요?

---



---



4. 블록의 크기(MB)는 얼마일까요?

---

---

---

5. 블록의 논스는 몇 개의 0으로 시작할까요?

---

---

---

6. 채굴자는 총 얼마를 벌었을까요?

---

---

---

7. 채굴자가 네트워크에 거래를 추가하기 위해 받은 수수료의 총 가치는 얼마일까요?

---

---

---

8. 블록의 가치가 가장 높은 거래 중 하나를 선택합니다. 비트코인은 몇 개의 지갑에 분배되었나요?

---

---

---

---



## 제 8장

# 희소성, 비용, 가격 및 변동성

8.1 블록 보상의 중요성

8.2 반감기

- 반감기 이벤트

8.3 시간 경과에 따른 비트코인의 가치

- 중장기 요인

8.4 채굴자에 대한 보상

- 채굴 난이도

8.5 무엇을 또는 누구를 조심해야 할까요?

- 비트코인 공격
- 51% 공격이란 무엇일까요?

# 희소성, 비용, 가격 및 변동성

## 8.1 블록 보상의 중요성

성공적인 탈중앙화 경제 시스템을 만들려면:

- 채굴자는 **비트코인**을 채굴하기 위해 자금을 투여합니다.
- 네트워크를 보호하는 동시에 다음을 수행합니다.
  - 채굴자들은 네트워크에서 자유롭게 순환할 수 있는 새로운 코인을 생성합니다.
- 블록 보상은 채굴자에게 보상 역할을 합니다.
  - 거래 수수료는 네트워크 장애를 방지합니다.

## 8.2 반감기

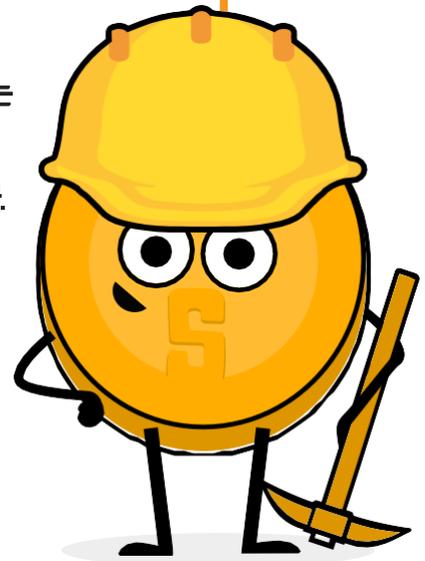
- 사토시 나카모토는 발행 담당자 없이 새로운 **비트코인**을 발행하는 매우 전략적인 방법을 고안했습니다.
- 보상이 점차 줄어드는 모델을 지향하였고 다음과 같이 설정 하였습니다.
  - 210,000 블록마다 생성되는 **비트코인** 수가 절반으로 줄어듭니다.
    - 약 4년마다 발생합니다.
  - 시스템에 얼마나 많은 부채가 생길지 알지 못하는 명목 화폐가 직면하는 문제와 달리,
    - **비트코인**의 총 발행량은 21,000,000입니다.
    - 고정된 공급량은 코드로 제어됩니다.
    - 합의를 통해 시행합니다.

- 처음에 보상은 블록당 50 **비트코인**으로 설정되었습니다.
- 약 4년마다 보상이 절반으로 줄어드는 것을 반감기 이벤트라고 합니다.

### 반감기 이벤트

- 첫 번째 반감기는 2012년 말에 발생했습니다.
  - 블록 210,001은 25 비트코인만 보상했습니다.
- 두 번째 반감기는 2016년에 발생했습니다.
  - 보상은 12.5 비트코인으로 감소했습니다.
- 그리고 반감기는 2140년까지 계속될 것입니다.
  - 2,100만 **비트코인**이 채굴될 때까지 계속됩니다.
- 반감기는 다음과 같은 의도로 만들어졌습니다
  - 인플레이션 방지.
  - 자연적 희소성 추구.

여기서 현재  
네트워크에서 순환하는  
채굴된 총 비트코인의  
개수를 볼 수 있습니다.



그렇다면 왜 보상을 줄어둘게 할까요? 보상을 동일하게 유지하지 않는 이유는 무엇일까요? 채굴자에게 불공평하지 않을까요?

그 질문에 대한 답은 수요와 공급의 법칙에 있습니다.

- 코인이 너무 빨리 생성되거나 **비트코인**의 발행량에 제한이 없는 경우:
  - 순식간에 너무 많은 **비트코인**이 유통되고 가치가 떨어질 것입니다.
- 한꺼번에 2,100만 개가 생성된 경우:
  - 몇몇 사람들이 독점했을 수 있습니다.
  - 다른 사람은 그것을 축적할 기회가 없었을 것입니다.
- 다음 그래프는 반감기가 시간 경과에 따라 가격에 어떤 영향을 미치는지 보여줍니다.

## 8.3 시간 경과에 따른 비트코인의 가치

**비트코인**의 가치가 상승했습니다:

- 2009년에는 0.01달러 미만(첫 거래 시) 이었습니다.
- 2021년 11월 최고 약 68,000달러 였습니다.
- 지난 10년간 최대 80%까지 하락했지만 모두 회복되었을 뿐만 아니라 장기적으로 상승하는 추세입니다.
- 수요와 공급에 영향을 미치는 요인이 다양해 졌습니다.

- 왜 비트코인이 가치가 있을까요?
- 왜 이렇게 가격이 올랐나요?
- 왜 그렇게 변동성이 있을까요?



# 희소성, 비용, 가격 및 변동성

반감기를 더 잘 이해하기 위한 몇 가지 중요한 용어가 있습니다.

## □ 1. 발행량:

- 지금까지 생성된 **비트코인**의 총 개수입니다.
- 2022년 7월 기준으로 약 19,101,000개의 **비트코인**이 생성되었습니다.

## □ 2. 공급량:

- 이미 유통 중인 코인의 개수와 아직 채굴되지 않은 비트코인 개수의 합입니다.
- **비트코인**의 총 발행량은 2,100만 개가 됩니다.
  - 현재 약 400만 **비트코인**이 분실된 것으로 추정됩니다.
  - 비밀번호 분실, 잘못된 출력 주소 또는 프로그램 오류로 인해 사용할 수 없는 것으로 간주됩니다..

## □ 3. 시가 총액:

- **비트코인** 발행량의 총 시장 가치는 법정화폐 가격으로 계산됩니다.
- **비트코인**의 현재 가격(USD)에 현재 발행량을 곱합니다.

$$\text{시가 총액} = \text{현재 가격} \times \text{발행량}$$



## 비트코인의 최근 5년 퍼포먼스



- 이전 페이지의 그래프에서 지난 5년 동안의 **비트코인** 가격을 볼 수 있습니다.
  - 이것은 가격이 얼마나 변동성이 있는지 시각화하는 쉬운 방법입니다.
    - X축은 시간, Y축은 USD 기준 가격입니다.

가격 변동과 관련될 수 있는 세계적 사건은 무엇일까요?

그렇다면 가격을 결정하는 요소는 무엇일까요? 채굴은 어떻게 진행되나요? 반감기가 가격에 언제 영향을 미칩니까?

- 수요는 계속해서 영구적으로 증가하고 있습니다.
- 공급에 관한 시스템의 규칙은 고정되어 있습니다.
- 이제 막 관리되기 시작한 13년 된 초기 자산입니다.
  - 물론 가격의 변동성은 계속 될 것입니다.
  - 그러나 그 가격은 계속해서 상승하고 있습니다.

비트코인 가격의 역사적 차트를 분석합니다.

ColinTalksCrypto.com



## 중장기 요인

- **비트코인**의 가격을 결정하는 요인은 중장기적으로 분석할 수 있습니다. 다음으로 우리는 그 요인들을 각각 볼 것입니다.

## □ 중기 요인:

- 트레이딩.
  - 다른 금융 시장과 달리 주 7일 24시간 운영됩니다.
  - 거래는 모바일을 통해 이루어질 수 있습니다.
    - 원하는 양의 **비트코인**을 쉽게 교환할 수 있습니다.
  - 홀더에게는 가격이 하루에 최대 20%까지 변동될 수 있으므로 이것은 악몽입니다.
  - 트레이더에게는 이러한 가격 변동을 활용하고 수익을 올릴 수 있는 기회입니다.
- 세계 뉴스 및 이벤트.
  - 세계 사건, 뉴스에 민감하게 반응합니다.
- 채굴 비용.
  - 채굴자는 채굴을 위한 비용을 지불해야 합니다.
  - 전기료가 오르면 채굴자들은 전기료 청구서와 하드웨어 비용을 충당해야 하기 때문에 **비트코인**의 40~60%를 팔아야 합니다.
- 시장 거품.
  - 최근 몇 년 동안 **비트코인** 구매자는 더욱 다양해지고 구매 및 저축 습관도 다양해졌습니다.
  - 비트코인 보유량과 그에 대한 행동은 **비트코인**의 전체 가격을 변동시킬 수 있습니다.
- 정부 규제.
  - 암호화폐 규제가 날로 증가하고 있어 **비트코인** 가치에 영향을 미칠 수 있습니다.
  - 조 바이든(미 합중국 대통령)은 10,000달러 이상의 디지털 자산 거래를 국세청에 신고해야 하는 법을 도입했습니다.

# 희소성, 비용, 가격 및 변동성

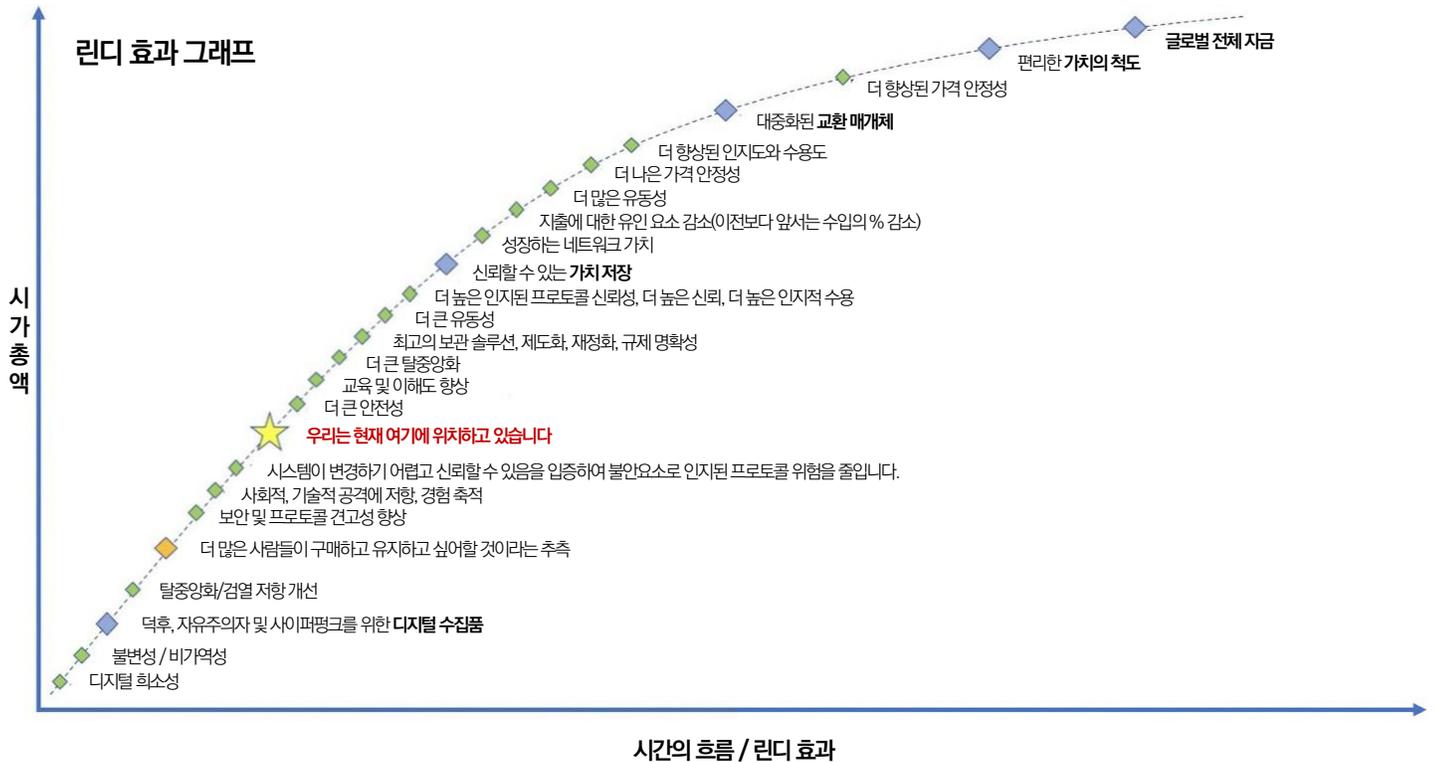
## □ 장기적 요인:

- 반감기.
  - 비트코인 보상은 4년마다 반으로 줄어듭니다.
  - 이 때 채굴자의 보상은 감소합니다.
  
- 대량 채택.
  - 모든 사람이 하이퍼 비트코인화라는 과정에 돌입하기 시작하고 더 많은 돈을 **비트코인**에 투자하면 가격이 기하급수적으로 상승합니다.

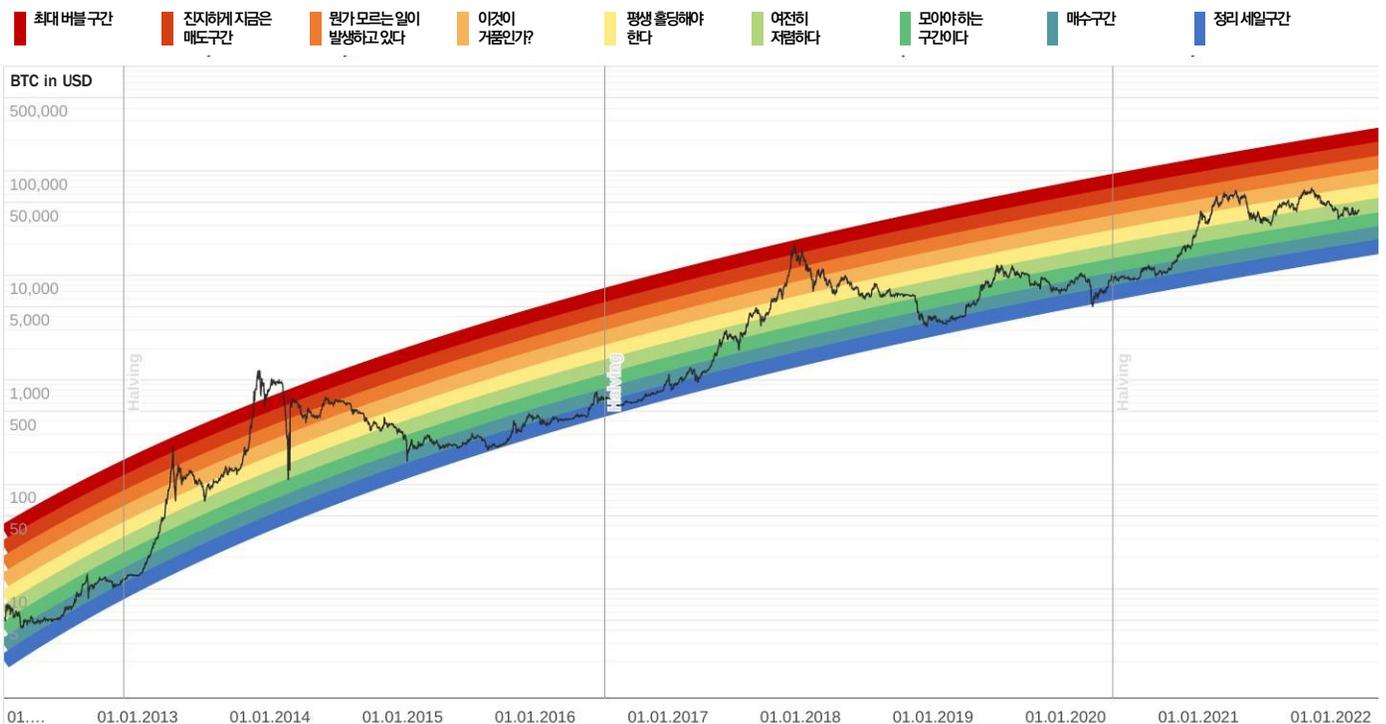


- 린디 효과.
  - 그것은 부패하지 않는 것들의 생존에 대한 이론입니다.
    - 아이디어나 기술이 오래될수록 기대 수명이 길어집니다.
  - 부패하지 않는 기술의 기대수명은 상품의 생존기간과 비례합니다.
  
- 제한된 발행량.
  - 비트코인 개수가 한정되어 있다는 사실은 2140년 이후에 시스템을 희석할 수 없다는 것을 의미합니다.
  - ‘무지개 차트’는 로그 스케일을 사용하여 비트코인 가격을 시각화 합니다.
    - 과매도 상태일 때에는 파란색 및 녹색 영역으로 표시됩니다.
    - 과매수 상태일 때에는 주황색, 빨간색 및 보라색 영역으로 표시됩니다.
  - 이 차트는 비트코인 매수, 매도 전략을 결정하는데 유용한 정보를 제공합니다.
  - 일부 매우 성공적인 투자자들은 다음과 같이 참을성 있게 기다립니다.
    - 가격이 파란색/녹색 영역에 도달하면 매수합니다.
    - 가격이 빨간색 영역에 접근하는 동안 조금씩 매도합니다.



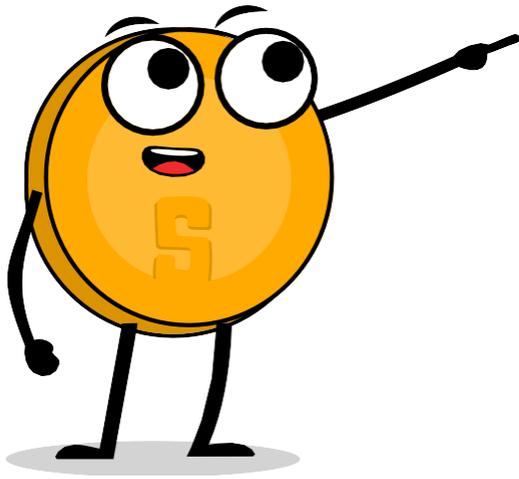


## 무지개 차트

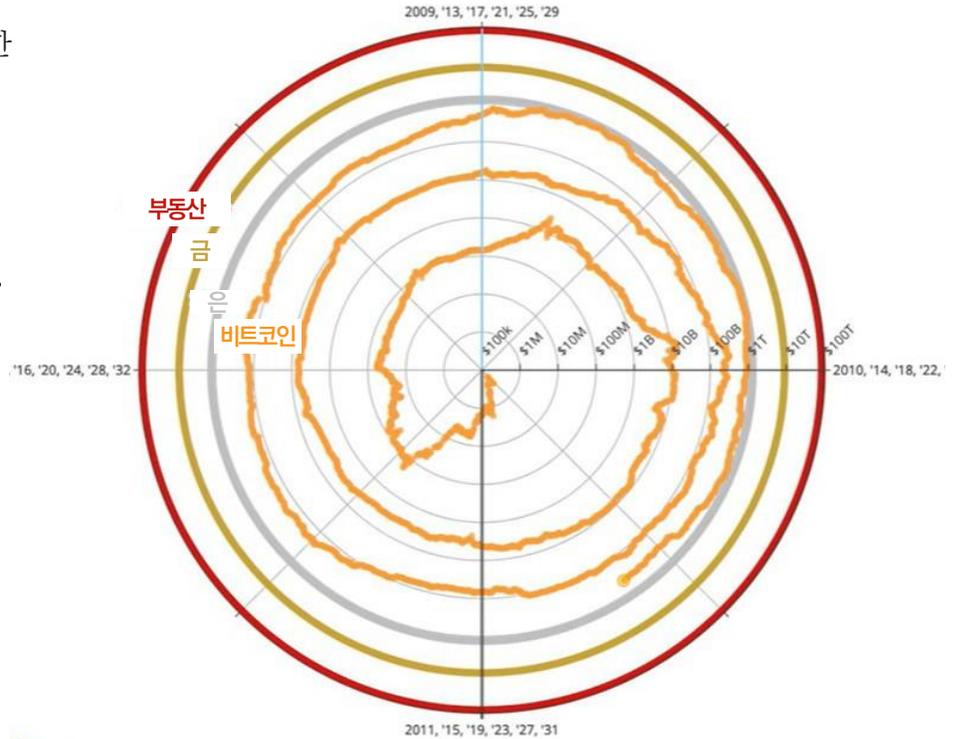


# 희소성, 비용, 가격 및 변동성

- 다른 글로벌 화폐 자산의 성장과 **비트코인**의 성장을 4년 주기 관점에서 비교해보겠습니다.
  - 오른쪽 차트에서 금, 은, 부동산에 대한 **비트코인** 시가총액을 볼 수 있습니다.

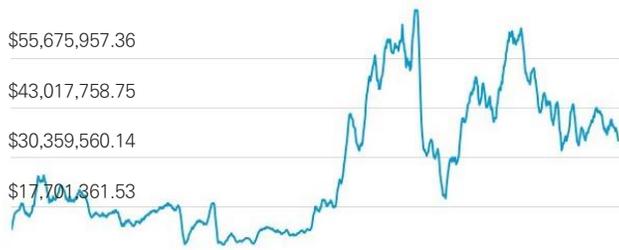


## 자산 비교 나선



## 8.4 채굴자에 대한 보상

- 채굴자에 대한 보상과 금전적 보상이 시간이 지남에 따라 어떻게 변했는지 살펴보고 다른 사람들보다 수익성이 높은 시간이 있음을 관찰합니다.
  - 채굴자는 작은 보상에도 불구하고 그 과정에서 장기적으로 **비트코인**의 가치가 증가하기 때문에 여전히 채굴을 이어 나갑니다.

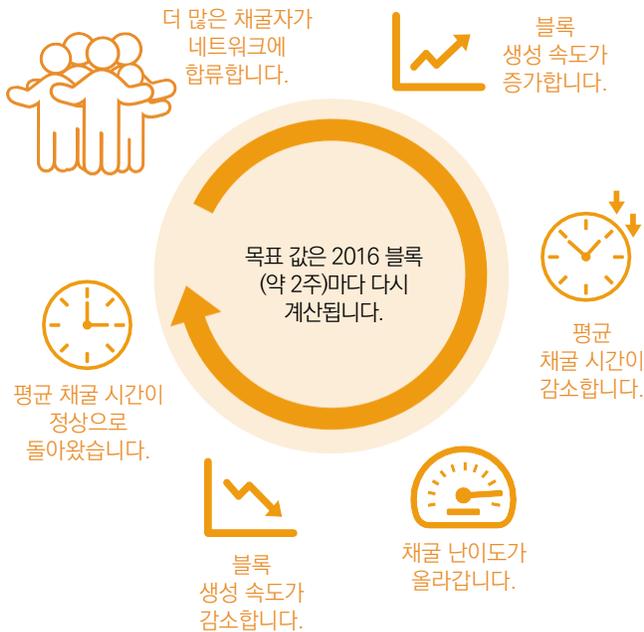


채굴자의 총 수입  
\$34,688,409.61

## 채굴 난이도

- 난이도는 **비트코인** 블록을 채굴하는 것이 얼마나 어려운지를 나타내는 척도입니다.
  - 또는 설정된 '목표 값' 보다 낮은 해시 값을 찾습니다.
- 난이도는 2016 블록마다 조정됩니다(약 2주마다).
  - 각 블록 사이의 평균 시간은 10분으로 유지됩니다.
- 난이도는 총 채굴력과 직접적인 관련이 있습니다.
  - 테라 해시/초(TH/s)로 추정됩니다. (테라 = 조).
    - 오늘날의 네트워크는 초당 수조 개의 해시를 계산할 수 있습니다.

- 난이도가 높을수록 동일한 수의 블록을 채굴할 수 있는 컴퓨팅 성능이 높아져 네트워크가 외부 공격으로부터 더 안전하게 보호됩니다.



## 8.5 무엇을 또는 누구를 조심해야 할까요?

**비트코인**은 전통적인 금융 시스템보다 훨씬 더 강력한 보호 기능을 제공할 수 있지만, 사기는 점점 더 정교해지고 있습니다. 예를 들어:

- 피싱.
  - 공격자는 피해자가 개인정보를 입력하도록 할 수 있습니다.
    - 비밀번호 변경을 유도한 후 개인정보를 도용합니다.
    - 개인 키를 알아내 비트코인을 훔칩니다.
    - 멀웨어 웹사이트를 방문하도록 유도하고 컴퓨터를 제어합니다.

- DNS 또는 브라우저 애드온 하이재킹.
  - 공격자는 합법적인 웹사이트를 하이재킹 합니다.
    - 사기 웹사이트로 변경합니다.
    - 그들은 이러한 가짜 사이트에 **개인 키**를 입력하도록 사용자를 속입니다.
- 해커는 두 휴대폰의 SIM 카드를 교환하고 모든 데이터를 훔칠 수 있습니다.
  - 사이버 범죄자는 모든 상황을 이용하려고 합니다. 기업과 보안 팀은 이를 막기 위해 고군분투하고 있습니다.

### 비트코인 공격

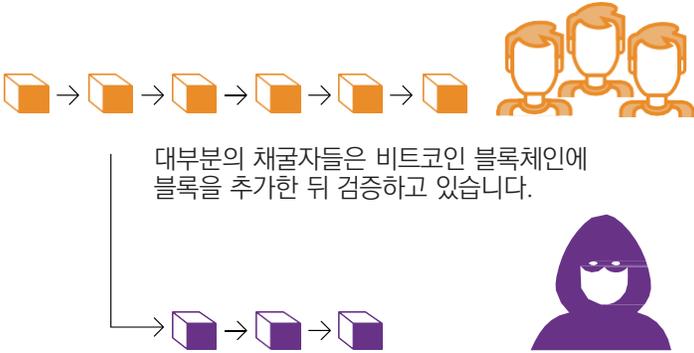


- 이러한 공격 중 어느 것도 **비트코인** 네트워크를 방해하지 못했습니다.
- **개인 키**가 안전한 장소에 남아 있는 경우.
  - 공격은 사실상 불가능 해집니다.
- 51%의 공격 확률은 매우 낮습니다.

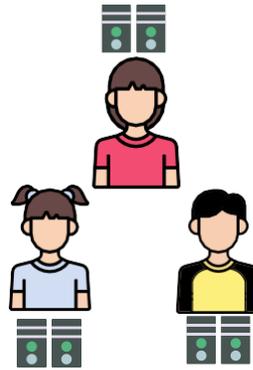
# 희소성, 비용, 가격 및 변동성

## 51% 공격이란 무엇일까요?

- 이를 달성하려면 에너지 및 컴퓨팅 파워가 필요합니다.



공격자는 개인적인 블록체인에 블록을 추가하고 비트코인 블록체인으로 전송하지 않습니다.

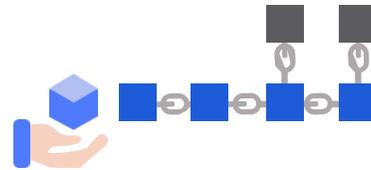


작업증명(POW) 기반 네트워크에는 새로운 블록을 추가하고 블록체인의 정보를 확인하는 여러 참여자(채굴 노드)가 있습니다.

채굴자들은 새로운 블록 보상을 받을 수 있는 권리를 얻기 위해 서로 경쟁합니다.

- 악의적인 채굴자는 네트워크 연산 능력의 50% 이상을 축적해야 합니다.

- 네트워크는 더 이상 분산되지 않고 해당 채굴자에 의해 제어 및 조작됩니다.
- 원래 체인 뒤에 연결된 새 체인이 생성됩니다.
  - 이것은 채굴자 중 일부가 자신의 블록을 추가하도록 속일 것입니다.
  - 체인을 쉽게 조작, 변경 할 수 있습니다.
  - 이중 지불 또는 거래 검열을 통해 돈을 훔칠 수 있습니다.



- 이러한 유형의 공격은 **비트코인**에서 발생한 적이 없습니다.







## 제 9장

# 비트코인의 현재와 미래

9.1 사용되는 에너지

9.2 혁신

- 소프트웨어 - 비트코인 코어
- 세그윗, 탭루트 및 슈노르 서명
- 타로

9.3 비트코인과 엘살바도르의 미래

9.4 수업 활동: 비트코인 시뮬레이터



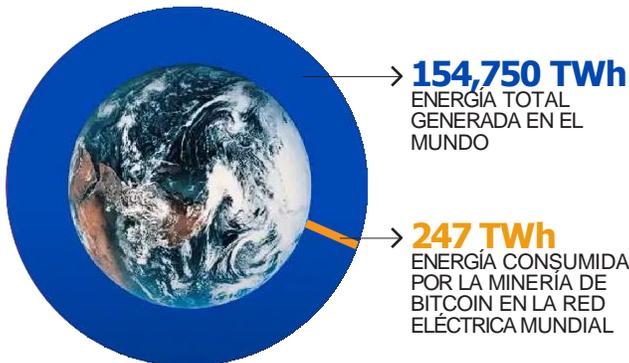
# 비트코인의 현재와 미래

## 9.1 사용되는 에너지

비트코인은 실제로 많은 에너지를 소모할까요?

수익을 증가시키려면:

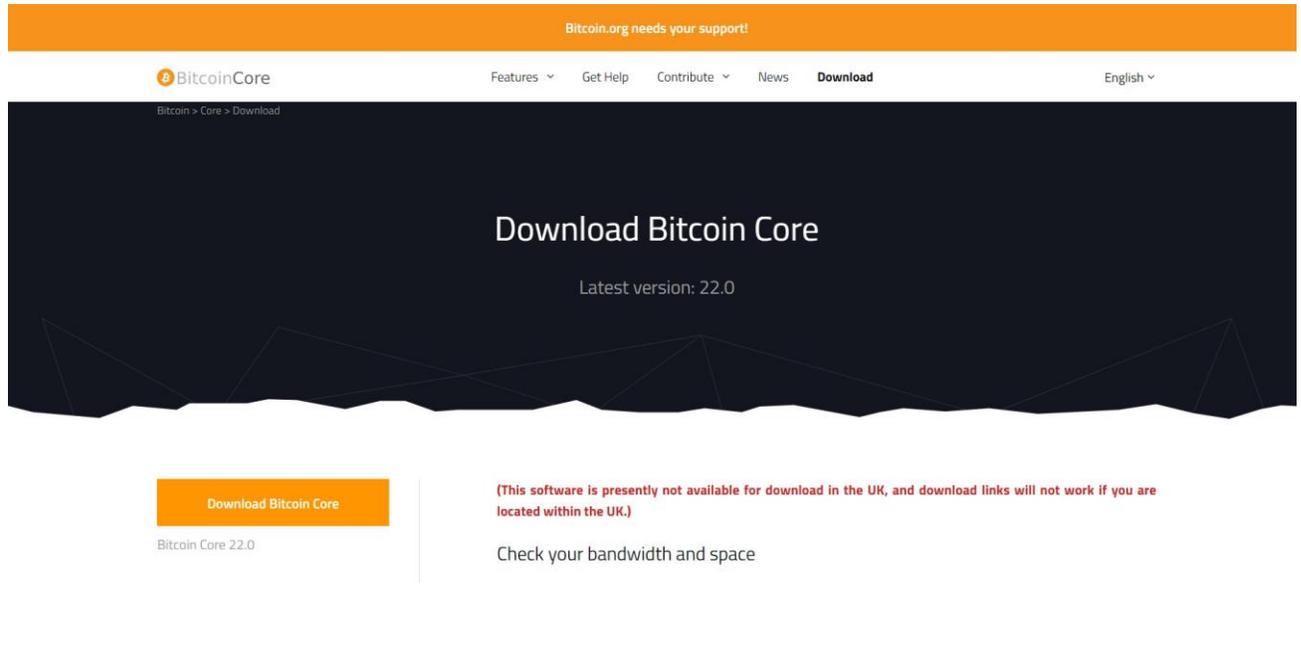
- 채굴자는 많은 수의 컴퓨터를 연결합니다.
  - **비트코인**을 얻을 확률을 높이기 위해 그렇게 합니다.
- 컴퓨터는 '복권'에 당첨되기 위해 거의 밤낮으로 일합니다.
  - 따라서 에너지 사용량이 상당히 높습니다.
- **비트코인** 채굴에 사용되는 기술은 나날이 친환경적으로 바뀌고 있습니다.
  - 지속 가능한 에너지의 채택은 2022년 4월에 59.5%로 증가했습니다.
- **비트코인** 해시레이트는 2021년 초에 비해 23% 증가했지만.
  - 비트코인 채굴의 에너지 사용량은 그 당시보다 25% 낮아졌습니다.
- 오늘날의 ASIC은 2009년 CPU보다 1000억 배 더 빠릅니다.
  - **비트코인**이 사용하는 에너지는 전 세계 에너지의 0.16%에 불과합니다.



## 9.2 혁신

### 소프트웨어 - 비트코인 코어

- 비트코인 코어(Bitcoin Core)는 사토시 나카모토가 만든 원본 소프트웨어입니다.
  - 동일한 프로그램을 실행하는 다른 사람들과 연결하도록 설계되었으며,
    - 서로 통신하는 컴퓨터 네트워크를 만듭니다.
  - 모든 사람이 동일한 규칙 집합으로 작동시키는데 목적이 있습니다.
    - 거래를 확인합니다.
    - 그리고 시스템의 보안과 탈중앙화에 기여합니다.
  - 다른 프로그램처럼 설치할 수 있습니다.
    - 전체 블록 체인의 사본을 다운로드하여 생성합니다.
    - 다른 컴퓨터로 거래를 전송하는 데 도움이 됩니다.
  - 인터넷에 접속할 수 있는 한 추가적인 권한이 필요하지 않습니다.
    - 자유롭게 다운로드하여 사용하세요.
    - **비트코인**을 다른 지갑으로 이체하거나 다른 사람에게서 받을 수 있습니다.
    - 블록의 생성을 검증할 수 있습니다.
    - 거래 내역과 각 **비트코인**의 소유자를 알 수 있습니다.
- 수십 명의 소프트웨어 및 암호화 전문가가 유지 관리 및 개선 작업을 수행합니다.
  - 소프트웨어 업데이트를 제안하는 사람은 업데이트를 구현하기 위해 대다수의 동의가 필요합니다.



### 오픈 소스코드

누구나 보고, 변경 사항을 제안하고, 수정하고, 적절하다고 생각하는 대로 배포할 수 있습니다. 식당에 가서 좋아하는 음식의 레시피(코드)를 보는 것과 비슷하지만 원하는 대로 만들고 원하는 재료를 추가하거나 빼서 정제할 수 있습니다.

### 세그윗, 탭루트 및 슈노르 서명

비트코인은 BIP(비트코인 개선 제안)를 통해 합의를 통해 개선되었습니다. 이것은 수년에 걸쳐 더 안전하고 효율적으로 만들었습니다.

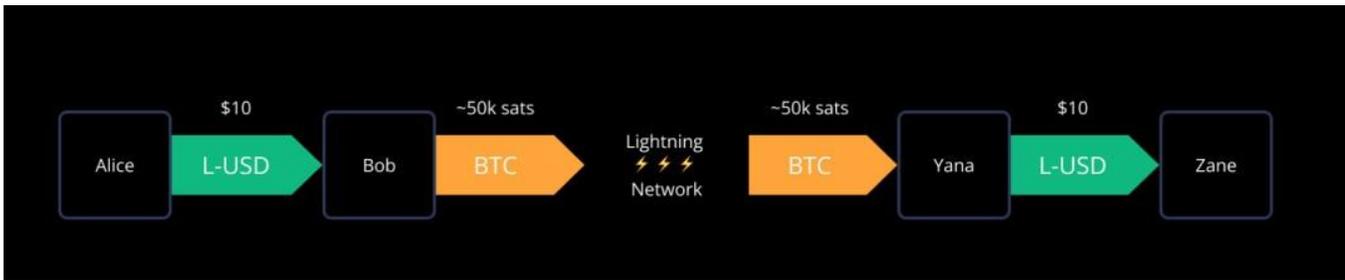
- 2017년에 구현된 소프트포크인 세그윗(SegWit).
  - 거래 서명의 일부를 변경하여 블록 크기 제한을 개선하였습니다.
  - 비트코인 거래의 처리 속도가 향상되었습니다.
  - 노드가 다음을 수행할 수 있는 프로토콜 약점을 수정했습니다.
    - 네트워크에서 거래 가변성 문제를 처리합니다.
    - 거래 가변성이란 공격자가 블록체인 내에서 거래의 해시를 수정하거나 변경할 수 있는 것입니다.
- 탭루트(Taproot)는 웹에서 개인 정보를 개선하고 익명성을 높이기 위해 만들어졌습니다.
  - 탭루트는 거래를 '위장'할 수 있습니다.
  - 거래 유효성 검사 시간을 줄입니다.
    - 비트코인이 지불 수단으로서 도움이 될 수 있습니다.
  - 거래 수수료를 크게 줄일 수 있습니다.

# 비트코인의 현재와 미래

- 슈노르(Schnorr) 서명으로 대체; 현재 ECDSA(타원 곡선 디지털 서명)를 대체합니다.
  - 복잡한 거래 내에서 여러 키를 통합하고 고유한 서명을 생성합니다.
  - 블록체인에서 스마트 계약을 간소화합니다.
  - 라이트닝 네트워크와 같은 레이어 2 지불 채널을 확장하는 데 도움이 됩니다.

## 타로(Taro)

- 새로운 타로 프로토콜의 목표는 **비트코인** 기술을 한 차원 높은 수준으로 끌어올리는 것입니다.
- 라이트닝 네트워크에서 스테이블코인 및 기타 자산을 발행할 수 있습니다.
- 모든 통화를 거의 무료로 즉시 다른 통화로 교환할 수 있습니다.



## 9.3 비트코인과 엘살바도르의 미래

- 비트코인의 독창성과 가능성은 주목을 받았습니다.
  - 투자자들에게 주목을 받았습니다.
  - 기업들에게 주목을 받았습니다.
    - 공기업과 사기업 모두 인플레이션과 구매력 감소라는 동일한 영향을 받습니다.
    - 그들은 대차 대조표를 강화하려고 합니다.
    - 그들은 큰 현금 보유고를 가지고 있습니다.
    - 그들은 비트코인을 장기적 가치 저장 수단으로 채택하고 있습니다.

- 엘살바도르는 미래에 전 세계적으로 엄청난 우위를 점하게 될 것입니다.
  - 비트코인을 법정화폐로 채택한 최초의 국가가 되었습니다.
    - 비트코인 비치는 이미 강력하고 튼튼한 프로젝트입니다. 지역 사회 내에서 순환 경제를 만들었습니다.
  - IMF와 세계은행은 이 결정에 반대 목소리를 냈습니다.
    - 한편, 엘살바도르는 계속해서 비트코인을 축적하고 있습니다.
- 그 다음 어떤 국가가 비트코인을 법정화폐로 채택할까요?
  - 더 빠르게 채택할 수록 더 큰 혜택을 볼 수 있습니다.











제 10장

# 최종 프로젝트

- 왜 비트코인 일까요?















추가

# 디지털 서명의 마법

- 공개 키 및 개인 키
  - 디지털 서명
  - 유효한 거래
- 

## 공개 키 및 개인 키

보안 문제를 이해하셨으므로 이제 지갑과 거래로 돌아가 보겠습니다.

가장 안전한 지갑은 다음을 제공합니다.

- '마스터 **개인 키**' 또는 '시드(Seed) 문구'
  - 무작위로 생성된 12~24단어의 목록입니다.
    - 어느 누구도 봐서는 안됩니다.
    - 모든 장치에서 사용자의 **비트코인**에 접근할 수 있는 고유 키입니다.
    - 각각의 **개인 키**를 생성하기 위한 도구로 사용됩니다.



- **개인 키**로 **공개 키**를 생성합니다.
- **공개 키**를 통해 거래에 **디지털 서명**을 할 수 있습니다.
- 거래에는 고유한 **디지털 서명**이 있습니다.
- 서명을 통해 **비트코인**을 특정 주소로 전송할 수 있습니다.

- Private Key = 개인 키
- Public Key = 공개 키
- Address = 주소
- Generate = 생성

## ● 개인 키

- 비밀번호와 유사하며 안전하게 보관해야 합니다.
- 지갑을 잃어버렸을 때 **비트코인**을 복구할 수 있습니다.
- 시드 문구가 존재하기 전에는 개인 키로 복구했습니다.
  - 개인 키는 완전히 무작위이며 1에서 115792089237316195423570985008687907852837564279074904382605163141518161494336 사이의 매우 큰 숫자입니다.
- 모든 개인 키는 16진수로 변환됩니다.
  - 16진수는 0-9, A-F(여기서 A=10, B=11 등)의 숫자입니다.
- 동일한 개인 키를 두 번 생성하는 것은 사실상 불가능합니다.

다음 링크에서 개인 키 생성을 연습해보세요.

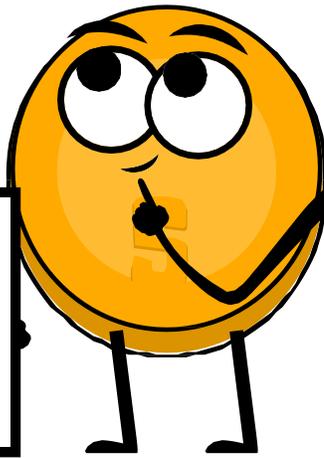
Learn Me a Bitcoin



## ● 공개 키

- 개인 키로 공개 키를 생성합니다.
  - 암호학을 사용하여 공개 키를 생성합니다.
- 단방향이기 때문에 공개 키로 개인 키를 알아낼 수 없습니다.

공개 키를  
생성해보세요.



개인 키 예시



458717487902476942636812561412180509625  
40558073528157656117113257366684871118



281655566938916207734774775745594237527  
921072031892196308809886888062824700225

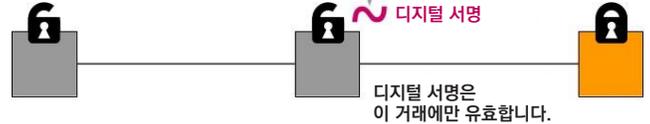
공개 키는 개인 키에서 생성됩니다.

## 디지털 서명

- 개인 키를 공개하지 않지만 소유권을 증명하는 데 사용됩니다.
- 개인 키와 거래에 포함된 정보로부터 생성됩니다.
- 고유하고 반복할 수 없으며 위조가 불가능합니다.
- 전송할 비트코인의 잠금(UTXO)을 해제할 때 사용합니다.



개인 키를 소유하고  
있음을 증명하지만  
공개해도 되는 숫자를  
생성합니다.



## ⚠️ 잠시 생각해보기.

해커가 비트코인 거래를 가로채면 개인 키를 알아내고 자금을 훔칠 수 있다고 생각하세요? 다시 말해서, 악의적인 사람이 비트코인을 공개되어 있는 보낼 주소에 접근한다면 비트코인을 자신의 금고로 보낼 수 있다고 생각하세요?

## 유효한 거래

디지털 서명의 목적은 공개 키의 소유권을 증명할 수 있도록 하는 것입니다.

- 채굴자는 비트코인을 보내는 사람의 공개 키로 서명을 확인합니다.
- 암호화 승인은 다음과 같습니다.
  - 거래가 조금이라도 수정된 경우 서명의 해시도 자동으로 변경되어 해당 거래는 위조로 판명 납니다.
  - 거부해야 하는 거래를 찾는 것은 매우 쉽습니다.





## 출처

1. The Free Silver Movement, Scott Wolla, Federal Reserve Bank of St. Louis. <https://www.stlouisfed.org/-/media/project/frbstl/stlouisfed/education/lessons/pdf/the-free-silver-movement-and-inflation.pdf>,
2. Video -¿Qué es el Dinero? MagicMarkers. TV, Colombia. <https://youtu.be/2yCIKkq8gKA>
3. <https://www.philadelphiafed.org/-/media/frbp/assets/institutional/education/lesson-plans/functions-and-characteristics-of-money-lesson.pdf>, Functions and Characteristics of Money, Chapter 3, Segment 301, Federal Reserve Bank of Philadelphia
4. <https://www.philadelphiafed.org/-/media/frbp/assets/institutional/education/lesson-plans/money-grades-6-8.pdf>, “Why Money”, Bonnie T. Meszaros, Federal Reserve Bank of Philadelphia
5. <https://www.kansascityfed.org/documents/2856/teachingresources-Lessonplangr9-12.pdf> Federal Reserve Bank of Kansas
6. ¡Historia de 1870 a 1971 en 10 minutos!, Robert Breedlove. Para la sección de 1870-1914: <https://www.forbes.com/sites/nathanlewis/2013/01/03/the-1870-1914-gold-standard-the-most-perfect-one-ever-created/?sh=5e0ab9864a6a>
7. Economía Desde Cero: Dinero-Video, <https://youtu.be/zcYw8a4RJC4>, Canal Encuentro, Argentina.
8. <https://www.kansascityfed.org/documents/2856/teachingresources-Lessonplangr9-12.pdf>, Activity 5, Auction, Federal Reserve Bank of Kansas.
9. Video -Qué es la Inflación, <https://youtu.be/gkDQGribCfc>](<https://youtu.be/gkDQGribCfc>), Banco de la República de Colombia
10. Video - ¿Cómo Nos Vigilan en Internet?, Magic Markers <https://youtu.be/-sWgOuFlaws>](<https://youtu.be/-sWgOuFlaws>,
11. McDonalds Menú Picture 1973. <https://muddyrivernews.com/opinion/daily-dirt-where-were-you-in-72-or-once-upon-a-time-when-a-big-mac-was-65-cents/20220323091958/>
12. McDonalds Menú 2022. McDonalds El Salvador, Twitter.
13. Causas de la Inflación, Video, Banco de la República, Colombia.

14. Declining purchasing power of the US dollar strengthens Bitcoin, <https://cryptopotato.com/is-there-a-pattern-between-usd-dow-jones-and-bitcoin/>, Toju Ometoruwa.
15. Ejemplo de Estado de Cuentas, [https://www.ejemplode.com/59-finanzas/4274-ejemplo\\_de\\_estado\\_de\\_cuenta.html](https://www.ejemplode.com/59-finanzas/4274-ejemplo_de_estado_de_cuenta.html)
16. Video –MagicMarkers.TV,Colombia. ¿Qué es Bitcoin y Cómo Funciona?, <https://youtu.be/S2HxMK7iO4c>,
17. Nodos Completos –Visualización de una Transacción <http://beautifuldata.net/2015/01/querying-the-bitcoin-blockchain-with-r/>
18. Video –(<https://youtu.be/ID8WQbS8-T8>), \*Que es La Red Relámpago\*, Whiteboard Crypto en Español
19. Bitcoin en Números, Nick Carter, Bitcoin Demystified.
20. Bitcoin, Will the Price of Bitcoin Rise or Fall?, Capital.com Research Team, 08:00 (UTC), 31 March 2022. <https://capital.com/de/bitcoin-prognose>,
21. U.S. dollar inflation visualized at the top versus bitcoin's deflation at the bottom: Lark Davis @TheCryptoLark.
22. <https://www.bitcoincharts.com>
23. <https://www.blockchaincenter.net/en/bitcoin-rainbow-chart/>
24. <https://www.blockchain.com/charts/miners-revenue>





