Coming Soon… !!

warning - warning - warning - warning - warning - warning - warning - warning - warning - warning

Bitcoin Seoul Hackathon

brought to you by:

Seoul Bitcoin

ORAKLE

nonce

sponsors and partners:

BitcoinSeoul

Human Rights Foundation

UTREEXO

BITCOIN DEV KIT

Decenter

2024 비트코인 서울 해커톤 워크샵

(2024 Bitcoin Seoul Hackathon Workshop)

임혜수 (Hyesoo Lim or Hesus Lim)

Chaincode Labs FOSS participant

Orakle Bitcoin Team Lead

Summer Bitcoin candidate

Bitcoin Dev Newbie

In Orakle Bitcoin Team

- 비트코인백서, 라이트닝네트워크백서 분석 및 구현체 변경사항 추적
- 비트코인 기반 자산발행 레이어 생태계 연구
- 수학적 접근법에 관한 연구, **ex)** 비트코인내 공리계에 관한 분석

Vision

- 국내 비트코인 코어 개발자 생태계 확장 및 기여자 양성
- 비트코인 기술, 역사, 문화적 지식을 대중에게 올바르게 전달

Objectives

- 국내, 국외 비트코인 코어 기여 생태계 적극교류추진 **(SeoulBitcoinMeetup, Chaincode Labs)**
- 컨퍼런스 오거나이징 지원, 비트코인 개발 학습자료 번역

Seoul Bitcoin Meetup

chaincode

bitcoinSeoul 2024

Contents

왜 비트코인인가(Why Bitcoin)?

Bitcoin is for all of us

Bitcoin CoreDev reflections 2023-2024

February 20, 2024

For a fifth year running, regular Bitcoin Core contributors received a survey to surface priorities and ensure that people feel that they can contribute effectively. Below is a summary of the results in a format similar to last year's survey.

https://adamjonas.com/

https://bitcoindevs.xyz/bitcoin-core

by Adam Jonas

February 20, 2024

CATEGORIES

bitcoin, coredev, retro

LEARNING @ CHAINCODE LABS

Bitcoin and Lightning Protocol Development Education

활동 요약

- 1323개의 PR이 마스터 브랜치 열림.
- 843개의 PR이 마스터에 병합.
- 93명의 고유한 PR 작성자 중 24명은 처음으로 PR을 작성.
- 285명의 정기 리뷰어와 355명의 처음 리뷰어가 있었음.
- 29014개의 리뷰 코멘트가 작성되었음.

회고

- 2023년에 잘된 점: 우선순위 프로젝트, BIP324, AssumeUTXO 등.
- 2023년에 실망스러웠던 점: 비공헌자의 GitHub 캠페인, 진행 속도 등.
- 2024년 Bitcoin Core에서 희망하는 바: Silent payments, Package relay 등.
- 2024년에 개인적으로 이루고 싶은 목표: 멘토링, 클러스터 메모리 풀 등.
- 프로세스/프로젝트 개선을 위한 변경사항: 더 나은 관리 도구, 신뢰할 수 있는 CI 등.
- 기여자들과의 연결감 및 협업 방안: 멘토링, 지식 공유를 위한 가상 환경 등.
- 다른 기여자를 멘토링할 의사: 관심 있는 사람이 80%.
- 더 많이 배우고 싶은 주제: 메모리 풀, 암호화, P2P 등.
- 다음 CoreDev 행사에서 논의하고 싶은 주제: 지갑, 클러스터 메모리 풀, Silent payments 등. - 추가 의견: PR 닫는 가이드라인, 유지자들의 명확한 피드백 요청 등.

비트코인 코어 생태계의 현재는?(Bitcoin Core Ecosystem?)

A. 라이트닝 네트워크 중심 비트코인 사용의 현재 (**“What is happening with Bitcoin?”**)

B. 현재 관점에서 비트코인 백서 읽기 (**“What was happening with Bitcoin ?”**)

C. 비트코인의 미래 (**“What is going to be being Bitcoin in the future?”**)

A. 라이트닝 네트워크 중심 비트코인 사용의 현재_세 가지 거래유형 예시를 중심으로

“What is happening with Bitcoin?”

(한방정리) ⚡빛보다 빠른⚡비트코인 라이트닝 결제해보고 싶다고? | 트레블 룰 | 해외거래소 - 네딸바 NL daughter's daddy

> “What is needed is an electronic payment system based on cryptographic proof instead of trust, allowing any two willing parties to transact directly with each other without the need for a trusted third party.”
>
> ”필요한 것은 신뢰 대신 암호화 증명에 기반한 전자 결제 시스템으로, 신뢰할 수 있는 제3자가 필요 없이 자발적인 두 당사자가 서로 직접 거래할 수 있게 하는 것입니다.”
>
> - 1. Introduction, Bitcoin WhitePaper

‘즉각적인 결제(Instant Payment)’

세 가지 유형의 즉각적인 비트코인 결제 (Three type of Instant Bitcoin Payment Examples)

a. 오프라인상 개인간 직접거래 (Off-line P2P)

b. 온라인기반 개인간 직접거래 (On-line P2P)

c. 온라인서비스상 개인간 소액 직접거래(On-line P2P)

- 매개교환의 수단으로써의 기능(medium of exchange)

- 검열저항 환경에서의 마이크로페이먼트
(Micropayment on censorship-resistant)

세 가지 유형의 즉각적인 비트코인 결제 (Three type of Instant Bitcoin Payment Examples)

a. 오프라인상 개인간 직접거래 (Off-line P2P)

b. 온라인기반 개인간 직접거래 (On-line P2P)

c. 온라인서비스상 개인간 소액 직접거래(On-line P2P)

- 매개교환의 수단으로써의 기능(medium of exchange)

- 검열저항 환경에서의 마이크로페이먼트
(Micropayment on censorship-resistant)

세 가지 유형의 즉각적인 비트코인 결제 (Three type of Instant Bitcoin Payment Examples)

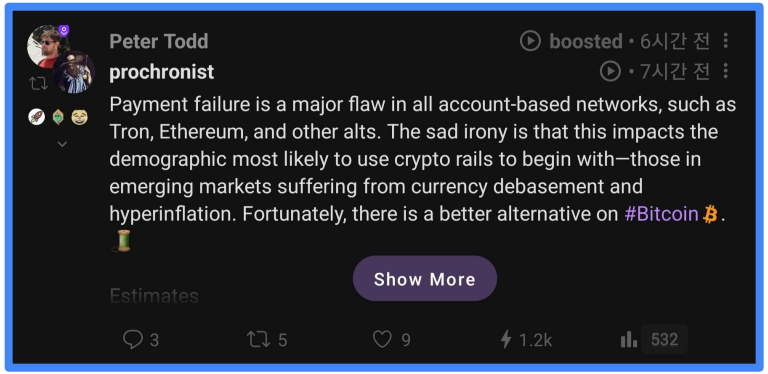
a. 오프라인상 개인간 직접거래 (Off-line P2P)

b. 온라인기반 개인간 직접거래 (On-line P2P)

c. 온라인서비스상 개인간 소액 직접거래(On-line P2P)

- 매개교환의 수단으로써의 기능**(medium of exchange)**

- 검열저항 환경에서의 마이크로페이먼트
  (Micropayment on censorship-resistant)



세 가지 유형의 즉각적인 비트코인 결제 (Three type of Instant Bitcoin Payment Examples)

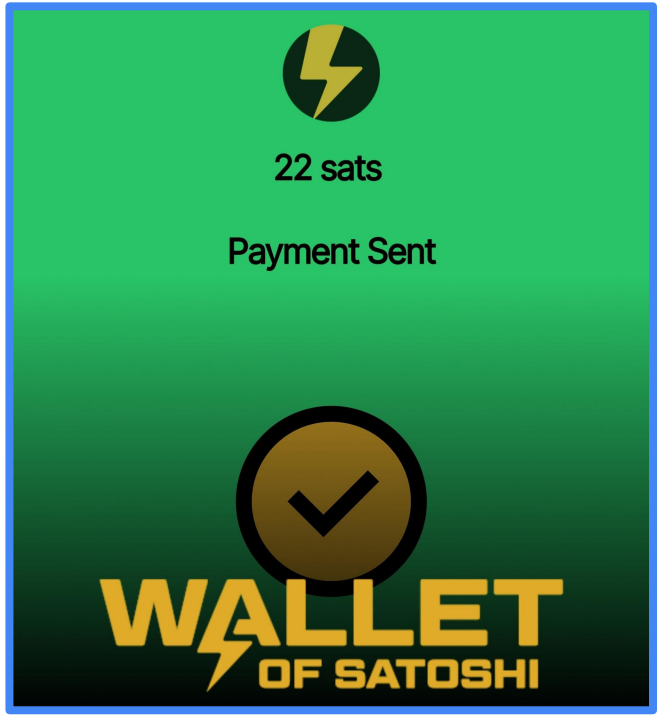
a. 오프라인상 개인간 직접거래 (Off-line P2P)

b. 온라인기반 개인간 직접거래 (On-line P2P)

c. 온라인서비스상 개인간 소액 직접거래(On-line P2P)

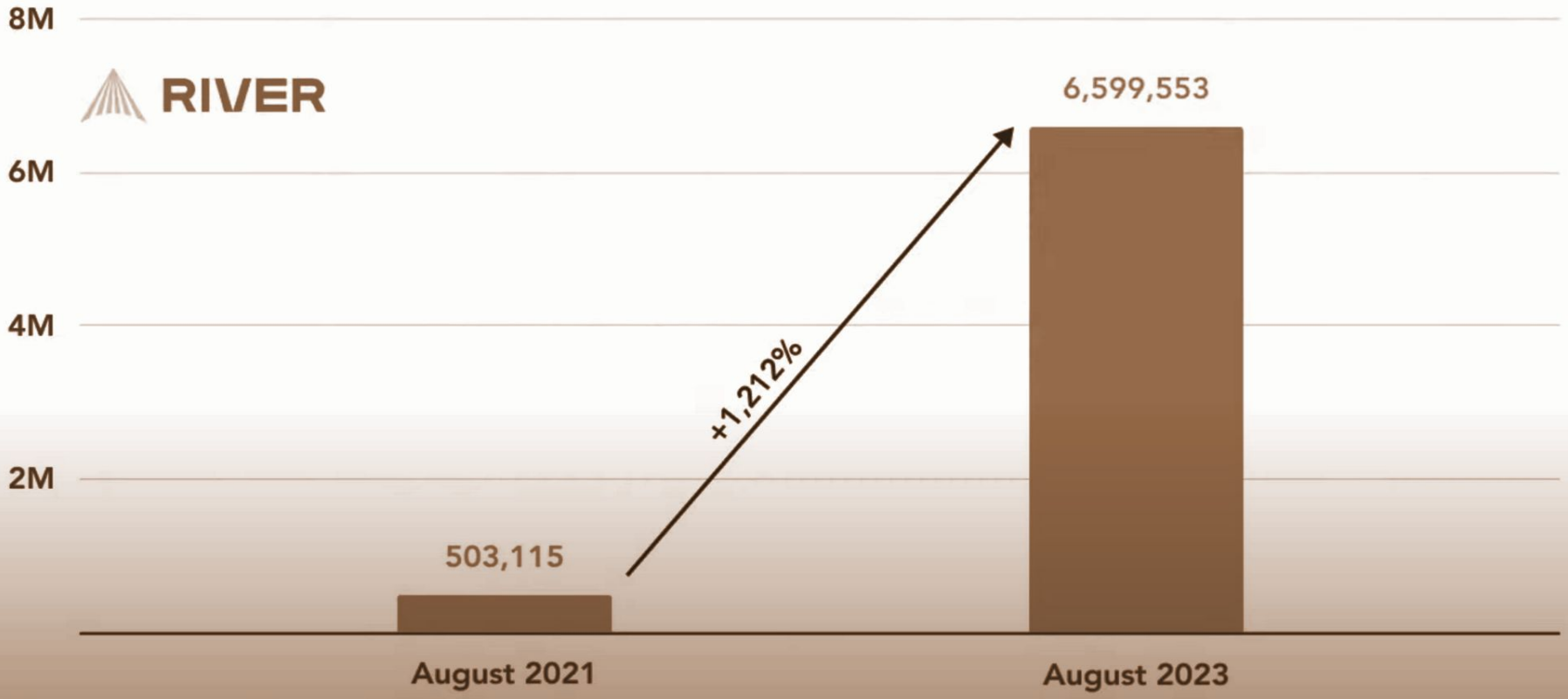
- 매개교환의 수단으로써의 기능(medium of exchange)

- 검열저항 환경에서의 마이크로페이먼트
(Micropayment on censorship-resistant)



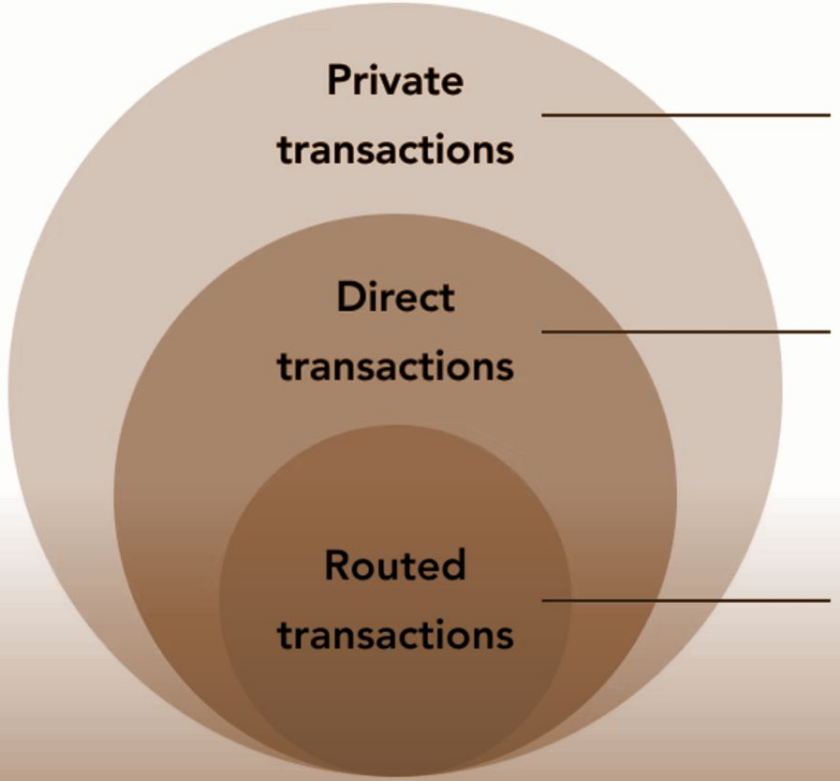
Estimated Growth in Routed Lightning Transactions

Lower bound estimates as private transactions are excluded



Methodology explained in River's 2023 Lightning Report

Lightning Transaction Categories Explained



Private transactions

Transactions between private nodes or over private channels. Could be many times more than routed transactions.

Quantity unknown

Direct transactions

Transactions between only two nodes. Could be bigger than routed transactions. Data often not shared for privacy reasons.

Quantity undisclosed

Routed transactions

Transactions that involve more than two nodes. Show up in transaction routing logs of more nodes.

6,599,553 in August 2023

Methodology explained in River's 2023 Lightning Report

RIVER

블록사이즈워 - 세그윗 (탈중앙화), 탭루트 업그레이드(프라이버시) 와 같은 사상적, 철학적, 정치적 갈등 및 다양한 논쟁 속에서

비트코인 코어 개발 커뮤니티 중심 **‘일반적인 거래(Casual Transaction)’를 위한**

‘즉각적인 결제(Instant Payment)’에 집중하며 지속적인 성장과 발전

B. 현재 관점에서 비트코인 백서 읽기_사토시의 프로토콜 디자인 의도 및 초기 구현에 대한

디자인변경 연구

문화(cypherpunk), 기술(cryptography based tech)

About ‘cypherpunk’ and ‘Block Size War’

데이비드 차움(David Chaum)

필 짐머만(Phil Zimmermann)

에릭 휴즈(Eric Hughes)

아담 백(Adam Back)

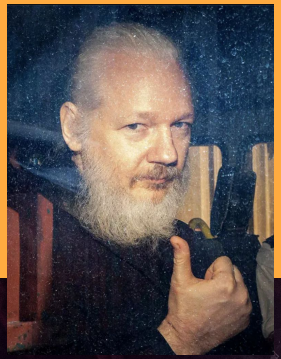
웨이 다이(Wei Dai)

닉 재보(Nick Szabo)

사토시 나카모토
(Satoshi Nakamoto)

할 피니(Hal Finney)

티모시 메이(Timothy May)



Q. 사이퍼펑크운동은 현재 진행형인가?

From: tcmay@netcom.com (Timothy C. May)
Subject: The Crypto Anarchist Manifesto
Date: Sun, 22 Nov 92 12:11:24 PST

Cypherpunks of the World,

Several of you at the "physical Cypherpunks" gathering yesterday in Silicon Valley requested that more of the material passed out in meetings be available electronically to the entire readership of the Cypherpunks list, spooks, eavesdroppers, and all. <Gulp>

Here's the "Crypto Anarchist Manifesto" I read at the September 1992 founding meeting. It dates back to mid-1988 and was distributed to some like-minded techno-anarchists at the "Crypto '88" conference and then again at the "Hackers Conference" that year. I later gave talks at Hackers on this in 1989 and 1990.

There are a few things I'd change, but for historical reasons I'll just leave it as is. Some of the terms may be unfamiliar to you...I hope the Crypto Glossary I just distributed will help.

(This should explain all those cryptic terms in my .signature!)

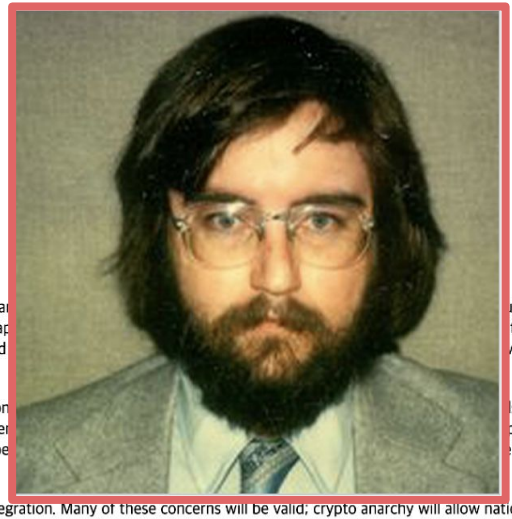
--Tim May

.....

The Crypto Anarchist Manifesto

Timothy C. May <tcmay@netcom.com>

A specter is haunting the modern world, the specter of crypto anarchy.



Computer technology is on the verge of providing the ability for individuals and groups to communicate and interact with each other in a totally anonymous manner. Two persons may exchar t ever knowing the True Name, or legal identity, of the other. Interactions over networks will be untraceable, via extensive re- routing of encrypted packets and tamper-proof boxes which implement cryptograp tions will be of central importance, far more important in dealings than even the credit ratings of today. These developments will alter completely the nature of government regulation, the ability to tax and will even alter the nature of trust and reputation.

The technology for this revolution--and it surely will be both a social and economic revolution--has existed in theory for the past decade. The methods are based upon public-key encryption s for interaction, authentication, and verification. The focus has until now been on academic conferences in Europe and the U.S., conferences monitored closely by the National Security Agency. But only recer peed to make the ideas practically realizable. And the next ten years will bring enough additional speed to make the ideas economically feasible and essentially unstoppable. High-speed networks, ISDN, tampe rsonal computers, and encryption chips now under development will be some of the enabling technologies.

The State will of course try to slow or halt the spread of this technology, citing national security concerns, use of the technology by drug dealers and tax evaders, and fears of societal disintegration. Many of these concerns will be valid; crypto anarchy will allow national secrets to be trade freely and will allow illicit and stolen materials to be traded. An anonymous computerized market will even make possible abhorrent markets for assassinations and extortion. Various criminal and foreign elements will be active users of CryptoNet. But this will not halt the spread of crypto anarchy.

Just as the technology of printing altered and reduced the power of medieval guilds and the social power structure, so too will cryptologic methods fundamentally alter the nature of corporations and of government interference in economic transactions. Combined with emerging information markets, crypto anarchy will create a liquid market for any and all material which can be put into words and pictures. And just as a seemingly minor invention like barbed wire made possible the fencing-off of vast ranches and farms, thus altering forever the concepts of land and property rights in the frontier West, so too will the seemingly minor discovery out of an arcane branch of mathematics come to be the wire clippers which dismantle the barbed wire around intellectual property.

Arise, you have nothing to lose but your barbed wire fences!

--

```
.....................................................................
Timothy C. May          | Crypto Anarchy: encryption, digital money,
tcmay@netcom.com        | anonymous networks, digital pseudonyms, zero
408-688-5409            | knowledge, reputations, information markets,
W.A.S.T.E.: Aptos, CA   | black markets, collapse of governments.
Higher Power: 2^756839 | PGP Public Key: by arrangement.
```

Back to activism.net/cypherpunk/

에릭 휴즈의 사이퍼펑크 선언중,

> “ 프라이버시는 전자 시대에서 열린 사회를 위해 필수적이다. 프라이버시는 비밀과 다르다. 프라이버시는 세상의 모든 사람들이 알게 되는 것을 원하지 않는 것이고, 비밀은 어느 누구도 알지 못하게 하는 것이다. 프라이버시는 자신에 대해 선택적으로 세상에 드러낼 수 있는 힘이다 “

개인권리보호와 사회적연대를 증진하기 위한 목적의 암호학, 무정부주의적 정신을 기반의 사이퍼펑크 문화의 연속

About ‘cypherpunk’ and ‘Block Size War’

Background of ‘Block Size War’

2008.5
웨이다이 메일링

2008.10
비트코인 백서 공개

2009.1
비트코인 제네시스블록

2009.1
첫번째 TX(사토시 → 할피니) 생성

2015
컬러드코인
옵리턴전쟁

2015
세그윗 제안
by Peter Wulle

2015
이더리움 백서 공

2015
BitcoinXT등장
(블록사이즈전
작)

2015
크레이그 라이트 등장

2016.1
라이트닝 네트워크 백서 공개

2016.6
더다오해

2023.12

Bitcoin Genesis Block

Raw Hex Version

```
00000000   01 00 00 00 00 00 00 00   00 00 00 00 00 00 00 00   ................
00000010   00 00 00 00 00 00 00 00   00 00 00 00 00 00 00 00   ................
00000020   00 00 00 00 3B A3 ED FD   7A 7B 12 B2 7A C7 2C 3E   ....;£íýz{.²zÇ,>
00000030   67 76 8F 61 7F C8 1B C3   88 8A 51 32 3A 9F B8 AA   gv.a.È.Ã^ŠQ2:Ÿ¸ª
00000040   4B 1E 5E 4A 29 AB 5F 49   FF FF 00 1D 1D AC 2B 7C   K.^J)«_Iÿÿ...¬+|
00000050   01 01 00 00 00 01 00 00   00 00 00 00 00 00 00 00   ................
00000060   00 00 00 00 00 00 00 00   00 00 00 00 00 00 00 00   ................
00000070   00 00 00 00 00 00 FF FF   FF FF 4D 04 FF FF 00 1D   ......ÿÿÿÿM.ÿÿ..
00000080   01 04 45 54 68 65 20 54   69 6D 65 73 20 30 33 2F   ..EThe Times 03/
00000090   4A 61 6E 2F 32 30 30 39   20 43 68 61 6E 63 65 6C   Jan/2009 Chancel
000000A0   6C 6F 72 20 6F 6E 20 62   72 69 6E 6B 20 6F 66 20   lor on brink of
000000B0   73 65 63 6F 6E 64 20 62   61 69 6C 6F 75 74 20 66   second bailout f
000000C0   6F 72 20 62 61 6E 6B 73   FF FF FF FF 01 00 F2 05   or banksÿÿÿÿ..ò.
000000D0   2A 01 00 00 00 43 41 04   67 8A FD B0 FE 55 48 27   *....CA.gŠý°þUH'
000000E0   19 67 F1 A6 71 30 B7 10   5C D6 A8 28 E0 39 09 A6   .gñ¦q0·.\Ö¨(à9.¦
000000F0   79 62 E0 EA 1F 61 DE B6   49 F6 BC 3F 4C EF 38 C4   ybàê.aÞ¶Iö¼?Lï8Ä
00000100   F3 55 04 E5 1E C1 12 DE   5C 38 4D F7 BA 0B 8D 57   óU.å.Á.Þ\8M÷º..W
00000110   8A 4C 70 2B 6B F1 1D 5F   AC 00 00 00 00            ŠLp+kñ._¬....
```

commons.wikimedia.org/wiki

2008.10
비트코인 백서 공개

2009.1
첫번째 TX(사토시 → 할피니) 생성

2009.1
비트코인 제네시스블록

2008.5
웨이다이 메일링

2015
세그윗 제안
by Peter Wulle

2015
컬러드코인
옵리턴전쟁

2015
이더리움 백

2015
BitcoinXT등
(블록사이즈
작)

2015
크레이그 라이트 등장

2016.1
라이트닝 네트워크 백서 공개

2016.6
더다

2008.10
비트코인 백서 공개

2009.1
첫번째 TX(사토시 → 할피니) 생성

2009.1
비트코인 제네시스블록

2008.5
웨이다이 메일링

2015
세그윗 제안
by Peter Wulle

2015
컬러드코인
옵리턴전쟁

2015
이더리움 백서 공개

2015
BitcoinXT등장
(블록사이즈전쟁시작)

2015
크레이그 라이트 등장

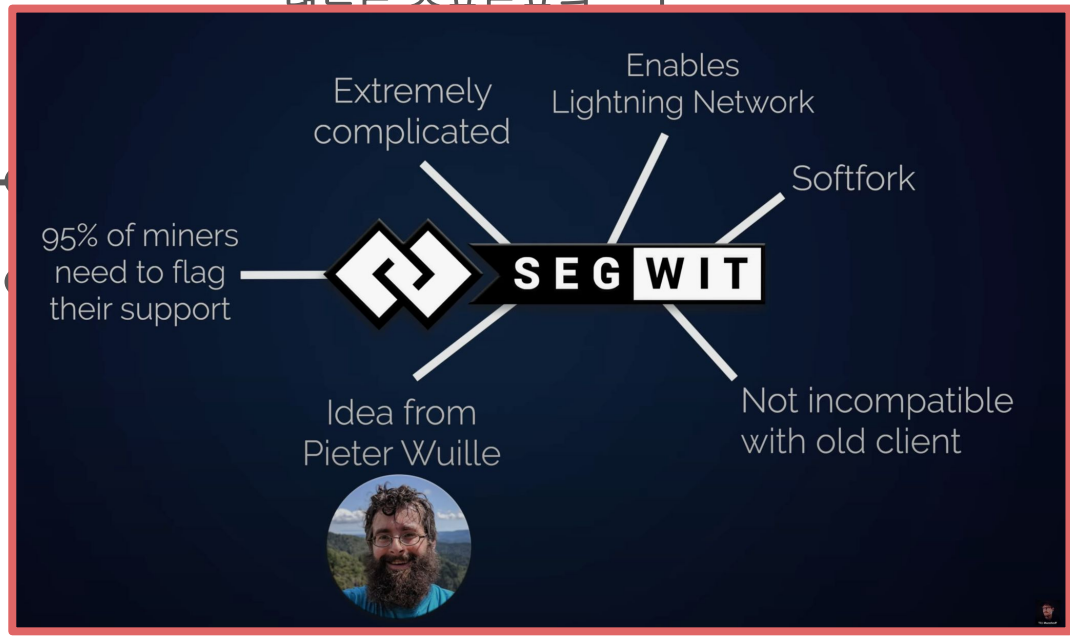
2016.1
라이트닝 네트워크 백서 공개

2016.6
더다오해킹

2017
세그윗 소프트포크,
라이트닝 네트워크 가동

2021.11
탭루트 소프트포크

2023.12
오디널스 검열 논쟁 by Luke



Wrap it up.

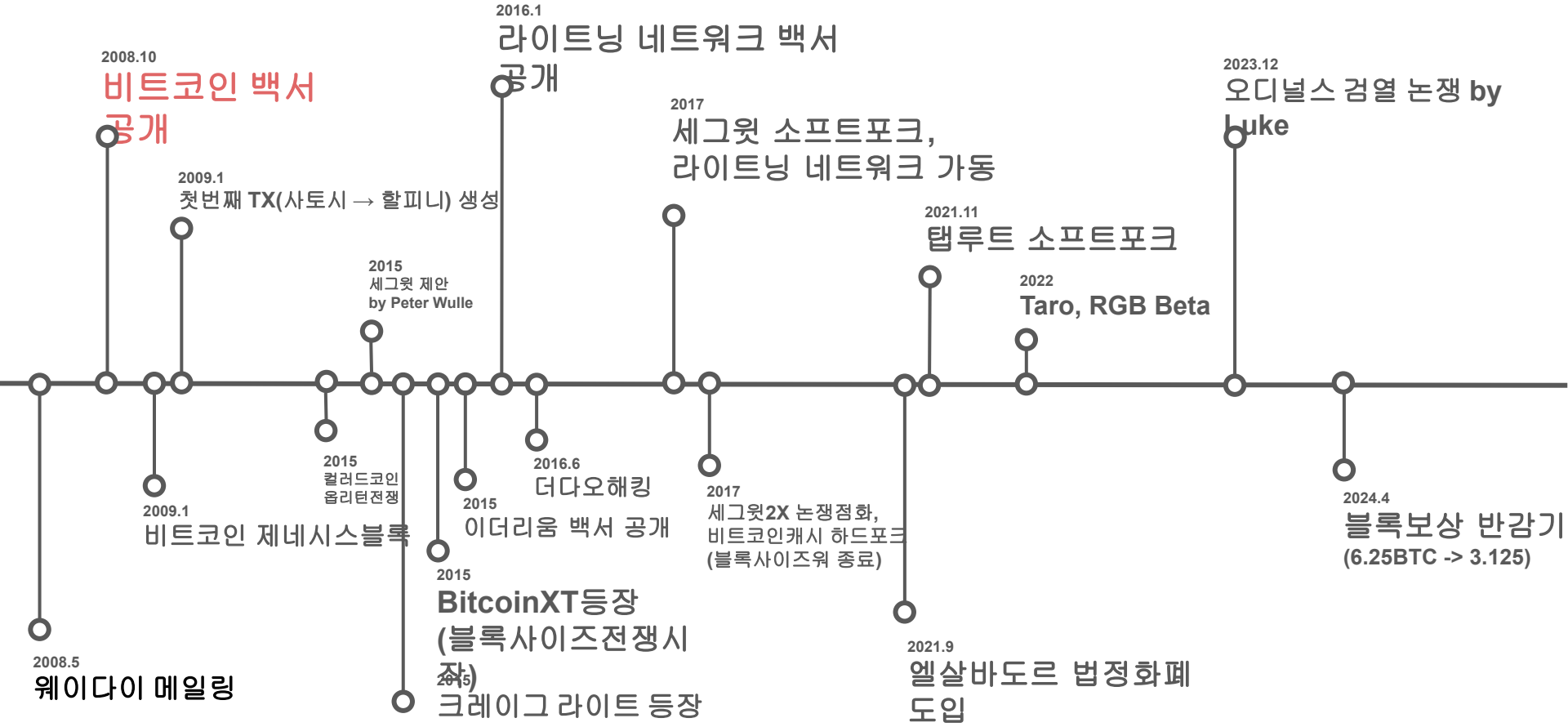
두 세력의 극단의 갈등과 대립 속에서도 ‘프라이버시’에 대한 공감대는 유지되었다 !

About ‘Technology’

1. 프로토콜 규칙 변경, 2. Tx 구조 변경 (Segwit) + HTLC, 3. 탭루드 업그레이드 (프라이버시강화)

"What was happening with Bitcoin ?"

그래서, 비트코인 기술발전의 흐름상 프라이버시에 관한 어떤 논의와 구현내용이 있었는가?



"What was happening with Bitcoin?"

그래서, 비트코인 기술발전의 흐름에서 프라이버시에 관한 공감대를 중심으로 어떠한 프로토콜 변경사항이 있었는가?

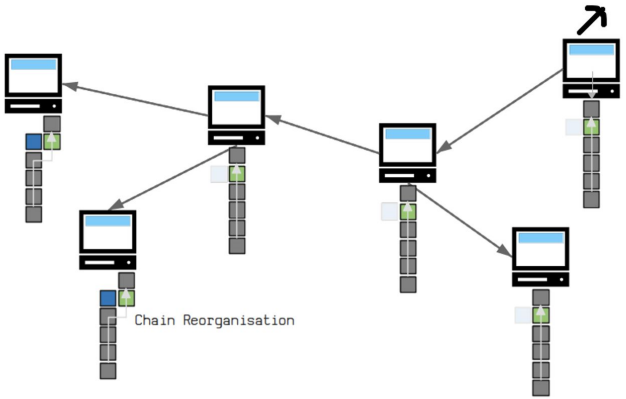
- 빅블로커vs스몰블로커(win), 스몰블록 세그윗소프트포크 논점 중심의 프로토콜 규칙 변경

오펀블록(Orphan Block)에 대한 용어가 더이상 사용되지 않고,

‘Stale Block’이라는 용어를 사용하며 1 stale block 을 허용하여 Reorg 에 관한 프로토콜 규칙으로 최종 변경됨

▼ Chain Reorganisation

Deactivating and activating blocks to adopt a new longest chain.



A chain reorganisation (or “reorg”) takes place when your node receives blocks that are part of a new longest chain. Your node will *deactivate* blocks in its old longest chain in favour of the blocks that build the **new longest chain**.

This process allows individual nodes across the network to **agree on the same version of the blockchain**, because the globally accepted view of the blockchain will always be the one with the longest chain of blocks*.

- It’s technically the chain with the most amount of *work*, but most number of blocks is usually the same thing.

비트코인 백서 읽기 - 사토시의 디자인 의도 및 이후 디자인 변경사항 주요 연구결과,

- 사토시의 디자인의도와 현재 비트코인 기술커뮤니티의 발전방향의 흐름과 프로토콜 변경의 핵심 지식 획득
- 네트워크 규칙 변경사항, 정직한노드의 행동에 관한 프로토콜 디자인 철학

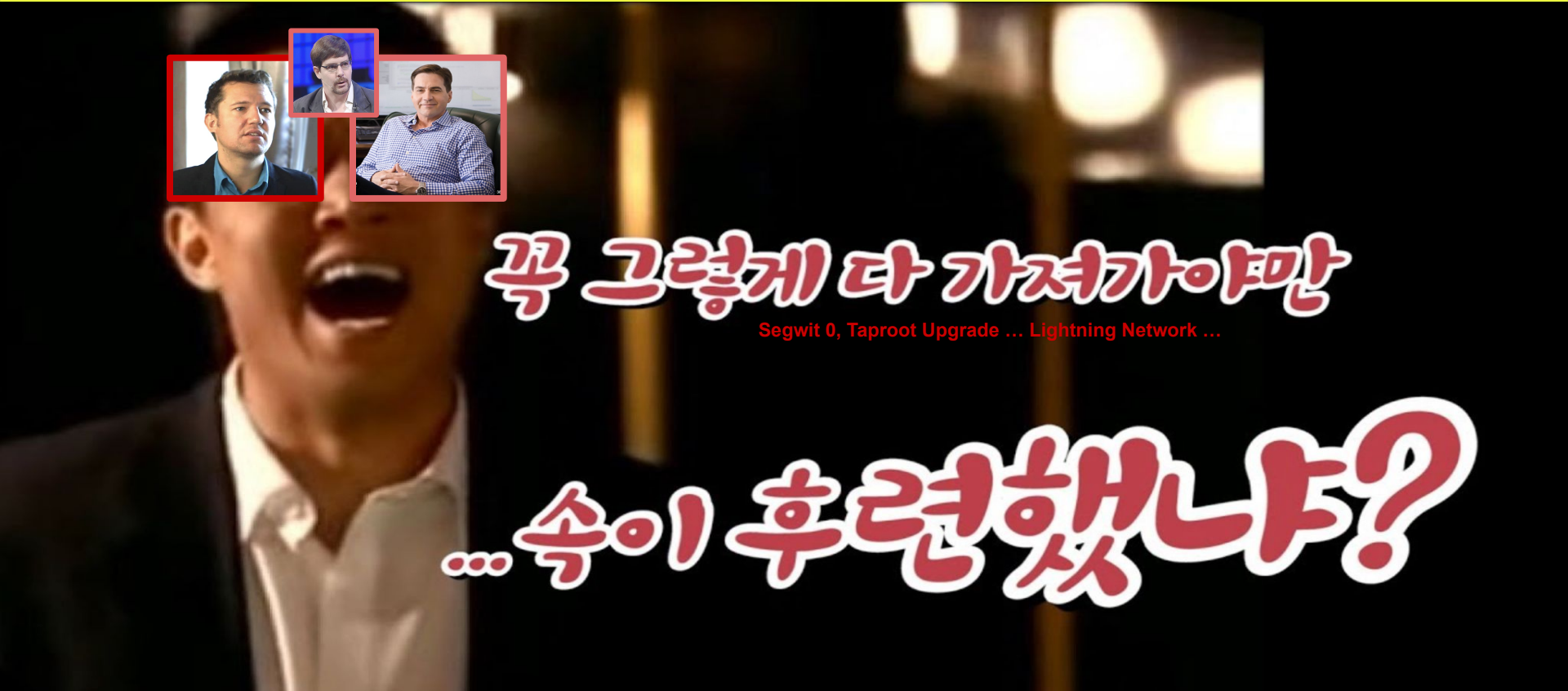
하지만, 프로토콜의 확장성의 관점에서 현재 **Stale Block = 1** 블록중심의 **Reorg** 규칙에 관한 비판적 시각 유지.

즉, **One-in-vote** 개념을 중심으로 비잔틴장애 허용에 관에 대한 좀 더 유연한 시각에서 네트워크의 참, 거짓의 결정에

관한 규칙변경

"What was happening with Bitcoin ?"

프로토콜 변경을 진행한 이유는 무엇을 위한 것이었을까?



프로토콜 변경을 진행한 이유는 무엇을 위한 것이었을까?

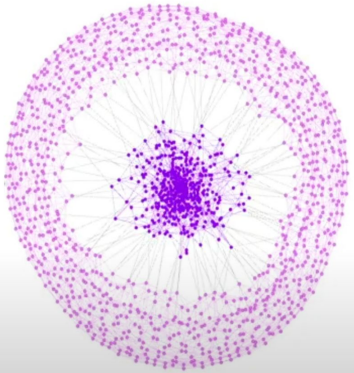
- 세그윗 소프트포크 기반 라이트닝 네트워크의 발전

“What was happening with Bitcoin ?”

즉각적인 결제 및 단순지급결제에 관한 관점에서, 사토시의 디자인에 따른 **Bitcoin on-chain상 SPV node** 중심으로 이뤄지던 네트워크가 중앙화 되어가며 프라이버시가 계속해서 문제가 되었던 배경

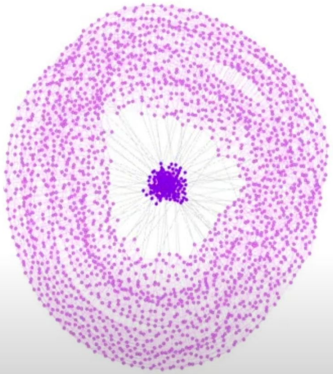
The network would centralize over time

- Full nodes
- Light nodes



The network would centralize over time

- Full nodes
- Light nodes



출처 : River

"What was happening with Bitcoin?"

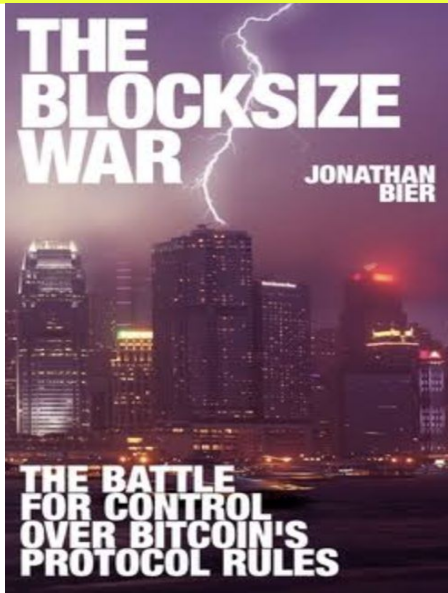
프로토콜 변경 및 세그윗 프로토콜 소프트포크 추진의 배경은 블록사이즈 변경에 관한 논쟁

- 블록이 가득 차있어야 하는가 아니면 항상 여분 용량이 있어야 하는가 ?
- 블록 크기에 관한 프로토콜 규칙이 쉽게 변경되어야 하는가 아니면 쉽게 변하기 않으며 대다수가 원할 때만 변경 가능해야하 하는가?
- 일반 사용자가 노드를 돌리는 것이 얼마나 중요한가 ?
- 스타트업 방식으로 빠르게 시장 점유율을 확보하는 것이 중요한가? 아니면 장기적인 관점으로 결정을 내리기 위해 오랜 시간 생각해야 하는가?

The Blocksize War

Overview

Smaller Blocks	Larger Blocks
Full blocks	Always enough capacity
Robust protocol rules	Change rules more easily
User nodes are really important	User nodes are less important
Long-term focus	Short-term focus

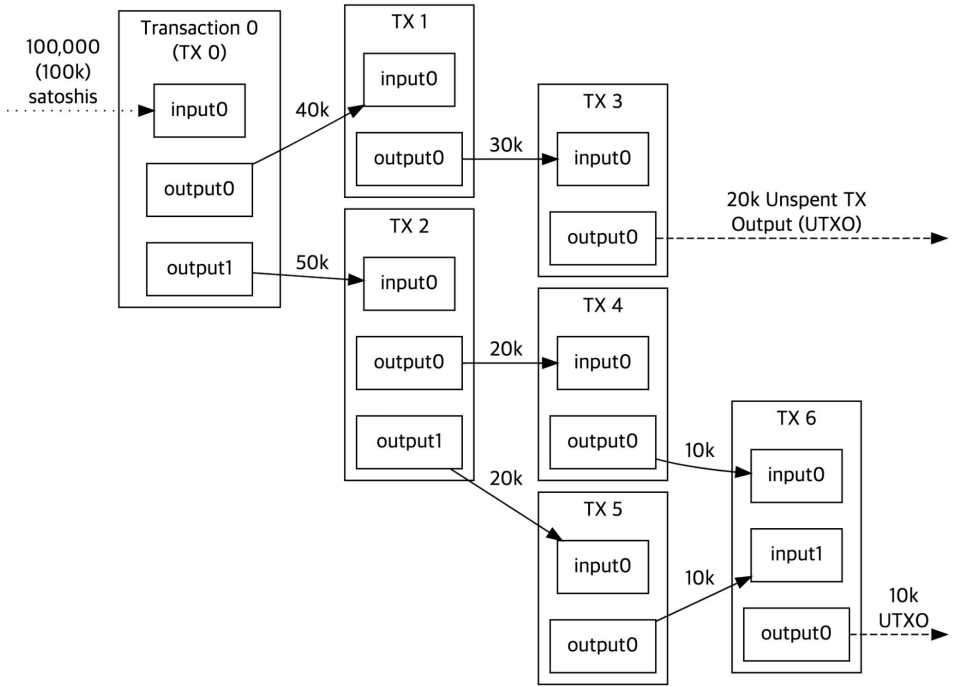


사상적, 철학적, 정치적 갈등 및 다양한 논쟁 속에서 오픈소스 기술 커뮤니티 중심으로 성장과 발전

About ‘Technology’

1. 프로토콜 규칙 변경, 2. Tx 구조 변경 (Segwit) + HTLC, 3. 탭루드 업그레이드 (프라이버시강화)

What is Transaction?



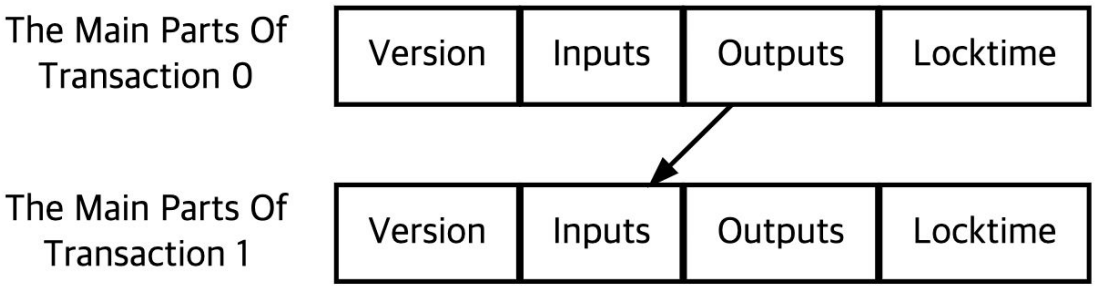
Triple-Entry Bookkeeping (Transaction-To-Transaction Payments) As Used By Bitcoin

Transaction Propagation

https://developer.bitcoin.org/devguide/block_chain.html

What is Transaction?

Each input spends a previous output



Each output waits as an Unspent TX Output (UTXO) until a later input spends it

The Parts Of A Transaction

https://developer.bitcoin.org/devguide/block_chain.html

What is Transaction?

The first bitcoin transaction

Legacy bitcoin transactions have four main components: the version, inputs, outputs, and locktime. To illustrate each of these fields and what they do, we'll go through an example using the first ever bitcoin transaction. On January 11, 2009 at 7:30 PM PST, Satoshi Nakamoto transfered 10 BTC to Hal Finney.

This transaction spent a UTXO that was mined directly by Satoshi, where the block reward was 50 BTC. The transaction had two outputs, one to Hal Finneyfor 10 BTC, and a change output for 40 BTC.

Here is the raw serialized transaction in hex, as you'd see it in the blockchain:

```
0100000001c997a5e56e104102fa209c6a852dd90660a20b2d9c352423edce25857fcd3704000000004847304402204e45e16932b8
af514961a1d3a1a25fdf3f4f7732e9d624c6c61548ab5fb8cd410220181522ec8eca07de4860a4acdd12909d831cc56cbbac46220822
21a8768d1d0901ffffffff0200ca9a3b00000000434104ae1a62fe09c5f51b13905f07f06b99a2f7159b2225f374cd378d71302fa28414e7
aab37397f554a7df5f142c21c1b7303b8a0626f1baded5c72a704f7e6cd84cac00286bee0000000043410411db93e1dcdb8a016b498
40f8c53bc1eb68a382e97b1482ecad7b148a6909a5cb2e0eaddfb84ccf9744464f82e160bfa9b8b64f9d4c03f999b8643f656b412a3ac
00000000
```

What is Transaction?

Transaction metadata

To make more sense of this transaction, we can decode it using the bitcoind command `decoderawtransaction`, or an online web app such as https://btc.com/tools/tx/decode.


```
{
    "txid": "f4184fc596403b9d638783cf57adfe4c75c605f6356fbc91338530e9831e9e16",
    "hash": "f4184fc596403b9d638783cf57adfe4c75c605f6356fbc91338530e9831e9e16",
    "version": 1,
    "size": 275,
    "vsize": 275,
    "weight": 1100,
    "locktime": 0,
    "vin": [
        {
            "txid": "0437cd7f8525ceed2324359c2d0ba26006d92d856a9c20fa0241106ee5a597c9",
            "vout": 0,
            "scriptSig": {
                "asm": "304402204e45e16932b8af514961a1d3a1a25fdf3f4f7732e9d624c6c61548ab5fb8cd410220181522ec
8eca07de4860a4acdd12909d831cc56cbbac4622082221a8768d1d09[ALL]",
                "hex": "47304402204e45e16932b8af514961a1d3a1a25fdf3f4f7732e9d624c6c61548ab5fb8cd410220181522
ec8eca07de4860a4acdd12909d831cc56cbbac4622082221a8768d1d0901"
            },
            "sequence": 4294967295
        }
    ],
    "vout": [
        {
            "value": 10,
            "n": 0,
            "scriptPubKey": {
                "asm": "04ae1a62fe09c5f51b13905f07f06b99a2f7159b2225f374cd378d71302fa28414e7aab37397f554a7df
5f142c21c1b7303b8a0626f1baded5c72a704f7e6cd84c OP_CHECKSIG",
                "hex": "4104ae1a62fe09c5f51b13905f07f06b99a2f7159b2225f374cd378d71302fa28414e7aab37397f554a7
df5f142c21c1b7303b8a0626f1baded5c72a704f7e6cd84cac",
                "type": "pubkey"
            }
        },
        {
            "value": 40,
            "n": 1,
            "scriptPubKey": {
                "asm": "0411db93e1dcdb8a016b49840f8c53bc1eb68a382e97b1482ecad7b148a6909a5cb2e0eaddfb84ccf974
4464f82e160bfa9b8b64f9d4c03f999b8643f656b412a3 OP_CHECKSIG",
                "hex": "410411db93e1dcdb8a016b49840f8c53bc1eb68a382e97b1482ecad7b148a6909a5cb2e0eaddfb84ccf9
744464f82e160bfa9b8b64f9d4c03f999b8643f656b412a3ac",
                "type": "pubkey"
            }
        }
    ]
}
```

What is Transaction?

Version

- 01000000 - Version number (4-byte signed integer, little endian)

The first four bytes of a transaction represents the version number. This number is a way for the transaction to signal what features or consensus rules the transaction may be using. To date, the only feature that uses the version field is relative timelocks (BIP68). A relative timelock will only be enforced if the version field is set to 2. We'll demonstrate this in the chapter on relative timelocks.

In the future, version numbers can be used to signal new features that don't currently exist.

Inputs

01c997a5e56e104102fa209c6a852dd90660a20b2d9c352423edce25857fcd3704000000004847304402204e45e16932b8af51496
1a1d3a1a25fdf3f4f7732e9d624c6c61548ab5fb8cd410220181522ec8eca07de4860a4acdd12909d831cc56cbbac4622082221a87
68d1d0901ffffffff

Breaking it down further:

- 01 - Number of inputs (1-9 byte variable integer)

This lets us know how many transaction inputs to expect in this transaction.

- For each input:
  - outpoint
    - c997a5e56e104102fa209c6a852dd90660a20b2d9c352423edce25857fcd3704 - Input txid (32-byte hash big endian)
    - 00000000 - Index (4-byte integer)

      indicates which output is being spent.
  - scriptSig
    - 48 - scriptSig length (1
    - 47304402204e45e169
      60a4acdd12909d831c
      Since the length of the
      ends and where the ne
      node will combine the
      the top stack item is n
  - sequence
    - ffffffff - (4 bytes)
      In satoshi's initial versi
      The solution didn't wo
      Any value less than 0
      transaction-level and s

```
            "scriptSig": {
                "asm": "304402204e45e16932b8af514961a1d3a1a25fdf3f4f7732e9d624c6c61548ab5fb8cd410220181522ec
8eca07de4860a4acdd12909d831cc56cbbac4622082221a8768d1d09[ALL]",
                "hex": "47304402204e45e16932b8af514961a1d3a1a25fdf3f4f7732e9d624c6c61548ab5fb8cd410220181522
ec8eca07de4860a4acdd12909d831cc56cbbac4622082221a8768d1d0901"
            },
```

Outputs

0200ca9a3b0000000043 4104ae1a62fe09c5f51b13905f07f06b99a2f7159b2225f374cd378d71302fa28414e7aab37397f554a7df5
f142c21c1b7303b8a0626f1baded5c72a704f7e6cd84cac00286bee0000000043 410411db93e1dcdb8a016b49840f8c53bc1eb68
a382e97b1482ecad7b148a6909a5cb2e0eaddfb84ccf9744464f82e160bfa9b8b64f9d4c03f999b8643f656b412a3ac

Breaking it down:

- 02 - Number of outputs (1-9 byte variable integer)

Similar to number of inputs, it lets us know how many outputs to expect in this transaction.

- For each output:
  - First output:
    - 00ca9a3b00000000 - amount in satoshis (8-byte signed integer little endian)
    - 43 - scriptPubkey length (1-9 byte variable integer)
    - 4104ae1a62fe09c5f51b13905f07f06b99a2f7159b2225f374cd378d71302fa28414e7aab37397f554a7df5f142c21c1b7
      303b8a0626f1baded5c72a704f7e6cd84cac - scriptPubkey (arbitrary length)

      The scriptPubkey (aka locking script) is what secures the output and the amount associated with it. This very first bitcoin transaction uses the outdated 'Pay to pubkey' output type. The scriptPubkey is an uncompressed (65-byte) pubkey, followed by `0xac` which correspeonds to `OP_CHECKSIG`. For more on bitcoin script see the chapter on bitcoin script.
  - Second output:
    - 00286bee00000000 - amount in satoshis (8-byte signed integer little endian)
    - 43 - scriptPubkey length (1-9 byte variable integer)
    - 410411db93e1dcdb8a016b49840f8c53bc1eb68a382e97b1482ecad7b148a6909a5cb2e0eaddfb84ccf9744464f82e160b
      fa9b8b64f9d4c03f999b8643f656b412a3ac - scriptPubkey

What is Transaction?

The first bitcoin transaction

Legacy bitcoin transactions have four main components: the version, inputs, outputs, and locktime. To illustrate each of these fields and what they do, we'll go through an example using the first ever bitcoin transaction. On January 11, 2009 at 7:30 PM PST, Satoshi Nakamoto transfered 10 BTC to Hal Finney.

This transaction spent a UTXO that was mined directly by Satoshi, where the block reward was 50 BTC. The transaction had two outputs, one to Hal Finneyfor 10 BTC, and a change output for 40 BTC.

Here is the raw serialized transaction in hex, as you'd see it in the blockchain:

```
01000000 01 c997a5e56e104102fa209c6a852dd90660a20b2d9c352423edce25857fcd3704 00000000 48 47304402204e45e16932b8
af514961a1d3a1a25fdf3f4f7732e9d624c6c61548ab5fb8cd410220181522ec8eca07de4860a4acdd12909d831cc56cbbac46220822
21a8768d1d0901 ffffffff 02 00ca9a3b00000000 43 4104ae1a62fe09c5f51b13905f07f06b99a2f7159b2225f374cd378d71302fa28414e7
aab37397f554a7df5f142c21c1b7303b8a0626f1baded5c72a704f7e6cd84cac 00286bee00000000 43 410411db93e1dcdb8a016b498
40f8c53bc1eb68a382e97b1482ecad7b148a6909a5cb2e0eaddfb84ccf9744464f82e160bfa9b8b64f9d4c03f999b8643f656b412a3ac
00000000
```

Locktime

- 00000000 - Locktime (4 bytes)

The final four bytes are the locktime. The locktime is used to set an absolute timelock on the transaction. The timelock can be expressed in blocks or unix time. Only once this timelock has expired can the transaction be included in a block. We will cover locktime in detail in the chapter on timelocks.

What is HTLC?

목차정리

▼ Contents

The Bitcoin Lightning Network: Scalable Off-Chain Instant Payments

- Keys and addresses
- Hash functions
- Digital signatures
- Transaction structure
- Transaction inputs and outputs
- Transaction chaining
- Bitcoin Script
- Multisignature addresses and scripts
- Timelocks
- Complex scripts

```
OP_DEPTH 3 OP_EQUAL OP_IF OP_HASH160 <R> OP_EQUALVERIFY OP_0 2
<AlicePubkey1> <BobPubkey1> 2 OP_CHECKMULTISIG OP_ELSE OP_0 2
<AlicePubkey2> <BobPubkey2> 2 OP_CHECKMULTISIG OP_END
```

About ‘Technology’

1. 프로토콜 규칙 변경, 2. Tx 구조 변경 (Segwit), 3. 탭루트 업그레이드 (Segwit1 프라이버시강화)

2008.10
비트코인 백서 공개

2009.1
첫번째 TX(사토시 → 할피니) 생성

2009.1
비트코인 제네시스블록

2008.5
웨이다이 메일링

2015
세그윗 제안
by Peter Wulle

2015
컬러드코인
옵리턴전쟁

2015
이더리

2015
Bitcoin
(블록사
작)

2015
크레이그 리

2016.1
라이트닝 네트워크 백서 공개

2017
세그윗 소프트포크,
라이트닝 네트워크 가동

2021.11
탭루트 소프트포크

2022
Taro, RGB Beta

2023.12
오디널스 검열 논쟁 by Luke

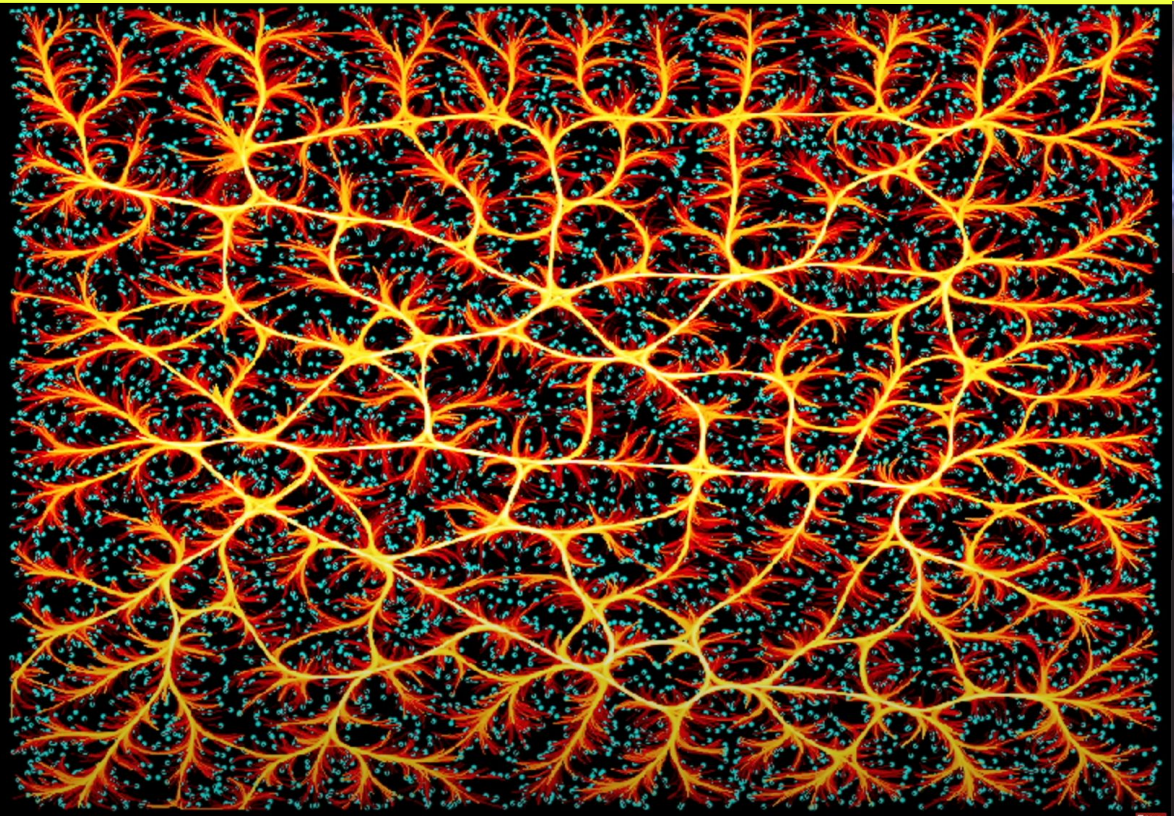
2024.4
블록보상 반감기
(6.25BTC -> 3.125)

"What was happening with Bitcoin ?"

프라이버시가 강화되고 즉각적인 결제가 가능해지면서 유기적인 비트코인+라이트닝 네트워크로 발전

Routing nodes on the highways

Edge nodes in blue



pymoment
@pymoment

19/Jan/2019

Hodlonaut, a dedicated Bitcoin enthusiast, kickstarted a global movement showcasing the power of the **Lightning Network**.

LIGHTNING NETWORK TRUST CHAIN

Wrap it up

1. 라이트닝 네트워크 중심 비트코인 사용의 현재_세 가지 거래유형 예시를
2. 현재 관점에서 비트코인 백서 읽기_사토시의 프로토콜 디자인 의도 및 초기 구현에 대한 중심으로
3. 라이트닝 네트워크 백서 읽기, 라이트닝 네트워크 결제 테스트_LNBook 테스트 리소스 디자인변경 연구

커스터마이징

"What is happening with Bitcoin?"

"What was happening with Bitcoin ?"

Wrap it up

“What is happening with Bitcoin?”

“What was happening with Bitcoin ?”

And then,

How to answer “What is going to be being Bitcoin in the future?” ?

C. 비트코인의 미래_National Bitcoin Adoption, Built on top of Bitcoin / Lightning Protocol, L1 scaling

National Bitcoin Adoption

2008.10
비트코인 백서 공개

2009.1
첫번째 TX(사토시 → 할피니) 생성

2015
세그윗 제안
by Peter Wulle

2016.1
라이트닝 네트워크 백서 공개

2017
세그윗 소프트포크, 라이트닝 네트워크 가동

2021.11
탭루트 소프트포크

2022
Taro, RGB Beta

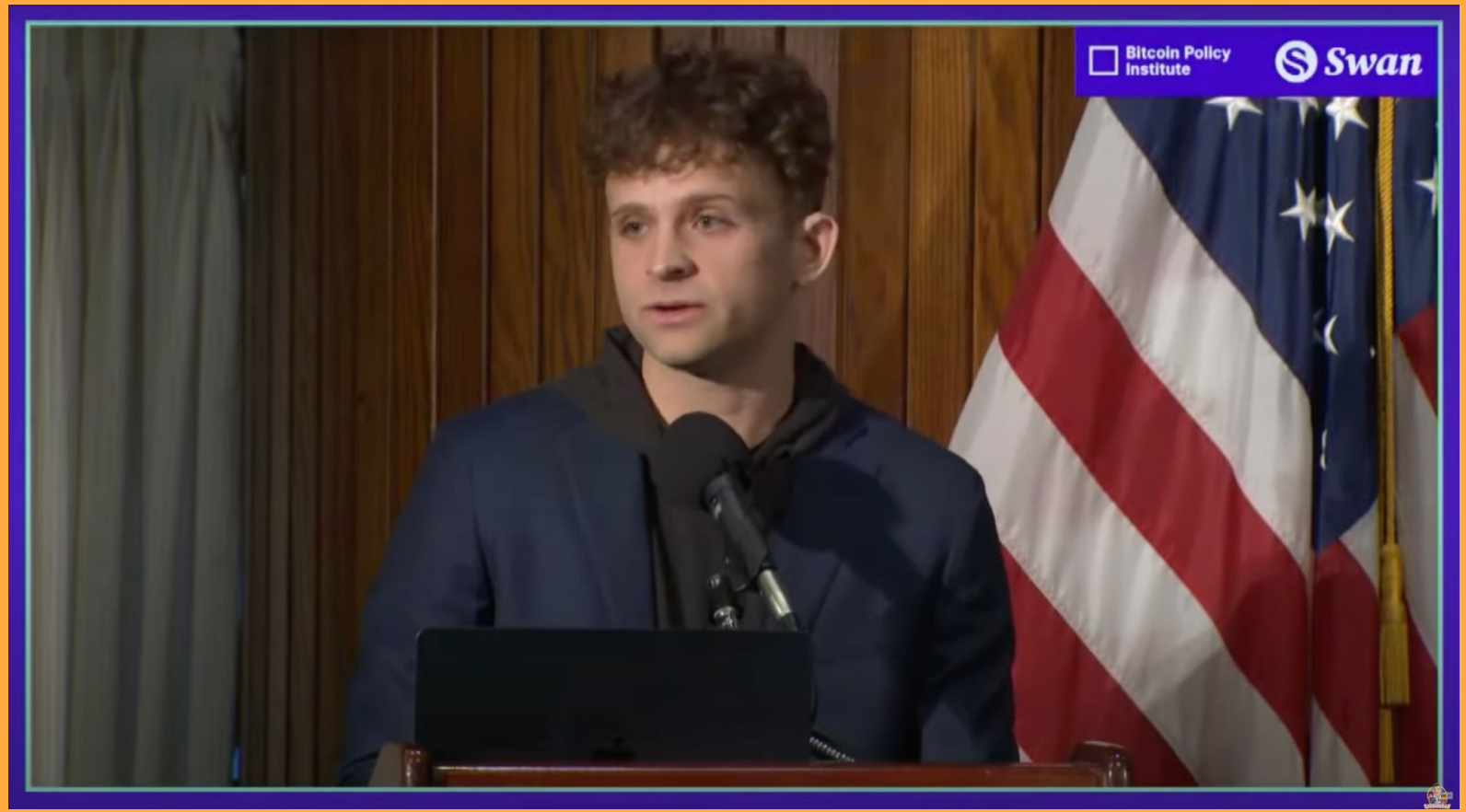
2023.12
오디널스 검열 논쟁 by Luke

2024.4
블록보상 반감기
(6.25BTC -> 3.125)

2021.9
엘살바도르 법정화폐 도입

"What was happening with Bitcoin ?"

National Bitcoin Adoption



Key Takeaways

1. 비트코인 코어 개발 커뮤니티 중심으로 ‘일반적인 거래(**Casual Transaction**)’를 위한 ‘즉각적인 결제(**Instant Payment**)’에 집중

하며 지속적인 성장과 발전

2. 블록사이즈전쟁을 겪은 비트코인 커뮤니티에서 비트코인코어 커뮤니티 중심으로 프로토콜 변경을 진행하고 세그윗 업그레이드, 라이트닝

네트워크 개발, 라이트닝 생태계확장을 중심으로 형성되어 즉각적인 결제가 가능한 실재하고 유기적인 네트워크로 발전

3. 국가적 단위로 비트코인의 화폐인정이 증가하는 추세와 라이트닝 네트워크 기반 자산발행 프로토콜 프로젝트,

3. 비트코인 개발은 무엇인가?(What is Bitcoin Development?)

비트코인 테크 토크: 비트코인 개발에 대해서

밋업에서 사용하였던 발표자료 공유

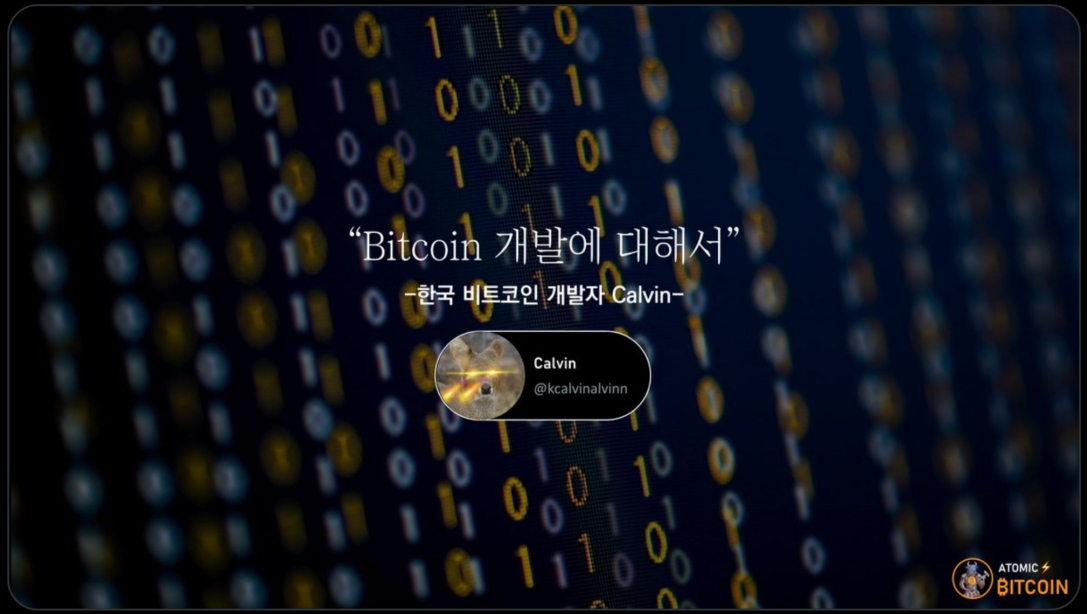
Posted on November 19, 2022

2022년 11월 19일 토요일에 있었던 밋업에서 사용했던 발표 자료입니다.

https://docs.google.com/presentation/d/1DGy6alYYrJz4Iu9cATMj2I3ZSgo2PTK-yjGm_APHmS8

#Bitcoin ₿ 개발에 대해서 (1부)
-한국 비트코인 개발자 Calvin(@kcalvinalvinn)

Translate post



Atomic Bitcoin

Korean Bitcoiner OG

무엇을 어떻게 할 수 있는가?(How? What we can make some execution?)

Scavenger Hunt game Mission

Track A 문제 예시, 2024 FOSS program scavenger hunt by Chaincode Labs

0# What is the hash of block 654,321?

1#(true / false) Verify the signature by this address over this message:

address: `1E9YwDtYf9R29ekNAfbV7MvB4LNv7v3fGa`
message: `1E9YwDtYf9R29ekNAfbV7MvB4LNv7v3fGa`
signature: `HCsBcgB+Wcm8kOGMH8IpNeg0H4gjCrlqwDf/GlSXphZGBYxm0QkKEPhh9DTJRp2IDNUhVr0FhP9qCqo2W0recNM=`

2# How many new outputs were created by block 123,456?

3# Using descriptors, compute the 100th taproot address derived from this extended public

key:`xpub6Cx5tvq6nACSLJdra1A6WjqTo1SgeUZRFqsX5ysEtVBMwhCCRa4kfgFqaT2o1kwL3esB1PsYr3CUdfRZYfLHJunNWUABKftK2NjHUtzDms2`

4#Create a 1-of-4 P2SH multisig address from the public keys in the four inputs of this

tx:`37d966a263350fe747f1c606b159987545844a493dd38d84b070027a895c4517`

5# Which tx in block 257,343 spends the coinbase output of block 256,128?

6# Only one single output remains unspent from block 123,321. What address was it sent to?

7# Which public key signed input 0 in this tx:

`e5969add849689854ac7f28e45628b89f7454b83e9699e551ce14b6f90c86163`

1.

풀이 제출시 주의사항

1. 문제와 제출해야 할 위치는 개인별로 **2024.05.23** 목요일에 메일로 발송 예정.

2. 비트코인 해커톤 공식 **Github(https://github.com/Bitcoin-Seoul-Hackathon/workshop)**내 개인별 공개파일에 제출

3. 쉘스크립트, **C++, Go, Rust, Python, JS** 중 하나 선택하여 **2024.5.26 23:59**까지 제출

사전준비 사항

1. **Bitcoin Testnet3** 노드 설치.
2. 참고 : https://bitcoincore.org/en/download/
3. **Utreexo** 등 타 노드 클라이언트 사용 가능

Appendix A _ 오라클 컨퍼런스 3rd 최종 발표자료

[성후] Mathematical Structure - Model Theorical Structure,
https://www.notion.so/_2023_2_-b52185093d984d618be158472f9a1d9a

[혜수] Reading Bitcoin Whitepaper,
https://deciduous-beech-21f.notion.site/Reading-Bitcoin-Whitepaper-6fb4067edd3b47eb9527e4a5a360a9cc

[경화] Bitcoin Whitepaper,
https://fluff-cake-2f8.notion.site/Bitcoin-Whitepaper-ef12c72ee35d405e8a587288d93738b2

[혜수] Bitcoin Layers and Scalable Ecosystem,
https://deciduous-beech-21f.notion.site/Bitcoin-Layers-and-Scalable-Ecosystem-Overview-2023-11-11-c4d6be94985a4d1f887e768805d9589b?pvs=4

[혜수] Tx툡아보기,
https://deciduous-beech-21f.notion.site/Tx-dd5a8575783241409e9248ad99ae72d3?pvs=4

[혜수] LNbook[Chapter4],
https://deciduous-beech-21f.notion.site/LNbook-Chapter4-85a95cb6b50d466bbb8ed584eaa742a4

Reference

1. Bitcoin Whitepaper, Satoshi Nakamoto, https://bitcoin.org/bitcoin.pdf
2. Bitcoin Core, https://github.com/bitcoin/bitcoin
3. Lightning Network Whitepaper, Joseph Poon Thaddeus Dryja, https://lightning.network/lightning-network-paper.pdf
4. Lightning Network Daemon, Lightning Labs ,https://github.com/lightningnetwork/lnd
5. Programming Bitcoin, Jimmy Song, https://github.com/jimmysong/programmingbitcoin
6. Mastering Bitcoin, Andreas M, https://github.com/bitcoinbook/bitcoinbook
7. Mastering the Lightning Network, Andreas M, Olaoluwa, Rene, https://github.com/lnbook/lnbook
8. The Crypto Anarchist Manifesto, Timothy C. May, https://www.activism.net/cypherpunk/crypto-anarchy.html
9. 사이퍼펑크,해시넷, http://wiki.hash.kr/index.php/%EC%82%AC%EC%9D%B4%ED%8D%BC%ED%8E%91%ED%81%AC
10. Bitcoin Core dev, https://developer.bitcoin.org/
11. Blocksize War, 라이프이즈굿_블록사이즈 전쟁(비트코인 내전), https://www.youtube.com/watch?v=xJ_QW89Cpis
12. Bitcoins History | The Blocksize War, https://www.youtube.com/watch?v=6YtS5ZNuuTw&t=0s
13. Colered Coin, https://en.bitcoin.it/wiki/Colored_Coins
14. Mempool.space,https://mempool.space/block/00000000d1145790a8694403d4063f323d499e655c83426834d4ce2f8dd4a2ee
15. Taproot Image, https://i.ytimg.com/vi/u_2FjtbChyg/maxresdefault.jpg, https://www.youtube.com/watch?v=u_2FjtbChyg
16. The State Of The Lightning Network, https://www.youtube.com/watch?v=BaL_wExuR3c
17. ChaincodeLabs tx-tutorial material,
18. KEYNOTE: Bitcoin and the Ligthning Network by Jack Mallers, https://www.youtube.com/watch?v=PxELH-vWKSA&t=2s

Reference

19. bitcoincore.org, https://bitcoincore.org/en/download/

20. 2024 Bitcoin Seoul Hackathon, https://github.com/Bitcoin-Seoul-Hackathon/workshop

21. Utreexo, https://github.com/utreexo