



Ken Sato, Yenpoint CEO

Bitcoin スケーリング

その歴史と技術的な課題



佐藤研一郎

円ポイント株式会社 CEO

略歴

連続起業家として、20年にわたって日本とアメリカでさまざまなビジネスを立ち上げてきました。オンライン・メディア、パブリックアート、都市計画、オーガニックフード、不動産開発、ブロックチェーン、自由市場経済の哲学、フィンテックスタートアップなどの多彩な分野で、才能を発揮し活躍しています。2019年に日本に戻り、円ポイント株式会社を設立し、ブロックチェーン技術を用いたマイクロペイメントツールを開発しています。

詳しい経歴 <https://www.linkedin.com/in/ken-sato-918b99/>

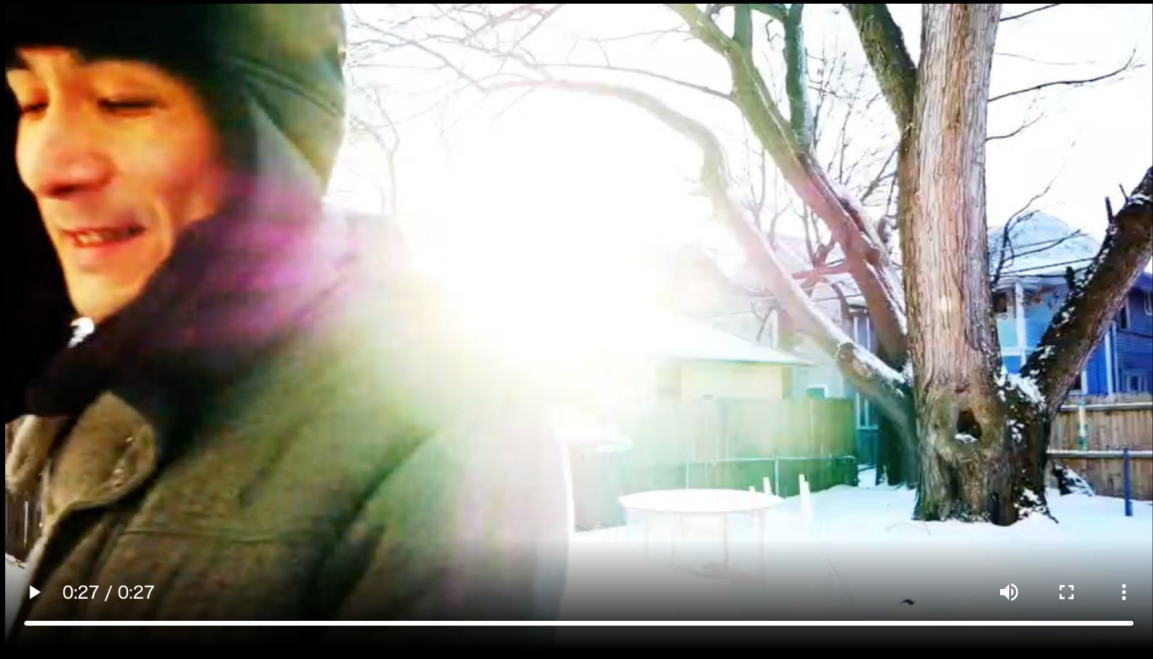


ロチェスター郊外で
ビットコインのマイニング施設の運用

ビットコインのスケーリング戦争に参戦

Bitcoin Hashwar

2018年12月、スケーリング派 (Bitcoin sv)



▶ 0:00 / 0:05 ——— 🔊 ⋮

This page is entirely on Bitcoin SV

Keep talking. We keep walking.



世界初オンチェーンにビデオを上げる

オンチェーンのWebpage

スケーラブルなブロックチェーンの可能性の探求

Bitcoin Activism

Bitcoin Script Op_Return size limit was lifted in 2019.



ビットコイン勉強会

185 subscribers

HOME

VIDEOS

PLAYLISTS

CHANNELS

DI



「オリジナルに向かって水面化で進 佐藤研一朗 - 第4回ビットコイン(BS

ビットコイン勉強会 • 238 views • 8 months ago

第4回 ビットコイン(BSV)勉強会 開催日：2020年1

=====

Uploads

▶ PLAY ALL



【質疑応答】 広がりつつある
BSV利用 - CBDC, サンドボ...

25 views • 11 hours ago



日本初!! 第1回BitcoinSVアイ
デアソン ~発表：TEAM4~

64 views • 1 week ago



日本初!! 第1回Bitco
デアソン ~発表：

59 views • 2 weeks ago

ビットコイン勉強会

BSV Night

日本帰国後、ビットコイン勉強会を毎月開催、日本でのコミュニティを作りつつ、世界から活躍するクリプト系の経営者や、開発者を招待し日本に紹介する。

第1回 Bitcoin^{sv} アイデアソン

発表者 チーム4

「masterpiece archives(骨董品NFT)」

BSV Night

千葉工業大学 藤原研究室

Sponsored by



おくら様



WallStreet5様



Zatoshi様



(株)ChainBow様

Web3ビジネスの可能性を探る

Bitcoin sv

アイデアソン

ブロックチェーンを研究している研究所をもつ千葉工業大学と共同で、ビットコインのアイデアソンを開催

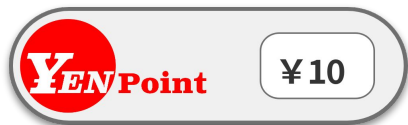
みんなが使える ブロックチェーンウォレット



YENPOINT

YENPOINT INC.

Products



ブロックチェーン ウォレット基盤

トークンプラットフォーム

自社ブランド & OEMの提供
FT & NFTのお財布



少額課金の マーケットプレイス

オンライン100円ショップ

100円以下に特化した
マーケットプレイスの運営

STVP

Simplified Token Verification Protocol

ステーブルコイン 発行基盤の開発

CBDCやステーブルコインの
基盤技術（特許出願中）

次世代のブロックチェーンを使った
デジタルキャッシュの基盤技術の開発



Ken Sato, Yenpoint CEO

Bitcoin スケーリング

その歴史と技術的な課題

Menu

ビットコインの歴史

スケーリング論争

技術と課題

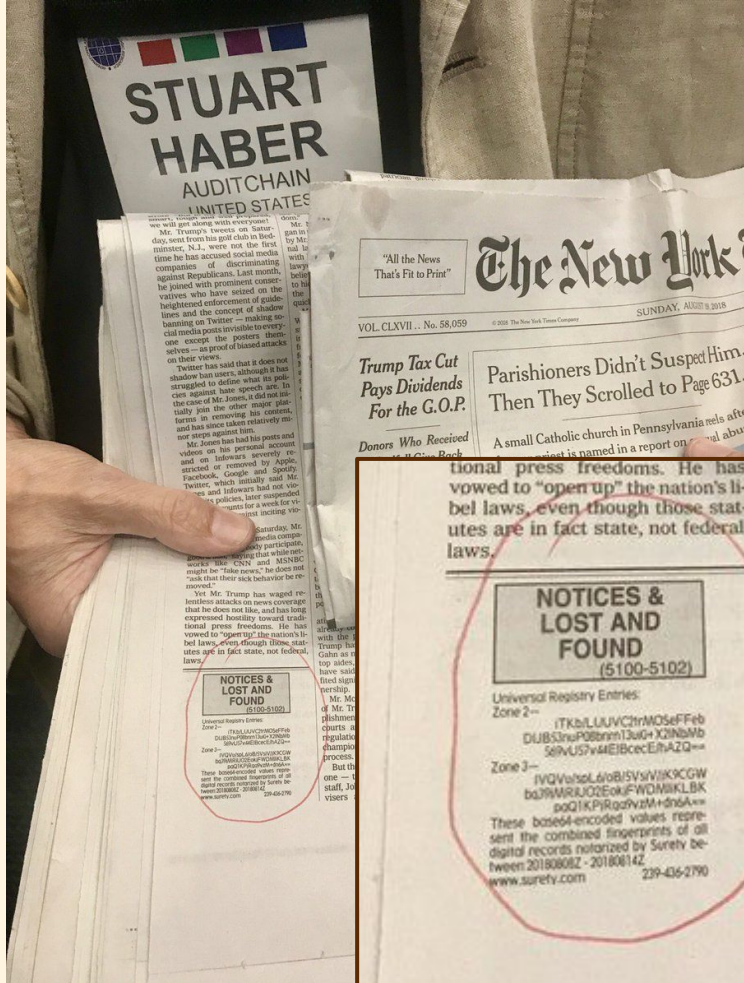
スケーリングを支える技術

ビットコインの今後

Ordinals からトレカへ

ブロックチェーンの始まり

1991 Stuart Haber and Scott Stornetta ベル研究室



Bitcoin年表



Bitcoin Whitepaper

2008 サトシナカモトが暗号メーリングリストに投稿
翌年、ネットワークがスタート

Bitcoin: A Peer-to-Peer Electronic Cash System

Satoshi Nakamoto
satoshin@gmx.com
www.bitcoin.org

Abstract. A purely peer-to-peer version of electronic cash would allow online payments to be sent directly from one party to another without going through a financial institution. Digital signatures provide part of the solution, but the main benefits are lost if a trusted third party is still required to prevent double-spending. We propose a solution to the double-spending problem using a peer-to-peer network. The network timestamps transactions by hashing them into an ongoing chain of hash-based proof-of-work, forming a record that cannot be changed without redoing the proof-of-work. The longest chain not only serves as proof of the sequence of events witnessed, but proof that it came from the largest pool of CPU power. As long as a majority of CPU power is controlled by nodes that are not cooperating to attack the network, they'll generate the longest chain and outpace attackers. The network itself requires minimal structure. Messages are broadcast on a best effort basis, and nodes can leave and rejoin the network at will, accepting the longest proof-of-work chain as proof of what happened while they were gone.

1. Introduction

Commerce on the Internet has come to rely almost exclusively on financial institutions serving as trusted third parties to process electronic payments. While the system works well enough for most transactions, it still suffers from the inherent weaknesses of the trust based model. Completely non-reversible transactions are not really possible, since financial institutions cannot avoid mediating disputes. The cost of mediation increases transaction costs, limiting the minimum practical transaction size and cutting off the possibility for small casual transactions, and there is a broader cost in the loss of ability to make non-reversible payments for non-reversible services. With the possibility of reversal, the need for trust spreads. Merchants must be wary of their customers, hassling them for more information than they would otherwise need. A certain percentage of fraud is accepted as unavoidable. These costs and payment uncertainties can be avoided in person by using physical currency, but no mechanism exists to make payments over a communications channel without a trusted party.

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. Transactions that are computationally impractical to reverse would protect sellers from fraud, and routine escrow mechanisms could easily be implemented to protect buyers. In this paper, we propose a solution to the double-spending problem using a peer-to-peer distributed timestamp server to generate computational proof of the chronological order of transactions. The system is secure as long as honest nodes collectively control more CPU power than any cooperating group of attacker nodes.

14年後 暗号資産の時価総額

2023 日本のGDPの三分の一

Cryptocurrency market

Market cap ⓘ

1d 7d 1m 1y All 📅

All coins ▾



手数料が高い

平均手数料

Fee

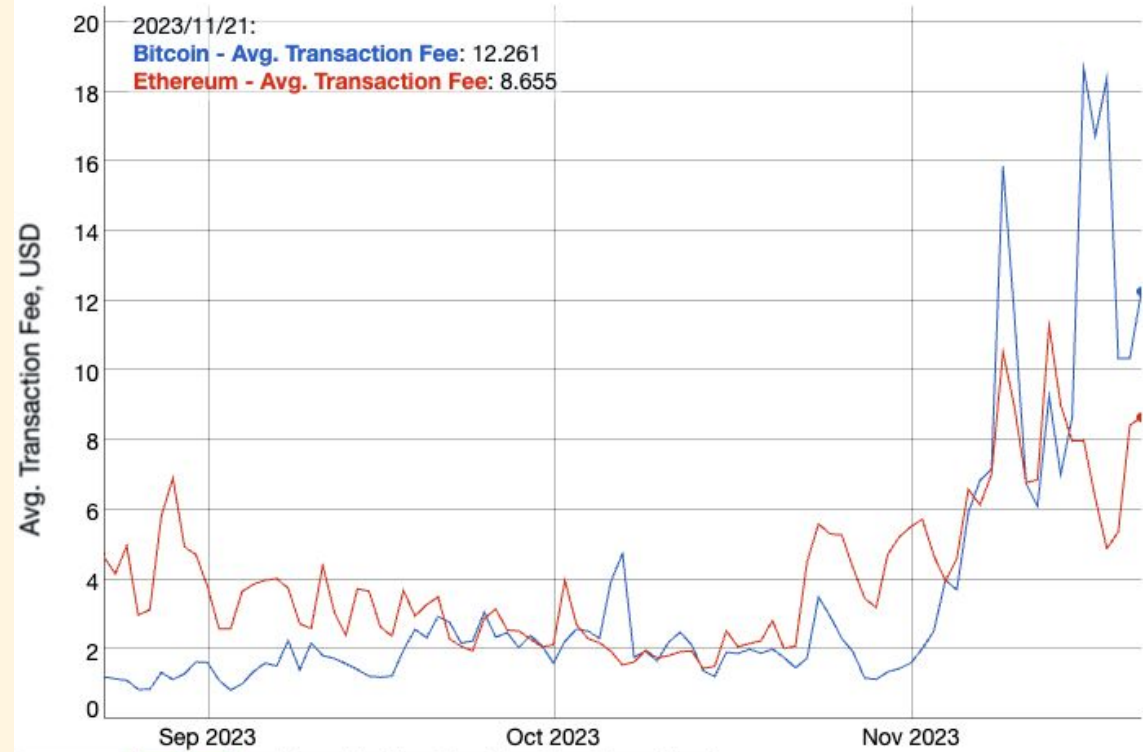
Bitcoin \$12 (1,800円)

Ethereum \$8(1,200円)

Bitcoin, Ethereum Avg. Transaction Fee historical chart

Average transaction fee, USD

Share:      



search

[btc](#) [eth](#) [xrp](#) [doge](#) [ltc](#) [bch](#) [etc](#) [xmr](#) [bsv](#) [dash](#) [zec](#)

Scale:

Latest Prices: [BTC/USD: 36406.2](#) (coinbasepro) | [BTC/USD: 36399.83](#) (p2pb2b) | [ETH/USD: 1986.49](#) (coinbasepro) | [ETH/BTC: 0.05457641](#) (bitforex)

[linear](#) [log](#)

Zoom:

[3 months](#) [6 months](#) [1 year](#) [3 years](#) [all time](#)

問題

ちょっとした思考実験？

Aさんは5000円分のビットコインを持っています。

このビットコイン全額を

自分の新しいウォレットに送金します。

その後、また最初のウォレットに戻しました。

全額移動しました。さていくら残っているでしょう？

答え

残りは1400円。。。😭

ブロックサイズ



BTCのブロックサイズリミットは1MB

フロッピーディスクと同じ



BTCのブロックサイズは

フロッピーディスクと同じ

処理能力	ビットコイン	イーサリアム (低い推定)
秒間トランザクション数 (tx/sec)	約7	約15
10分毎のトランザクション数	$7 \text{ tx/sec} \times 600 \text{ sec} = 4200$	$15 \text{ tx/sec} \times 600 \text{ sec} = 9000$
1日毎のトランザクション数	$7 \text{ tx/sec} \times 86400 \text{ sec} = 604800$	$15 \text{ tx/sec} \times 86400 \text{ sec} = 1296000$

Bitcoin Whitepaper

2008 サトシナカモトが暗号メーリングリストに投稿
翌年、ネットワークがスタート

Bitcoin: A Peer-to-Peer Electronic Cash System

Satoshi Nakamoto
satoshin@gmx.com
www.bitcoin.org

Abstract. A purely peer-to-peer version of electronic cash would allow online payments to be sent directly from one party to another without going through a financial institution. Digital signatures provide part of the solution, but the main benefits are lost if a trusted third party is still required to prevent double-spending. We propose a solution to the double-spending problem using a peer-to-peer network. The network timestamps transactions by hashing them into an ongoing chain of hash-based proof-of-work, forming a record that cannot be changed without redoing the proof-of-work. The longest chain not only serves as proof of the sequence of events witnessed, but proof that it came from the largest pool of CPU power. As long as a majority of CPU power is controlled by nodes that are not cooperating to attack the network, they'll generate the longest chain and outpace attackers. The network itself requires minimal structure. Messages are broadcast on a best effort basis, and nodes can leave and rejoin the network at will, accepting the longest proof-of-work chain as proof of what happened while they were gone.

1. Introduction

Commerce on the Internet has come to rely almost exclusively on financial institutions serving as trusted third parties to process electronic payments. While the system works well enough for most transactions, it still suffers from the inherent weaknesses of the trust based model. Completely non-reversible transactions are not really possible, since financial institutions cannot avoid mediating disputes. The cost of mediation increases transaction costs, limiting the minimum practical transaction size and cutting off the possibility for small casual transactions, and there is a broader cost in the loss of ability to make non-reversible payments for non-reversible services. With the possibility of reversal, the need for trust spreads. Merchants must be wary of their customers, hassling them for more information than they would otherwise need. A certain percentage of fraud is accepted as unavoidable. These costs and payment uncertainties can be avoided in person by using physical currency, but no mechanism exists to make payments over a communications channel without a trusted party.

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. Transactions that are computationally impractical to reverse would protect sellers from fraud, and routine escrow mechanisms could easily be implemented to protect buyers. In this paper, we propose a solution to the double-spending problem using a peer-to-peer distributed timestamp server to generate computational proof of the chronological order of transactions. The system is secure as long as honest nodes collectively control more CPU power than any cooperating group of attacker nodes.

Bitcoinの歴史は スケーリング論争

Cryptography Mailing List

Bitcoin P2P e-cash paper

November 3, 2008 at 01:37:43 UTC

[Original email](#) · [View in thread](#)

>Satoshi Nakamoto wrote:

>> I've been working on a new electronic cash system that's fully
>> peer-to-peer, with no trusted third party.

>>

>> The paper is available at:

>> <http://www.bitcoin.org/bitcoin.pdf>

>

>We very, very much need such a system, but the way I understand your
>proposal, it does not seem to scale to the required size.

>

>For transferable proof of work tokens to have value, they must have
>monetary value. To have monetary value, they must be transferred within
>a very large network - for example a file trading network akin to
>bittorrent.

>

>To detect and reject a double spending event in a timely manner, one
>must have most past transactions of the coins in the transaction, which,
> naively implemented, requires each peer to have most past
>transactions, or most past transactions that occurred recently. If
>hundreds of millions of people are doing transactions, that is a lot of
>bandwidth - each must know all, or a substantial part thereof.


>

スケーリングについてサトシ・ナカモトの意見 2008

今の技術でもVISAくらい処理できる、数ギガブロックは問題なし、専門のサーバーファームでマイニングされユーザーはSPVウォレットを使うことになる

If the network were to get that big, it would take several years, and by then, sending 2 HD movies over the Internet would probably not seem like a big deal.

Satoshi Nakamoto

Long before the network gets anywhere near as large as that, it would be safe for users to use Simplified Payment Verification (section 8) to check for double spending, which only requires having the  ain of block headers, or about 12KB per day. Only people trying to create new coins would need to run network nodes. At first, most users would run network nodes, but as the network grows beyond a certain point, it

Bitcoin年表



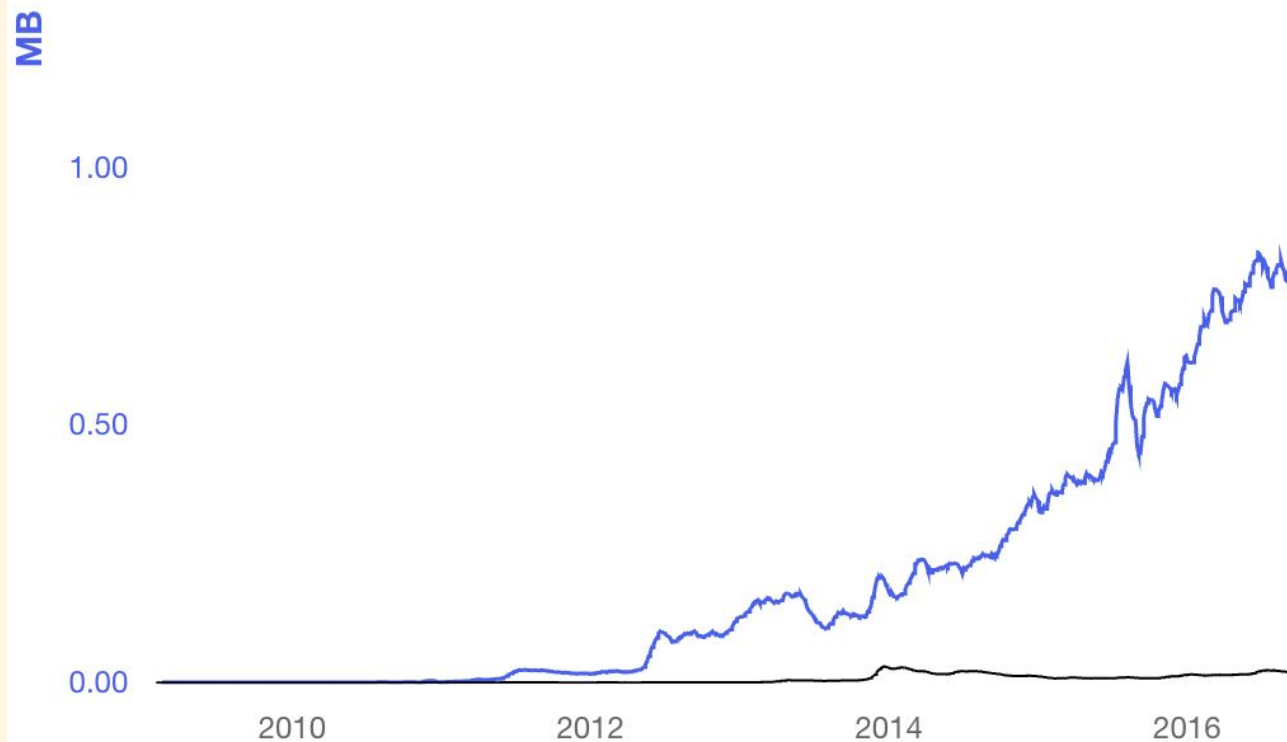
サトシの後継者

Gavin Andresen 2016



Bitcoinの人気に火がつく

ブロックのサイズが1mbに近づく



Data

Bitcoin XT

Gavin Andresen & Mike Hearn 2015



提案：二年間に一回8mb ブロックサイズの上限を引き上げる。

ブロックサイズ論争

2015—2017 On chain or Off chain scaling
Segwit, Bitcoin cash, Hashwar

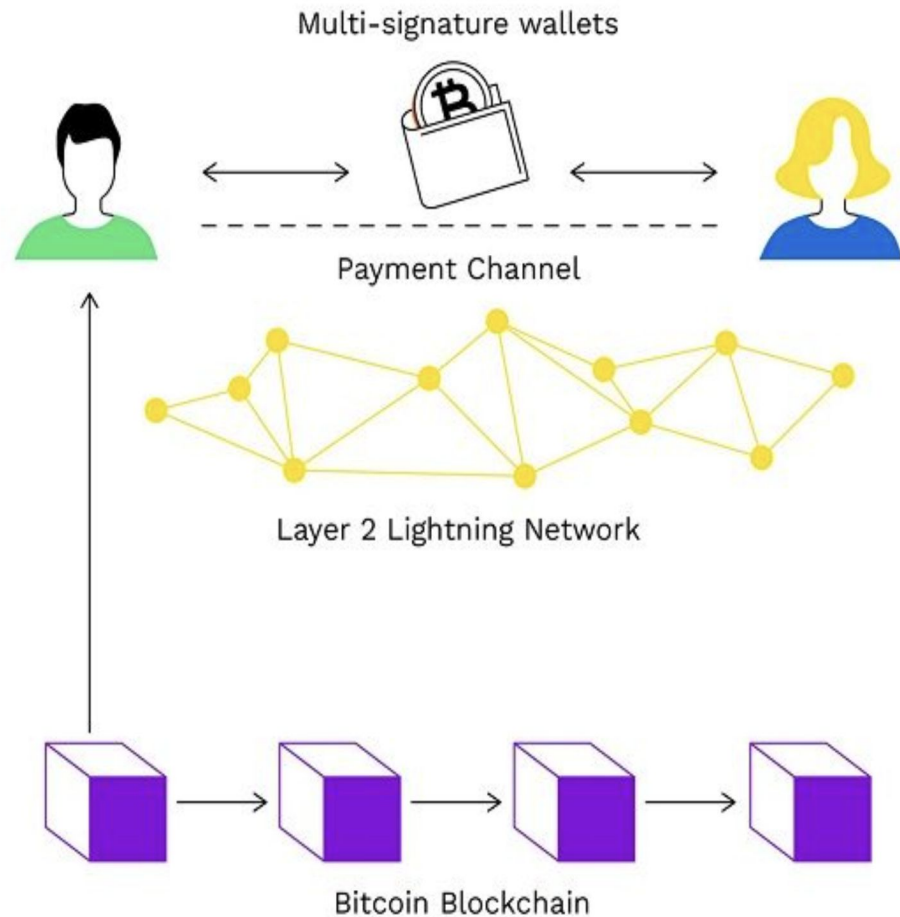


ビッグブロック VS ライトニング

ライティングとは

Layer2の貸し借りのネットワーク

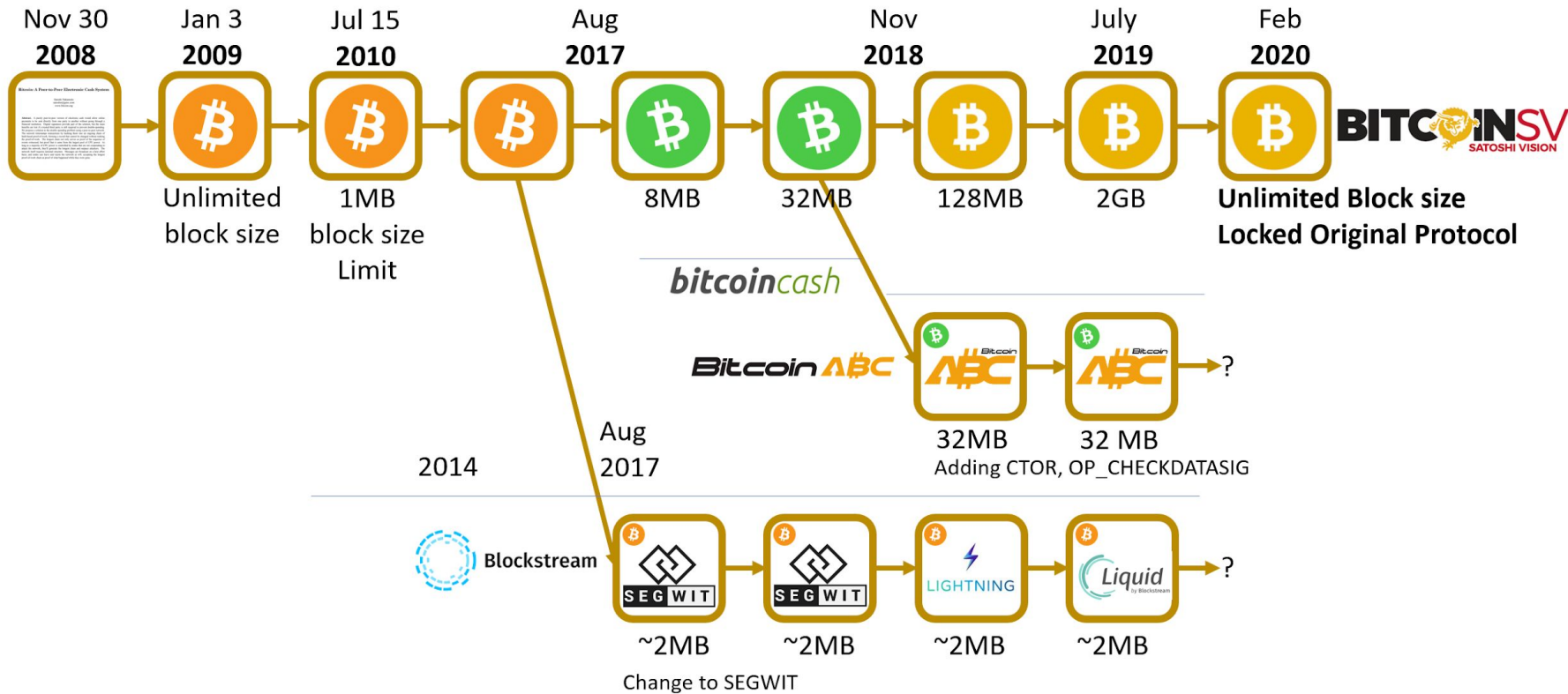
Lightning Network



ブロックサイズをめぐるフォーク

2015-2017 On chain or Off chain scaling
Segwit, Bitcoin cash, Hashwar





Bitcoin Core 乗っ取り

ライトニングやサイドチェーンによるスケーリング



Bitcoin年表



Bitcoin SVの誕生

オリジナルなビットコインを目指す
スケーリングしかつスマートコントラクトができる



The screenshot shows the homepage of the BSV Blockchain website. The header includes the 'BSV BLOCKCHAIN' logo, a navigation menu with 'Learn', 'Build', 'Ecosystem', 'Network', 'Solutions', and 'Association', and a 'Contact' button with a 'Get BSV' button and a search icon. The main content area features the headline 'One Blockchain for Everyone' in large blue text, followed by the subtext 'Reliable open source software, providing the fundamental requirements for enterprise grade blockchain applications.' Below this is a blue button labeled 'Ecosystem' with a dropdown arrow and a link 'Intro to BSV'. To the right is a 3D graphic of a blue, translucent cube. At the bottom, three key statistics are displayed: '1.95 Billion Total transactions', '\$ 0.000003 Transaction Fee', and '<2 Secs Transaction Time'.

BSV BLOCKCHAIN

Learn ▾ Build ▾ Ecosystem ▾ Network ▾ Solutions ▾ Association

Contact Get BSV 🔍

One Blockchain for Everyone

Reliable open source software, providing the fundamental requirements for enterprise grade blockchain applications.

Ecosystem () ▷ Intro to BSV

1.95 Billion Total transactions

\$ 0.000003 Transaction Fee

<2 Secs Transaction Time

サトシナカモトの正体

Bitcoin年表



Craig Steven Wright

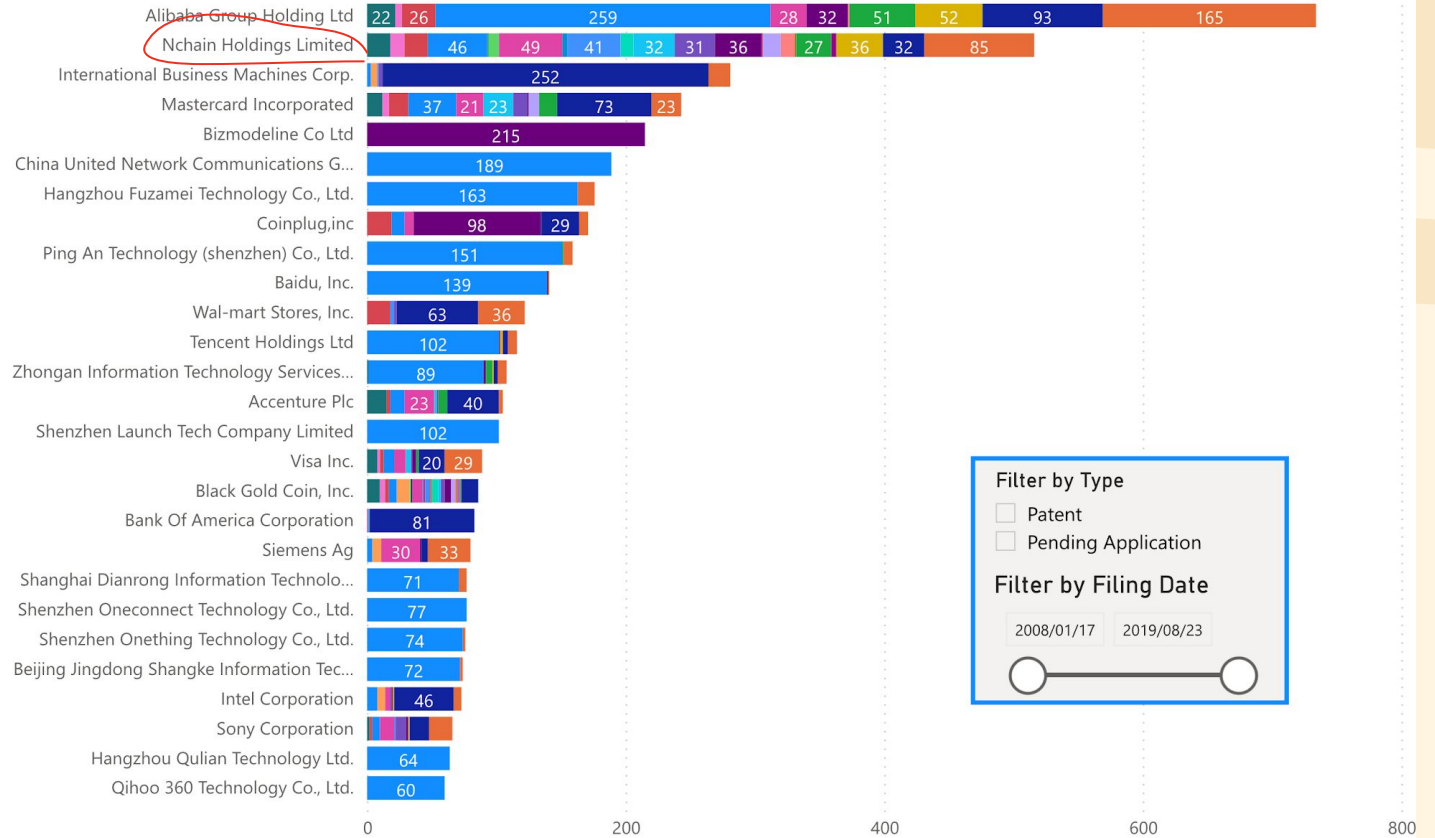
この人がサトシ・ナカモト



TOP PLAYERS IN THE BLOCKCHAIN SPACE

(active patents & pending applications as of 10/1/2019)

Harrity Patent Analytics publishes interactive dashboards for clients that provide insights into technology areas, competitors, and their own portfolio. To learn more about Harrity Patent Analytics, visit <https://harrityllp.com/>




Filter by Type

Patent

Pending Application

Filter by Filing Date

2008/01/17 2019/08/23



サトシが鍵を渡した男が認めている

Gavin Andresen 2016



半端ない知識

その道の専門家と言われる人も知らないことを知っている 2015



ニック・ザボー

<https://www.youtube.com/watch?v=LdvQTwjVmrE>

個人的な直感

直接会って話をした経験



繰り返し囚人のジレンマ ゲーム理論

業界から嫌われているBSV

世界中の取引所からDelistされる 2019



CZ ◆ **Binance** ✓

@cz_binance

Craig Wright is not Satoshi.

Any more of this sh!t, we delist!

[DeepLで翻訳する](#) 🗣️



Bitcoin Magazine ✓ @BitcoinMagazine · Apr 12, 2019

An attack against one is an attack against all. #WeAreAllHodlonaut

Artwork: @CryptoScamHub

[DeepLで翻訳する](#) 🗣️

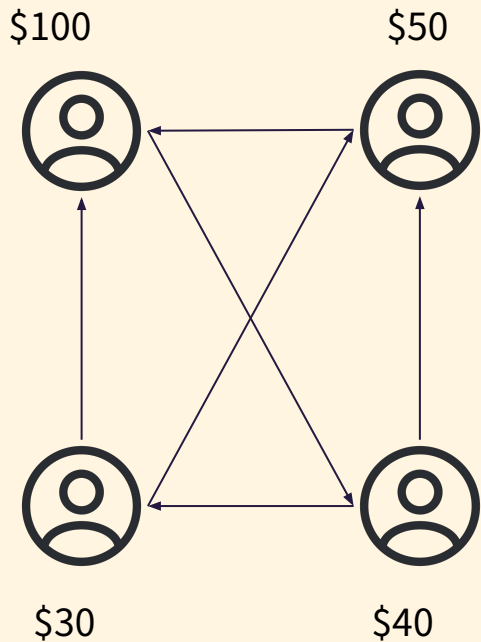


スケーリングをめぐる技術的な課題

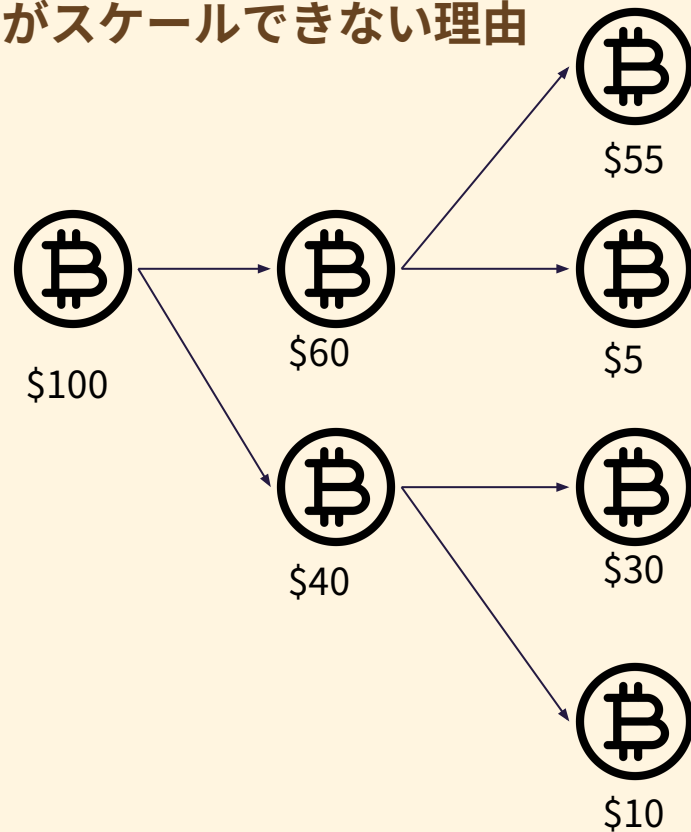
1. 並列化の壁

UTXO vs アカウト モデル

ビットコインはスケールするがイーサリアムがスケールできない理由



アカウント式



UTXO式

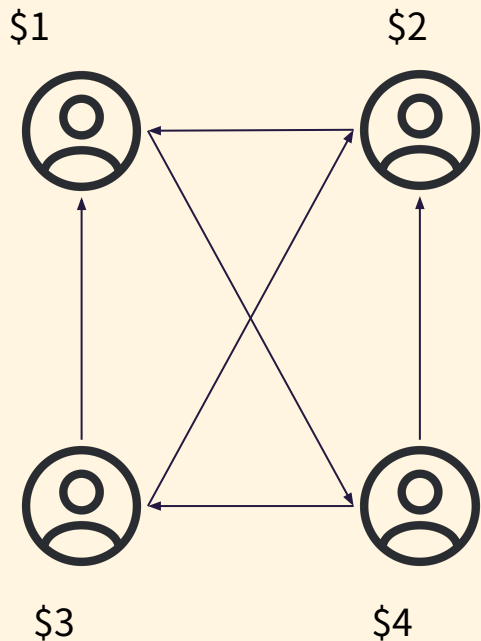
ブロックチェーンの種類

アカウント式 VS UTXO式

	アカウント式	UTXO 式
仕組み	ユーザアカウントの残高	コインの動き
例	Ethereum系	Bitcoin系
ネットワークの拡張性	スケールしない	スケールする
開発	比較的容易	複雑
トークン	可能	可能だが

ブロックチェーンの種類

アカウント式の弱点 グローバルステート

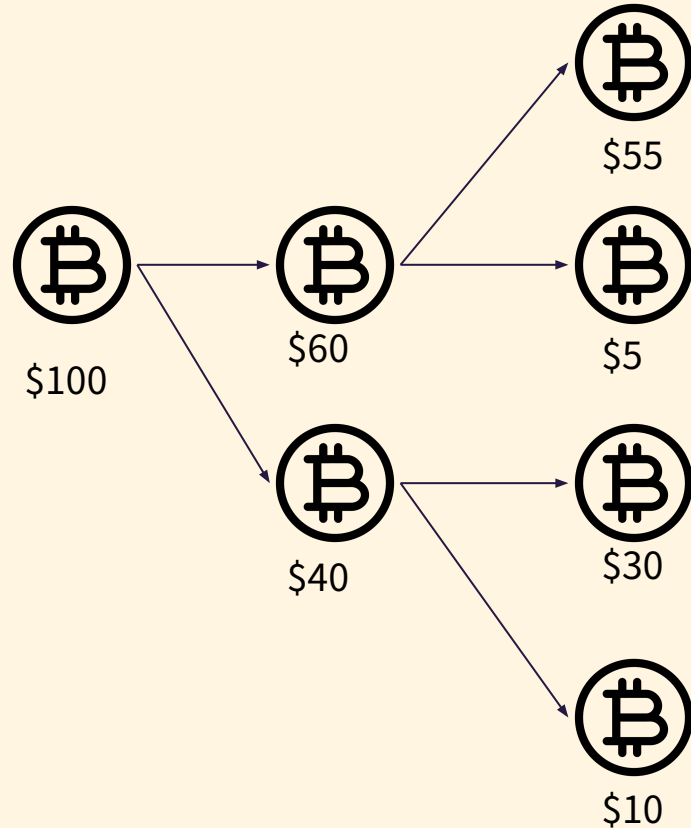


アカウント式

fx =SUM(B2:B5)	
A	B
合計	10
ユーザA	1
ユーザB	2
ユーザC	3
ユーザD	4

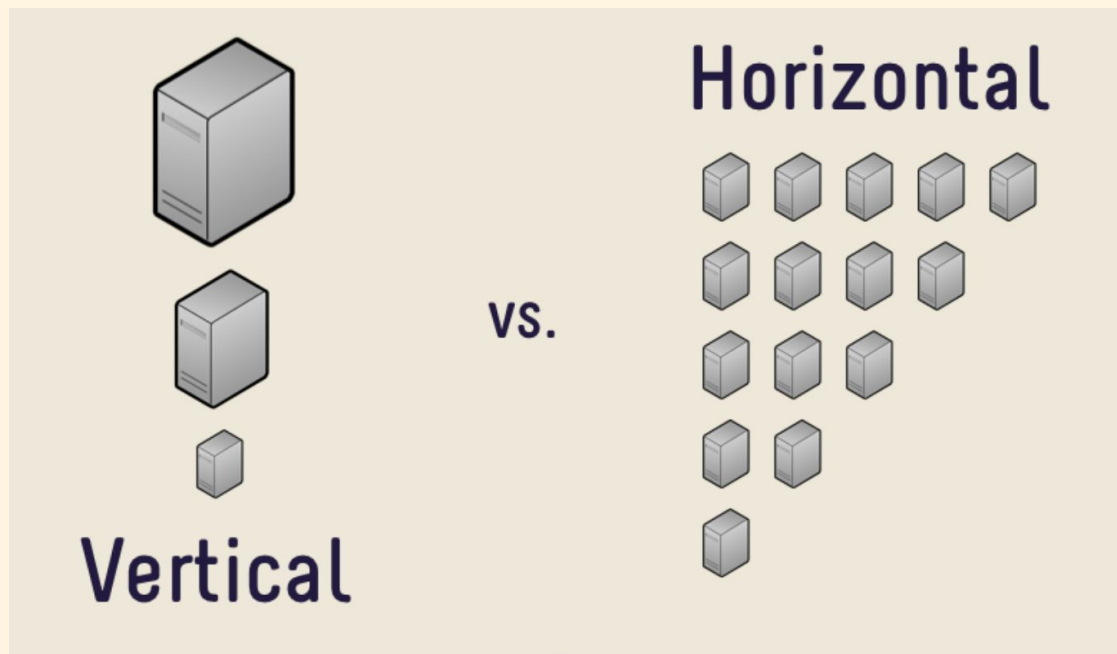
UTXO モデル

トークンの動きを追跡するデータ形式 一つずつのUnspent Transaction Outputs



ブロックチェーンの種類

アカウント式 VS UTXO式

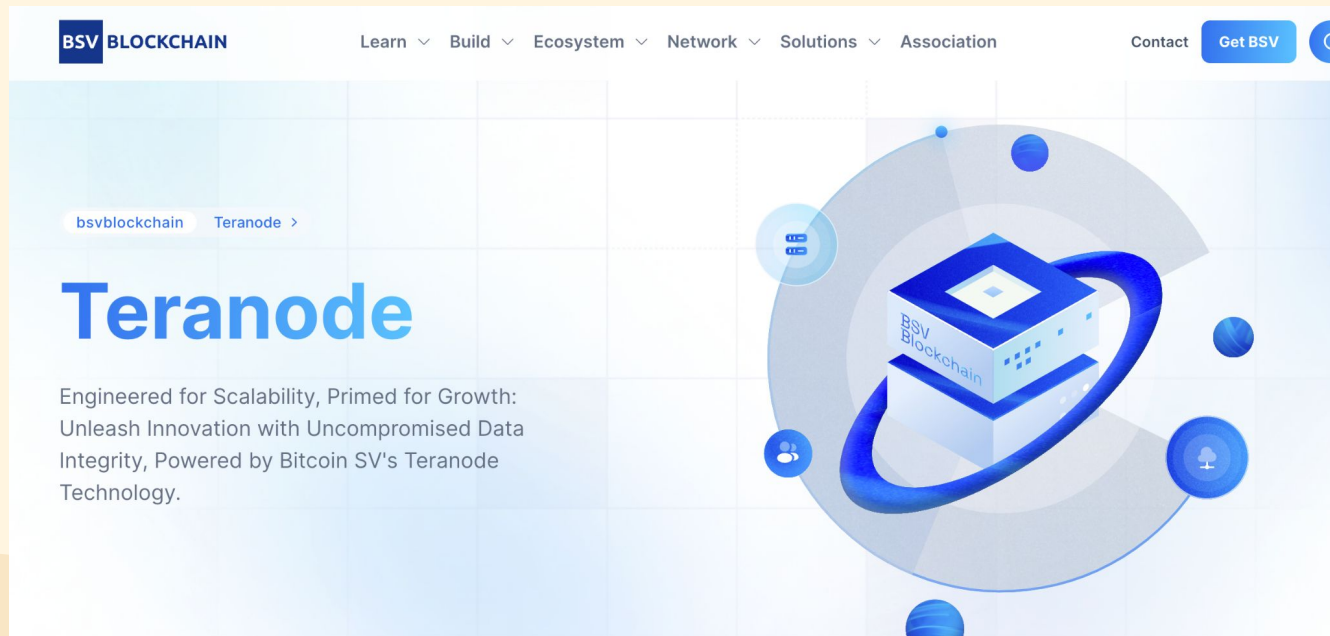


アカウント式

UTXO式

並列化できるかどうか

Teranode 次世代のマイニングソフトウェア



BSV BLOCKCHAIN

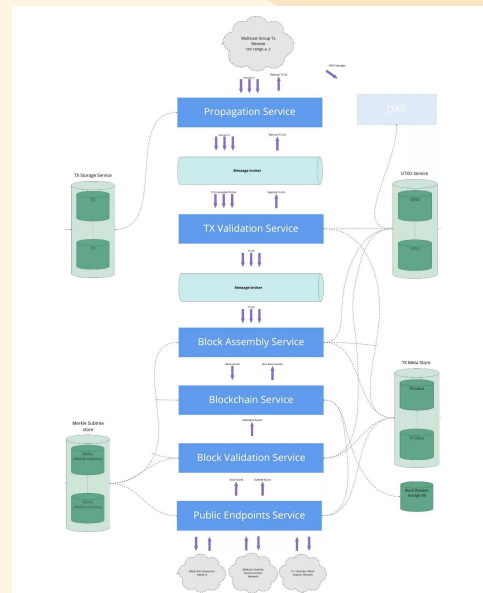
Learn ▾ Build ▾ Ecosystem ▾ Network ▾ Solutions ▾ Association

Contact Get BSV

bsvblockchain Teranode >

Teranode

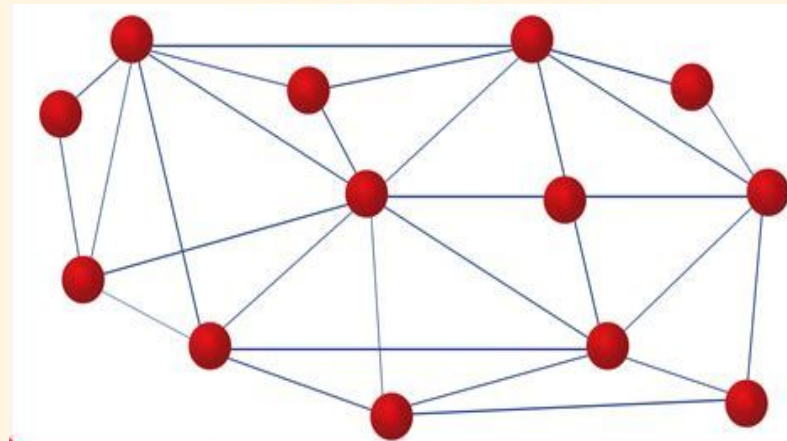
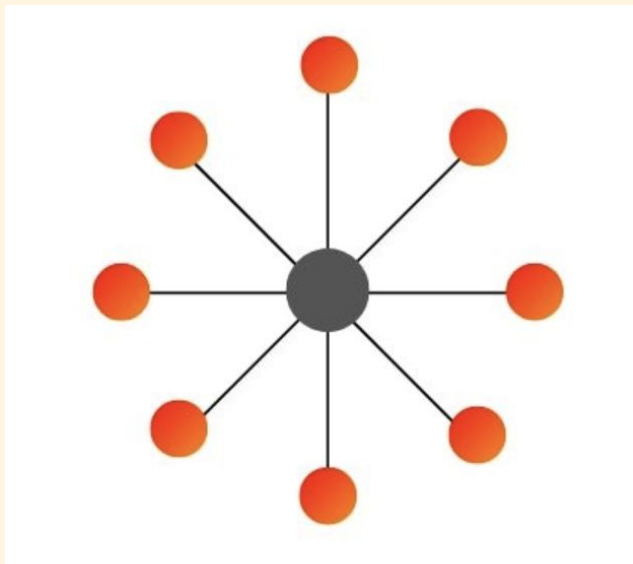
Engineered for Scalability, Primed for Growth:
Unleash Innovation with Uncompromised Data
Integrity, Powered by Bitcoin SV's Teranode
Technology.



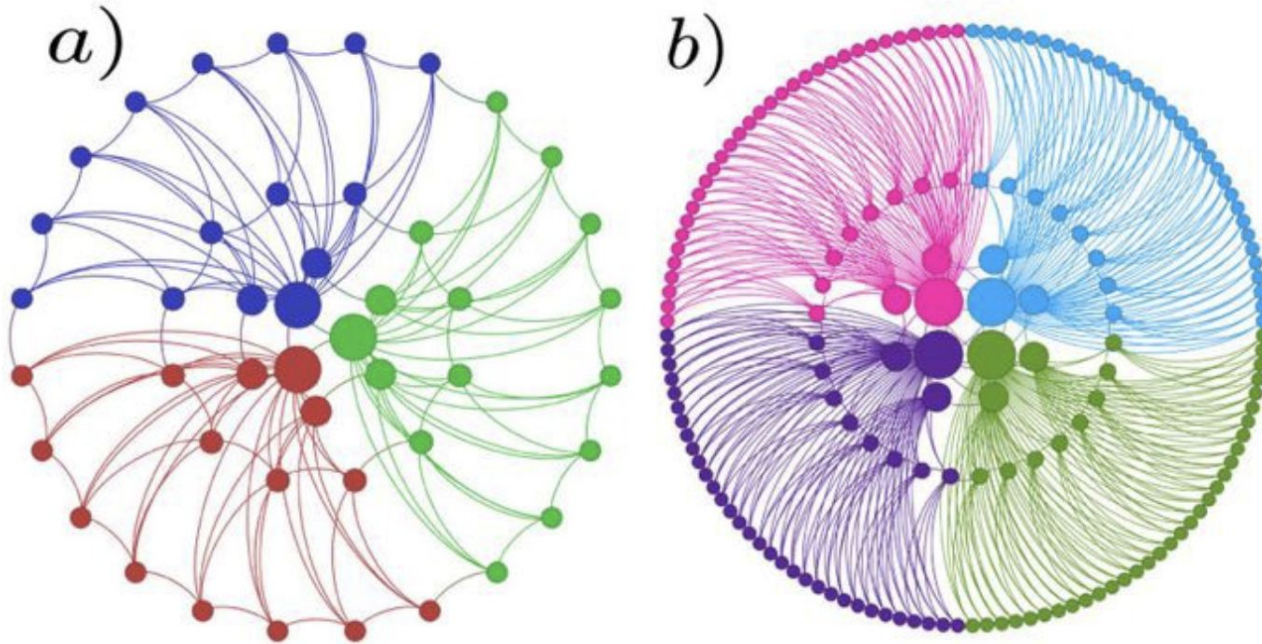
2. 分散型の壁

Network topology

分散か中央集権かそれが問題だ



Mandela Network



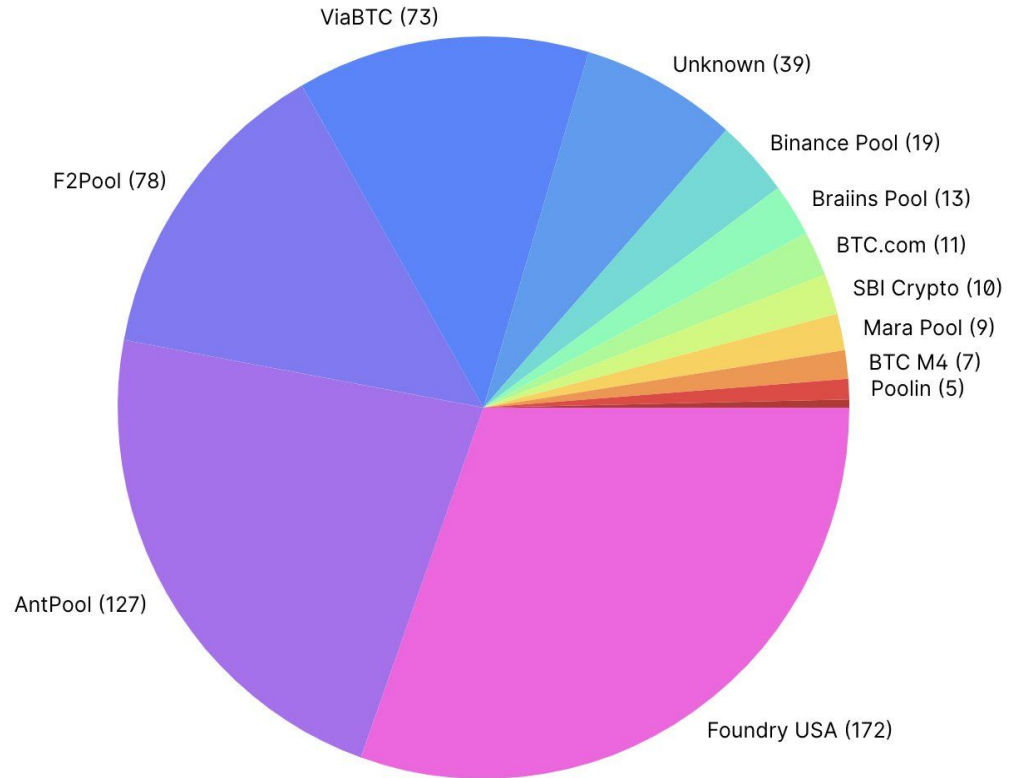
Bitcoin works in layers.

マイニングプール分布 BTC

tion

distribution amongst the largest mining pools.

7D 10D 6M 1Y 2Y 3Y

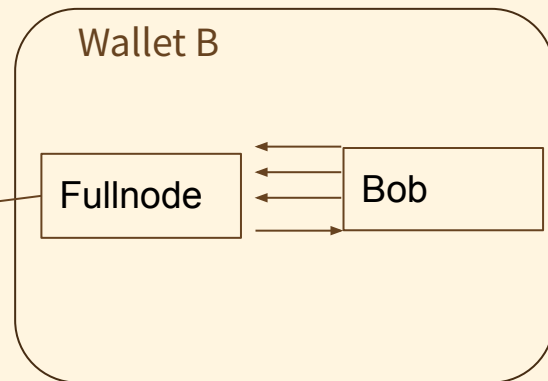
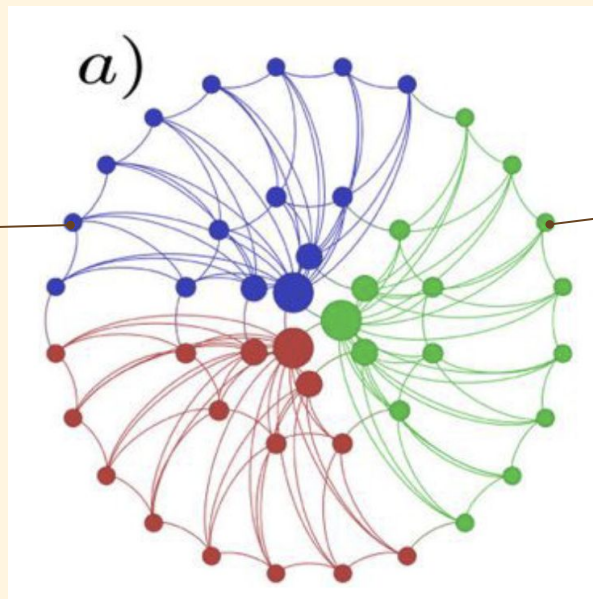
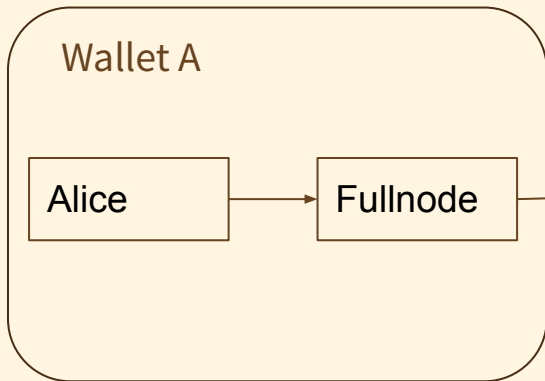


3. フルノード運用の壁

Conventional Wallet

現状のウォレットのtxの検証

Bitcoin network




スケーリングについてサトシ・ナカモトの意見 2008

今の技術でもVISAくらい処理できる、数ギガブロックは問題なし、専門のサーバーファームでマイニングされユーザーはSPVウォレットを使うことになる

If the network were to get that big, it would take several years, and by then, sending 2 HD movies over the Internet would probably not seem like a big deal.

Satoshi Nakamoto

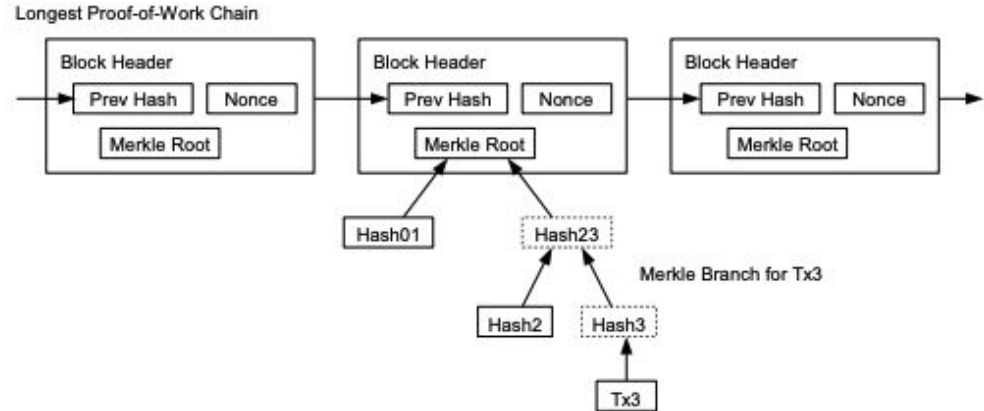
Long before the network gets anywhere near as large as that, it would be safe for users to use Simplified Payment Verification (section 8) to check for double spending, which only requires having the  ain of block headers, or about 12KB per day. Only people trying to create new coins would need to run network nodes. At first, most users would run network nodes, but as the network grows beyond a certain point, it

SPV

Simplified Payment Verification

8. Simplified Payment Verification

It is possible to verify payments without running a full network node. A user only needs to keep a copy of the block headers of the longest proof-of-work chain, which he can get by querying network nodes until he's convinced he has the longest chain, and obtain the Merkle branch linking the transaction to the block it's timestamped in. He can't check the transaction for himself, but by linking it to a place in the chain, he can see that a network node has accepted it, and blocks added after it further confirm the network has accepted it.




As such, the verification is reliable as long as honest nodes control the network, but is more vulnerable if the network is overpowered by an attacker. While network nodes can verify transactions for themselves, the simplified method can be fooled by an attacker's fabricated transactions for as long as the attacker can continue to overpower the network. One strategy to protect against this would be to accept alerts from network nodes when they detect an invalid block, prompting the user's software to download the full block and alerted transactions to confirm the inconsistency. Businesses that receive frequent payments will probably still want to run their own nodes for more independent security and quicker verification.

SPV

Simplified Payment Verification

SPV WALLET

ken@yenpoint.jp 

Transactions history

Page: 1

Sender/receiver	Amount	Status	Direction	Date
from: ken@yendopay.net	+ 0.00001187 BSV	●	⇩	18.03.2024, 14:19:22
to: ken@yendopay.net	- 0.00000101 BSV	●	⇧	16.03.2024, 18:20:30
to: erwrewer@bsv01.dais.cds.tohoku.ac.jp	- 0.00000201 BSV	●	⇧	15.03.2024, 15:27:58
to: ken@yendopay.net	- 0.00000789 BSV	●	⇧	12.03.2024, 16:35:09
from: kensato@simply.cash	+ 0.00000300 BSV	●	⇩	12.03.2024, 16:30:22
from: ysato@sp.buxbit.net	+ 0.00000002 BSV	●	⇩	12.03.2024, 10:35:25
to: ysato@sp.buxbit.net	- 0.00000004 BSV	●	⇧	12.03.2024, 10:31:55
from: ysato@sp.buxbit.net	+ 0.00000002 BSV	●	⇩	12.03.2024, 10:28:45
to: ysato@sp.buxbit.net	- 0.00000004 BSV	●	⇧	12.03.2024, 10:27:55
from: yasu@bsvyendo.info	+ 0.00000100 BSV	●	⇩	11.03.2024, 19:37:28

1 2 3 4 5 6 7

Your total balance

ken@buxtest.net

0.00075086 BSV

75086 sat.

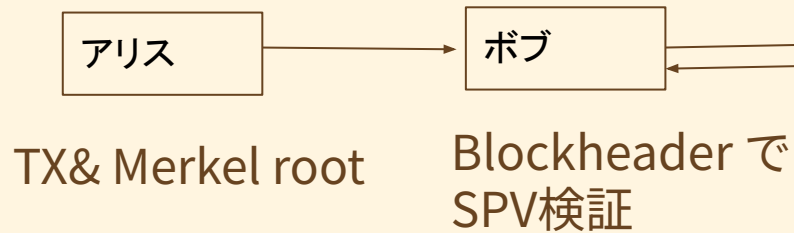
0.06235992414666667 USD

Send money

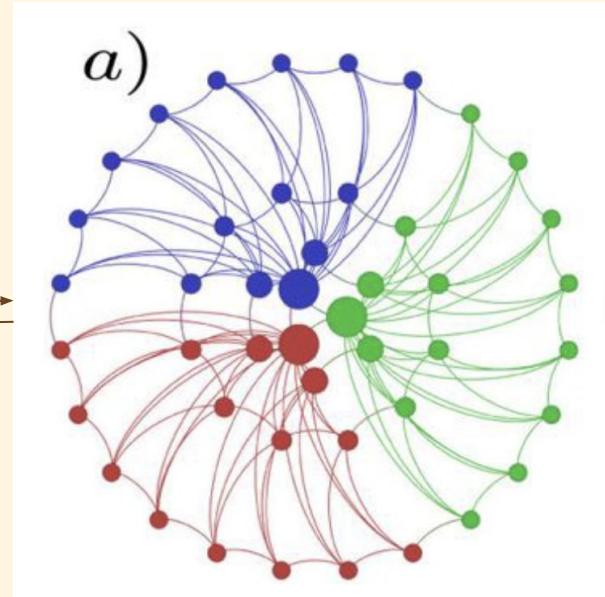
BSV: 0.00000000

SPV Wallet

SPVでP2PでTXの簡易検証

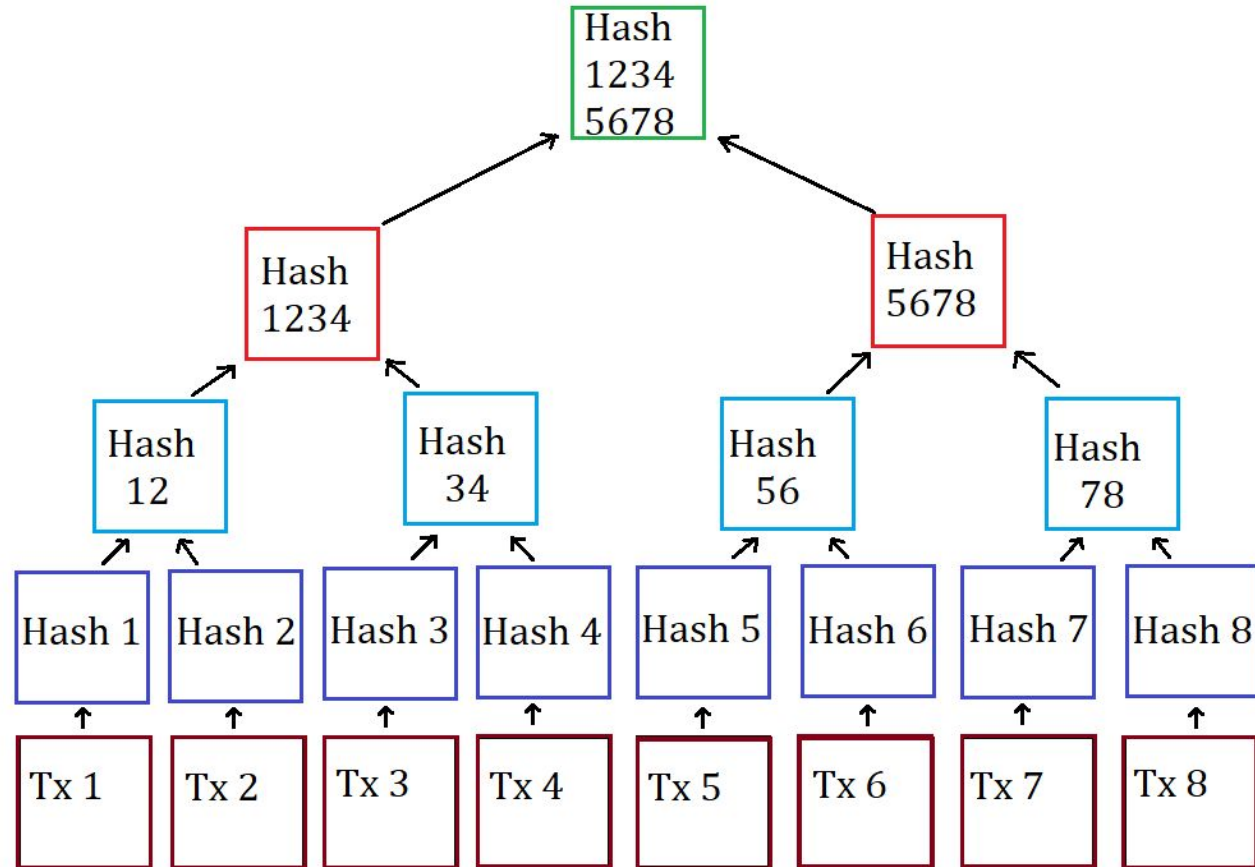


Bitcoin network



Merkel Tree

Simplified Payment Verification



Bitcoin Block

Tx1

Tx2

Tx3

Tx4

Tx5

.

.

.

.

.

.

.

.

Tx100

Bitcoin Block

Tx1

Tx2

Tx3

Tx4

Tx5

.

.

.

.

.

.

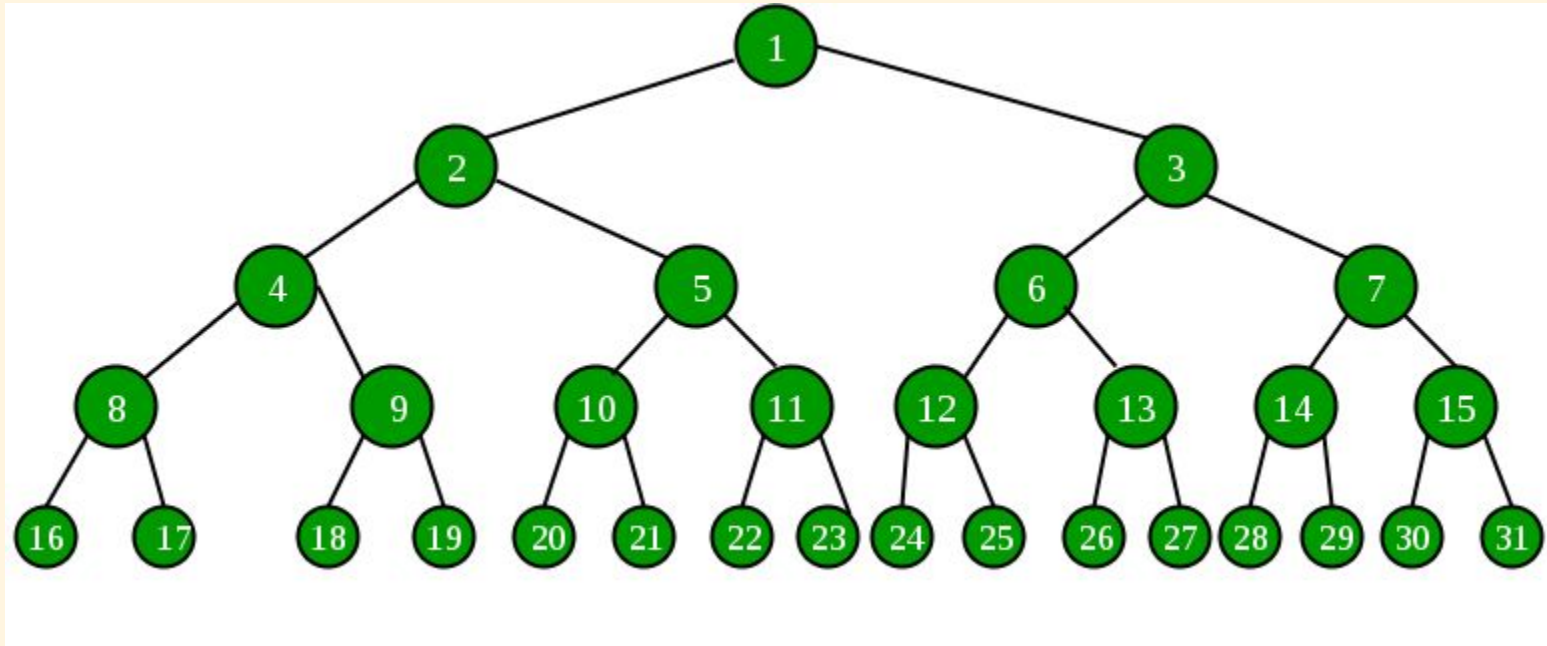
.

.

Tx1,000,000,000

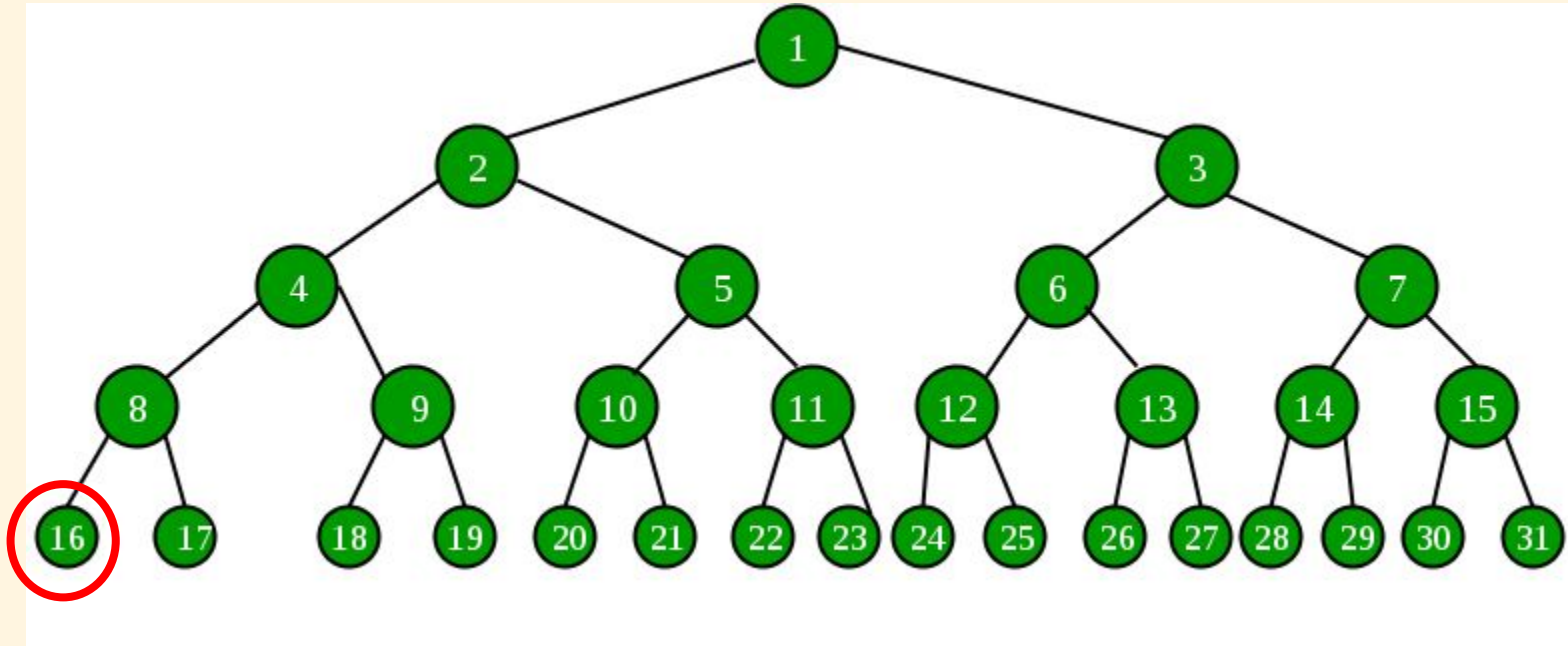
Merkel Tree

Simplified Payment Verification



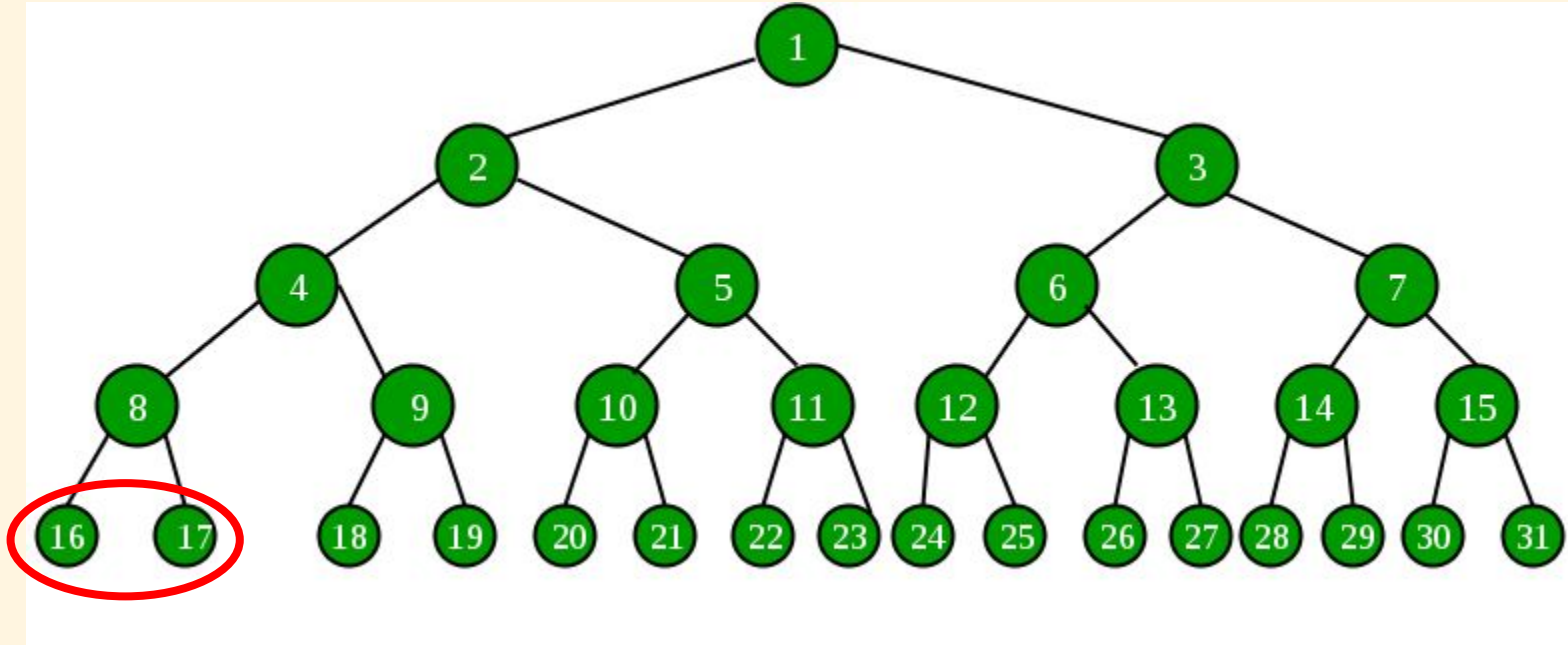
Merkel path

Simplified Payment Verification



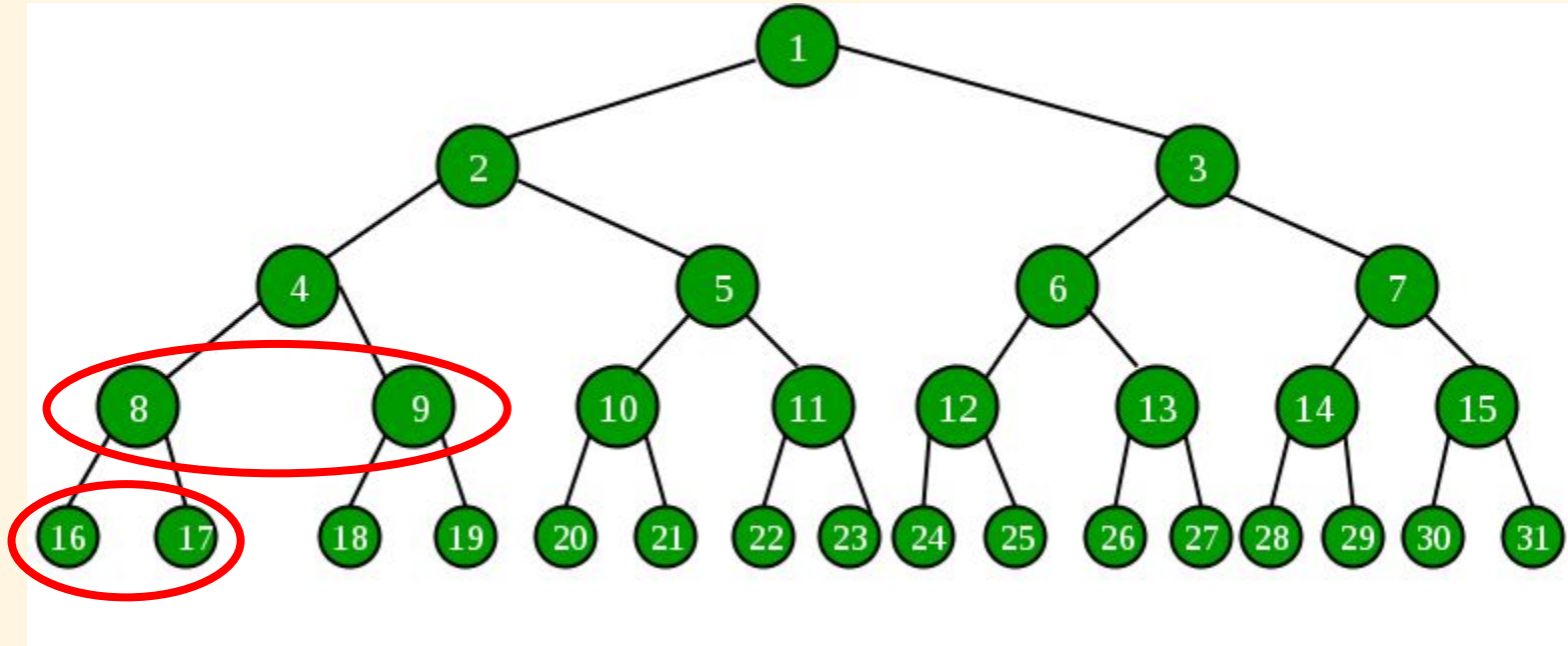
Merkel path

Simplified Payment Verification



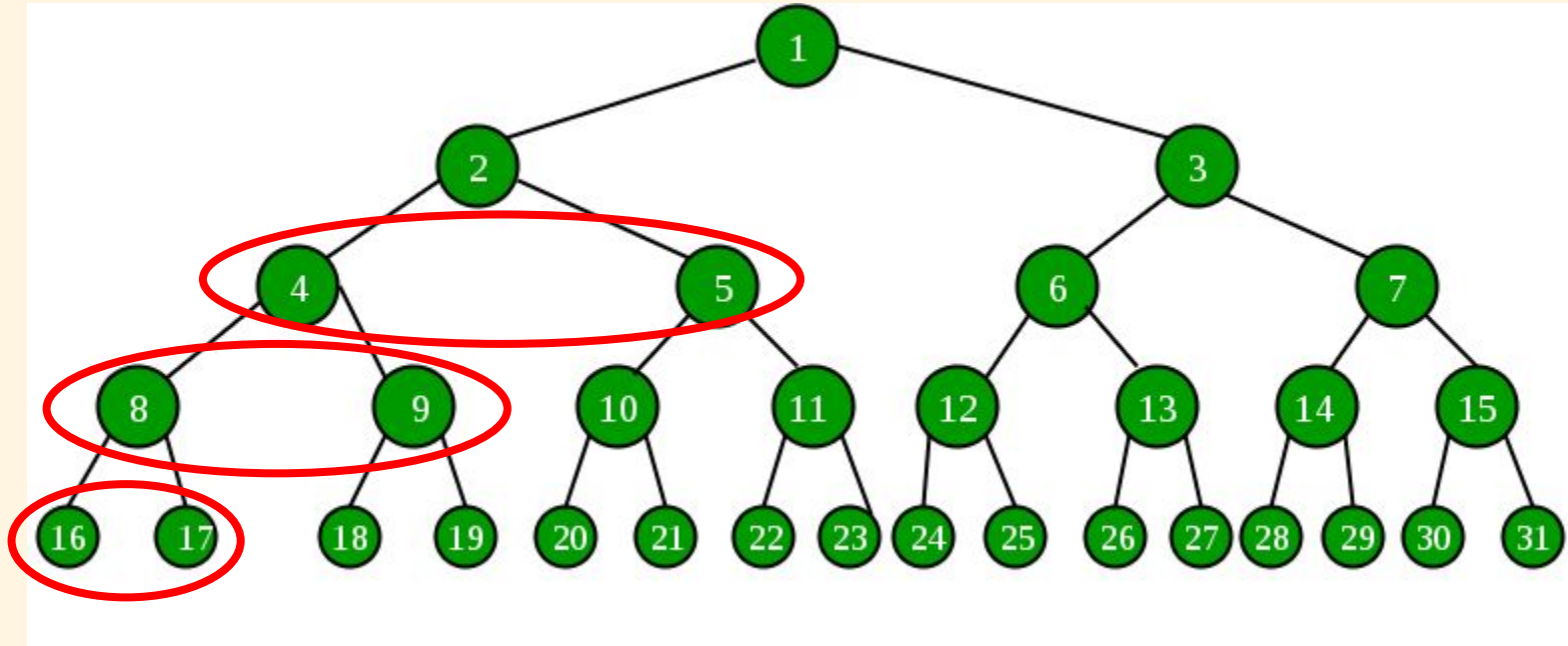
Merkel path

Simplified Payment Verification



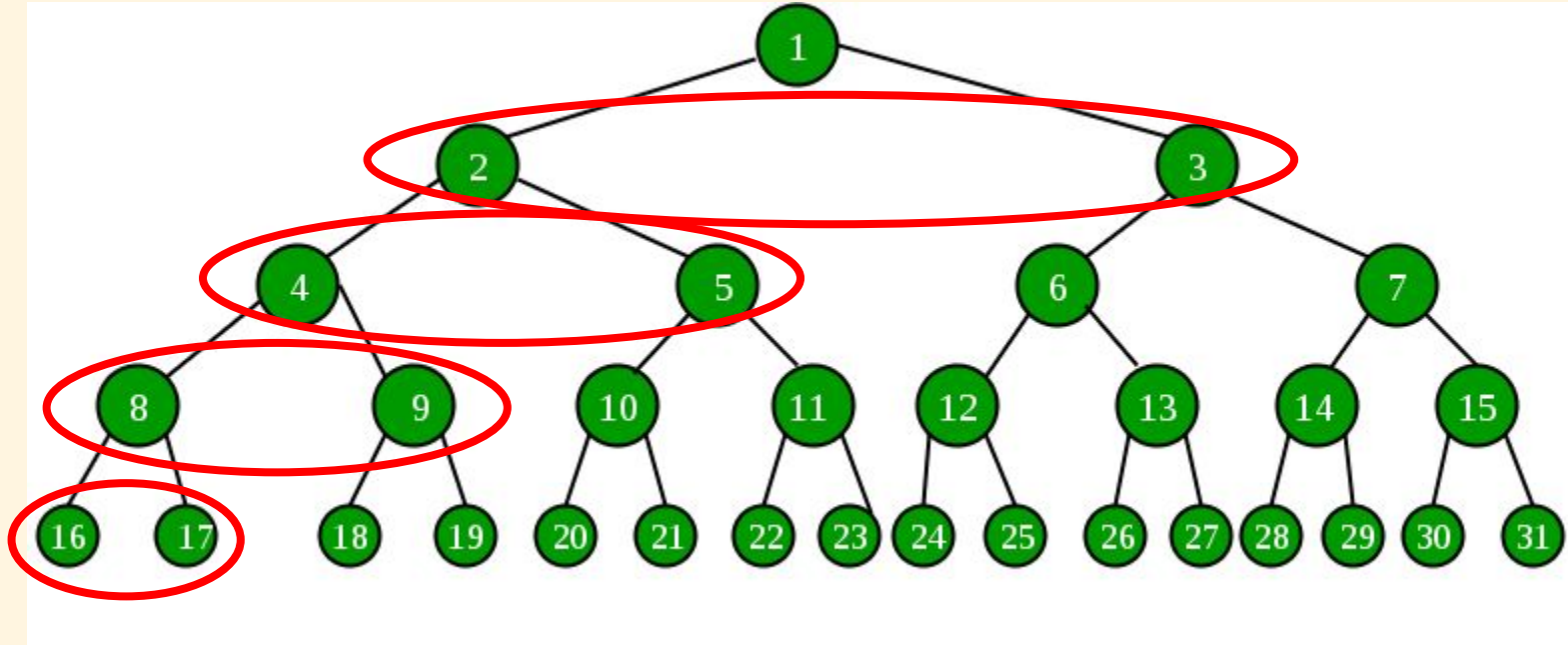
Merkel path

Simplified Payment Verification



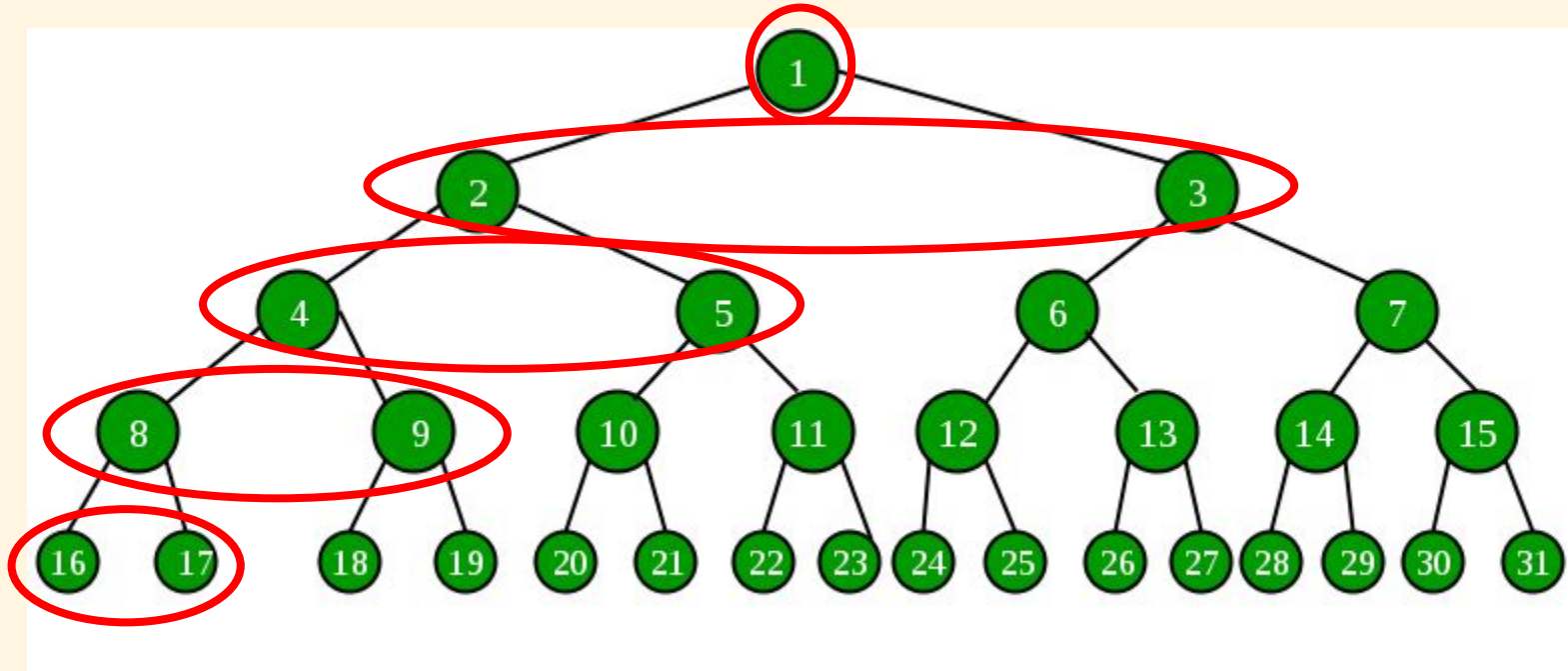
Merkel path

Simplified Payment Verification



Merkel path

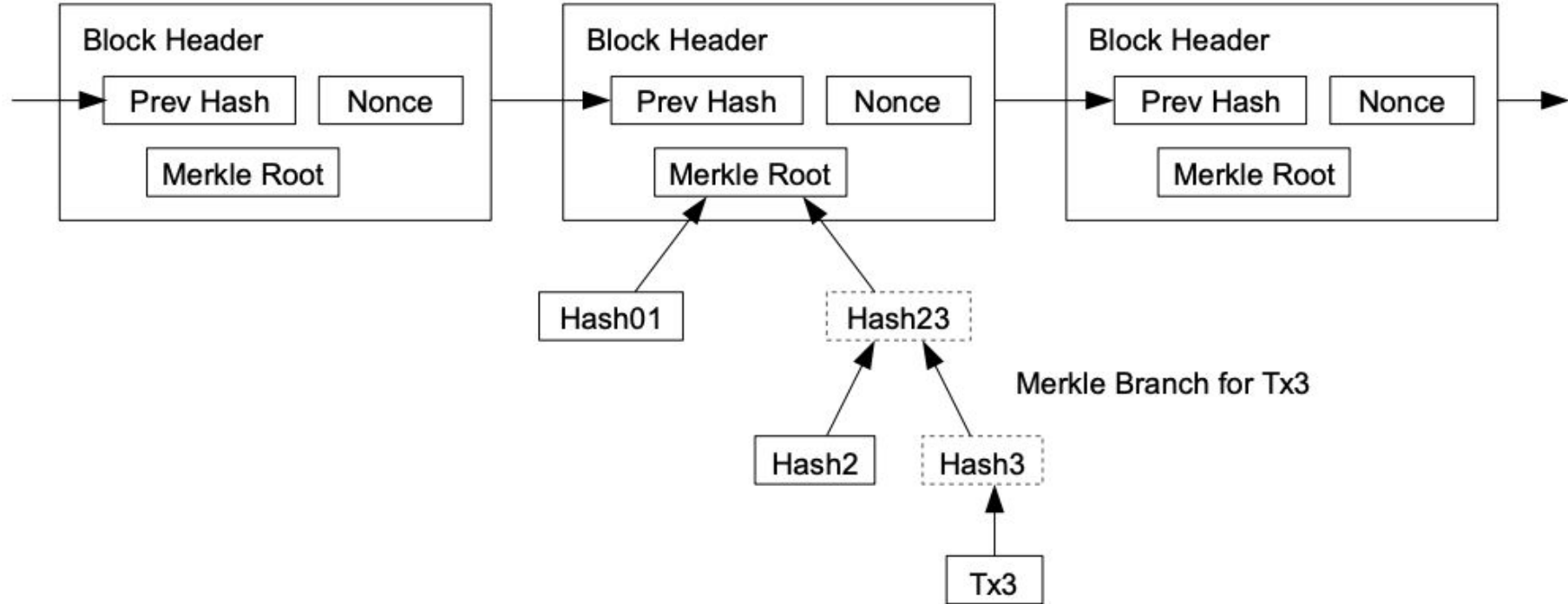
Simplified Payment Verification



Merkel path

Simplified Payment Verification

Longest Proof-of-Work Chain



4. UTXOのトークンの壁

Bitcoin Script

ビットコイン スマートコントラクト Forthのような言語

Splice

If any opcode marked as disabled is present in a script, it must abort and fail.

Word	Opcode	Hex	Input	Output	Description
OP_CAT	126	0x7e	x1 x2	out	Concatenates two strings. <i>disabled.</i>
OP_SUBSTR	127	0x7f	in begin size	out	Returns a section of a string. <i>disabled.</i>
OP_LEFT	128	0x80	in size	out	Keeps only characters left of the specified point in a string. <i>disabled.</i>
OP_RIGHT	129	0x81	in size	out	Keeps only characters right of the specified point in a string. <i>disabled.</i>
OP_SIZE	130	0x82	in	in size	Pushes the string length of the top element of the stack (without popping it).

Bitwise logic

If any opcode marked as disabled is present in a script, it must abort and fail.

Word	Opcode	Hex	Input	Output	Description
OP_INVERT	131	0x83	in	out	Flips all of the bits in the input. <i>disabled.</i>
OP_AND	132	0x84	x1 x2	out	Boolean <i>and</i> between each bit in the inputs. <i>disabled.</i>
OP_OR	133	0x85	x1 x2	out	Boolean <i>or</i> between each bit in the inputs. <i>disabled.</i>
OP_XOR	134	0x86	x1 x2	out	Boolean <i>exclusive or</i> between each bit in the inputs. <i>disabled.</i>
OP_EQUAL	135	0x87	x1 x2	True / false	Returns 1 if the inputs are exactly equal, 0 otherwise.
OP_EQUALVERIFY	136	0x88	x1 x2	Nothing / fail	Same as OP_EQUAL, but runs OP_VERIFY afterward.

Arithmetic

sCrypt

Typescript でビットコインのスマートコントラクトを構築



P2PKH

```
export class P2PKH extends SmartContract {
  @prop()
  readonly pubKeyHash: PubKeyHash

  constructor(pubKeyHash: PubKeyHash) {
    super(...arguments)
    this.pubKeyHash = pubKeyHash
  }

  @method()
  public unlock(sig: Sig, pubkey: PubKey) {
    assert(
      hash160(pubkey) == this.pubKeyHash,
      'public key hashes are not equal'
    )
    assert(this.checkSig(sig, pubkey), 'signature invalid')
  }
}
```

ZK-Rollup

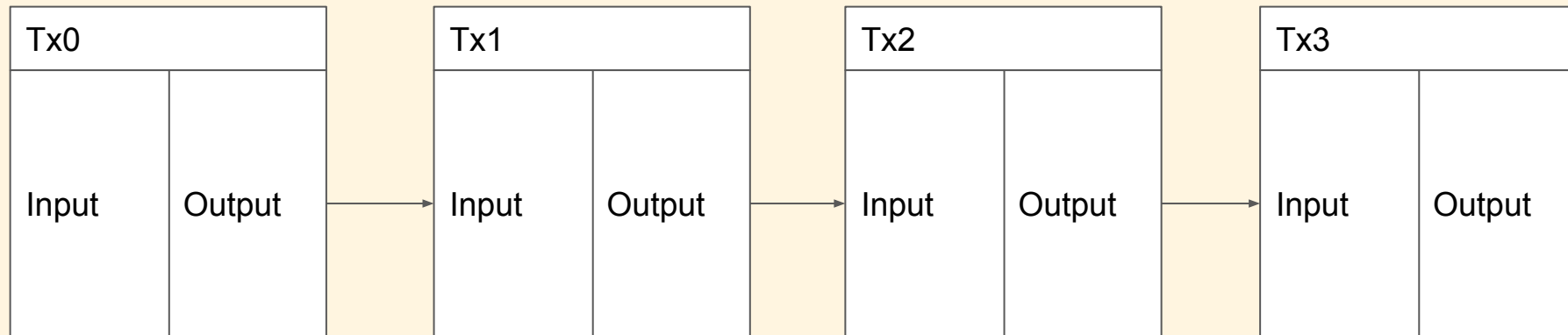
```
let vk_x = vk.gammaAbc[0]
for (let i = 0; i < N_PUB_INPUTS; i++) {
  const p = BN256.mulG1Point(vk.gammaAbc[i + 1], inputs[i])
  vk_x = BN256.addG1Points(vk_x, p)
}

const a0: G1Point = {
  x: proof.a.x,
  y: -proof.a.y,
}

return BN256Pairing.pairCheckP4Precalc(
  a0,
  proof.b,
  vk.millerb1a1,
  vk_x,
  vk.gamma,
  proof.c,
  vk.delta
)
```

Back to Genesis

信頼する第三者のIndexer なしでトークンが困難
スケーラビリティが低い



出願人又は代理人の書類記号 001	今後の手続 については、	様式PCT/ISA/220 及び下記5を参照すること。
国際出願番号 PCT/JP2023/001	国際出願日 (日.月.年) 26.08.2023	優先日 (日.月.年)
出願人 (氏名又は名称) 円ポイント株式会社		

国際調査機関が作成したこの国際調査報告を法施行規則第41条 (PCT18条)の規定に従い出願人に送付する。
この写しは国際事務局にも送付される。

この国際調査報告は、全部で 3 ページである。

この国際調査報告に引用された先行技術文献の写しも添付されている。

1. 国際調査報告の基礎

a. 言語に関し、この国際調査は以下のものに基づき行った。

出願時の言語による国際出願

出願時の言語から国際調査のための言語である _____ 語に翻訳された、この
国際出願の翻訳文 (PCT規則12.3(a)及び23.1(b))

b. この国際調査報告は、PCT規則91の規定により国際調査機関が許可した又は国際調査機関に通知された明
らかな誤りの訂正を考慮して作成した (PCT規則43.6の2(a))。

c. この国際出願は、スクレオチド又はアミノ酸配列を含んでいる (第I欄参照)。

2. 請求の範囲の一部の調査ができない (第II欄参照)。

3. 発明の単一性が欠如している (第III欄参照)。

4. 発明の名称は

出願人が提出したものを承認する。

次に示すように国際調査機関が作成した。

5. 要約は

出願人が提出したものを承認する。

第IV欄に示されているように、法施行規則第47条第1項 (PCT規則38.2)の規定により国際調査機関が作
成した。出願人は、この国際調査報告の発送の日から1月以内にこの国際調査機関に意見を提出することが
できる。

6. 図面に関して

a. 要約とともに公表される図は、第 5 図とする。

出願人が示したとおりである。

出願人は図を示さなかったため、国際調査機関が選択した。

本図は発明の特徴を一層よく表しているため、国際調査機関が選択した。

b. 要約とともに公表される図はない。

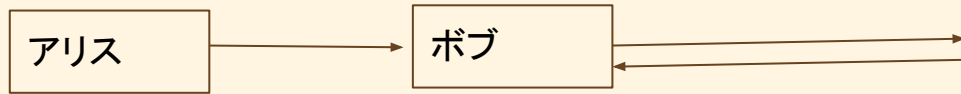
Simplified Token Velification

Yenpoint 特許技術

- Trustless
- 中央Indexerに依存しない
- スケーラビリティが高い
- SPVとの親和性が高い

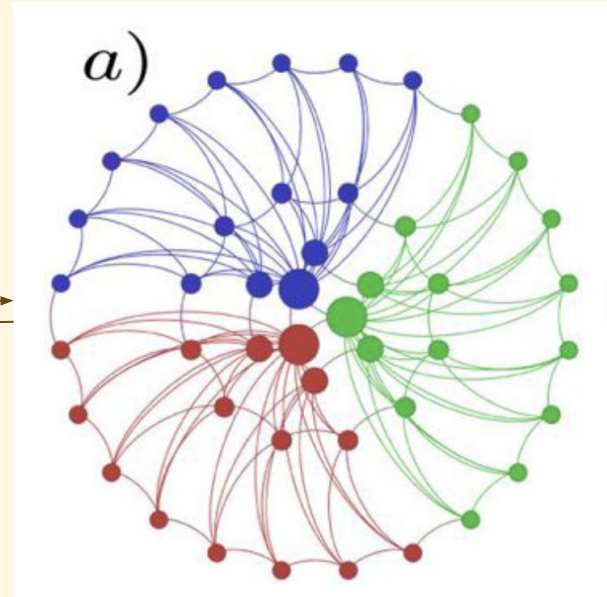
STV Wallet

Yenpoint 特許技術
P2Pでトークンを検証に



Chain of TXs (token) & Merkel Path Blockheader で検証

Bitcoin network

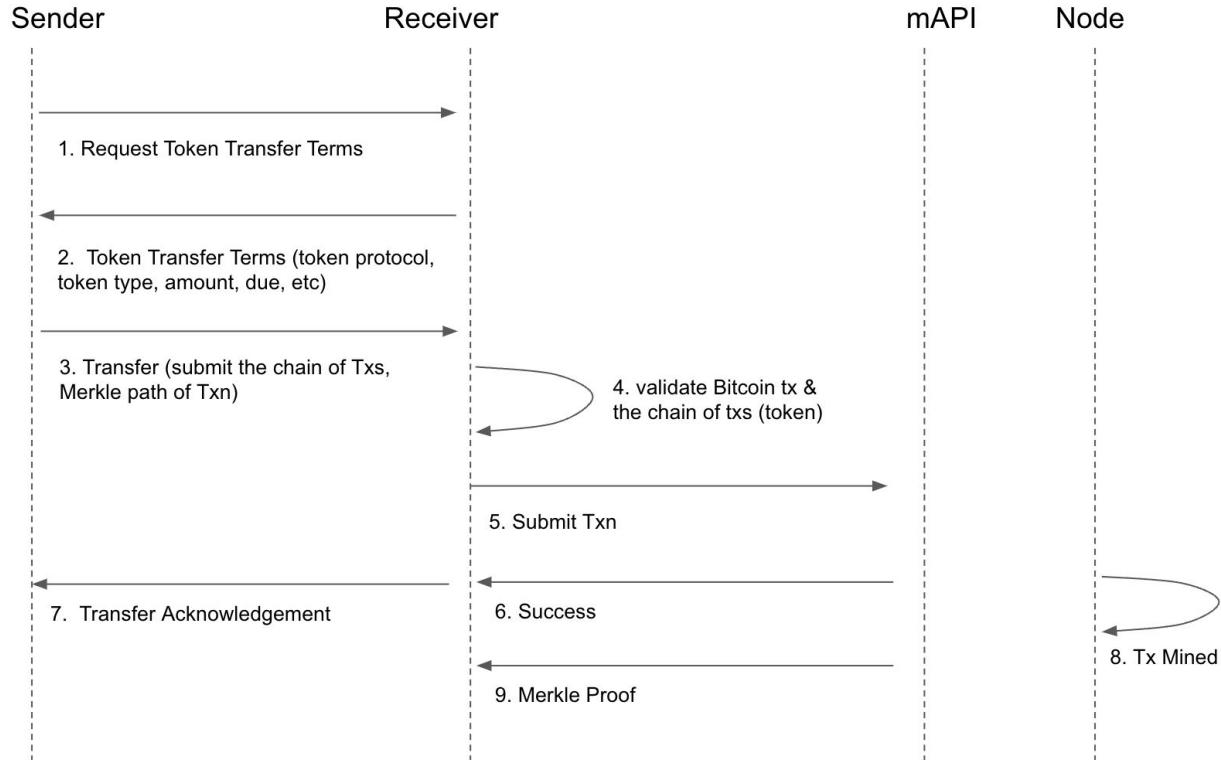


Technical Advantages

STVP on SPV Wallets



STVP on SPV sequence diagram



BEEF

STV on SPV Wallets

Field	Description	Size
Version no	Version number starts at 4022206465, encoded Uint32LE ⇒ <code>0100BEEF</code>	4 bytes
nBUMPs	VarInt number of BSV Unified Merkle Paths which follow	1-9 bytes
BUMP data	All of the BUMPs required to prove inclusion of inputs in longest chain of blocks BRC-74	many bytes x nBUMPs
nTransactions	VarInt number of transactions which follow	1-9 bytes
Raw Transaction	RawTx bytes as in standard format BRC-12	many bytes
Has BUMP	<code>01</code> if so, followed by the BUMP index; <code>00</code> if not, followed by nothing.	1 byte
BUMP index	VarInt index number - indicating the BUMP to which the prior tx belongs if there is one.	1-9 bytes

BEEF

STVP on SPV Wallets

ここにChain
of TXを埋め
込む

0100beef **version**

01 **how many merkle paths**

fe8ec00c000a025c009d625558be035fa56c1e69f19bbdbba3a7b50ce574154b458424947e01a2ec415
d0281f639c2690b6963163cd1ea23227ed7d3ccd92c1d981f6b9c45053ff80b8b61012f00e1b04d137f
60efcce9caf3622d096295fe69367a037843ba041f0c66521d205d0116001d44cca0e22453bd85ca4fa0
ca8f88947c9dea1f5e1950bda8000e8fd1bd066f010a001ec0ce29cbb7c731c85a496c5a3268118b9da6
f0c118b763140be2bdabaf96d60104009dd319edd80695d478939e03fea48cdb68c1b7478cf9e1858a1
f8c4f916e0a650103006d7b96ed87cb6efc68364a5a11ae39a9b2eedae7713ab7a1bbfd4a3c8285df010
10000bca101132258ad7d68ef4398437943d6ed98bbfd6d89068f7f68812d9c01947b0101008e9994d
ba949fb7fddb6443111d07cd3b1eecd415d8d917f7daf02abaf98e2b50101004f4571db8036f4f867858
1aade26f0c67b0380ededab9d05a2b117d1c723db7801010018e8e20fc143d7c34e8d670b0b1bf73f8c
a4236472264dbc4a65386c0dfa8fd **merkle path**

02 **how many transactions**

010000000144b164db1fa1a5a230aca78ce3f5ecec9c5f5b4601ca4d8676dcc0d2e8d2c01000000006b
483045022100b295f687c13d968440ea82836965cfa94c656a56642e68d16059dc703f8bdf84022007
8c7943435716f0ee15627fbbf318e136b4ea42e1df46e3fac4cba5227c3dfd41210286039ef5a252cac96
5c68b374e06ea88cd27c74fa9be0bf9dc710d148abb5f39ffffff023c330000000000001976a91455daf
4e5fedb28c57835acca9318d1faa4bc331188ac3c330000000000001976a91455daf4e5fedb28c57835a
cca9318d1faa4bc331188ac00000000 **parent transaction**

01000100000001 **81f639c2690b6963163cd1ea23227ed7d3ccd92c1d981f6b9c45053ff80b8b61**

000000006a473044022045287fac6218b8a217b0157cacf9d281b5f39577d49db8b7fac54cb215dc2f0
a022075b5a291a8ad1c439ac7ac9d4a3cc0aed7189a48ec08e78f78476474368e030341210286039ef5
a252cac965c68b374e06ea88cd27c74fa9be0bf9dc710d148abb5f39ffffff013a330000000000001976
a91455daf4e5fedb28c57835acca9318d1faa4bc331188ac0000000000 **current**

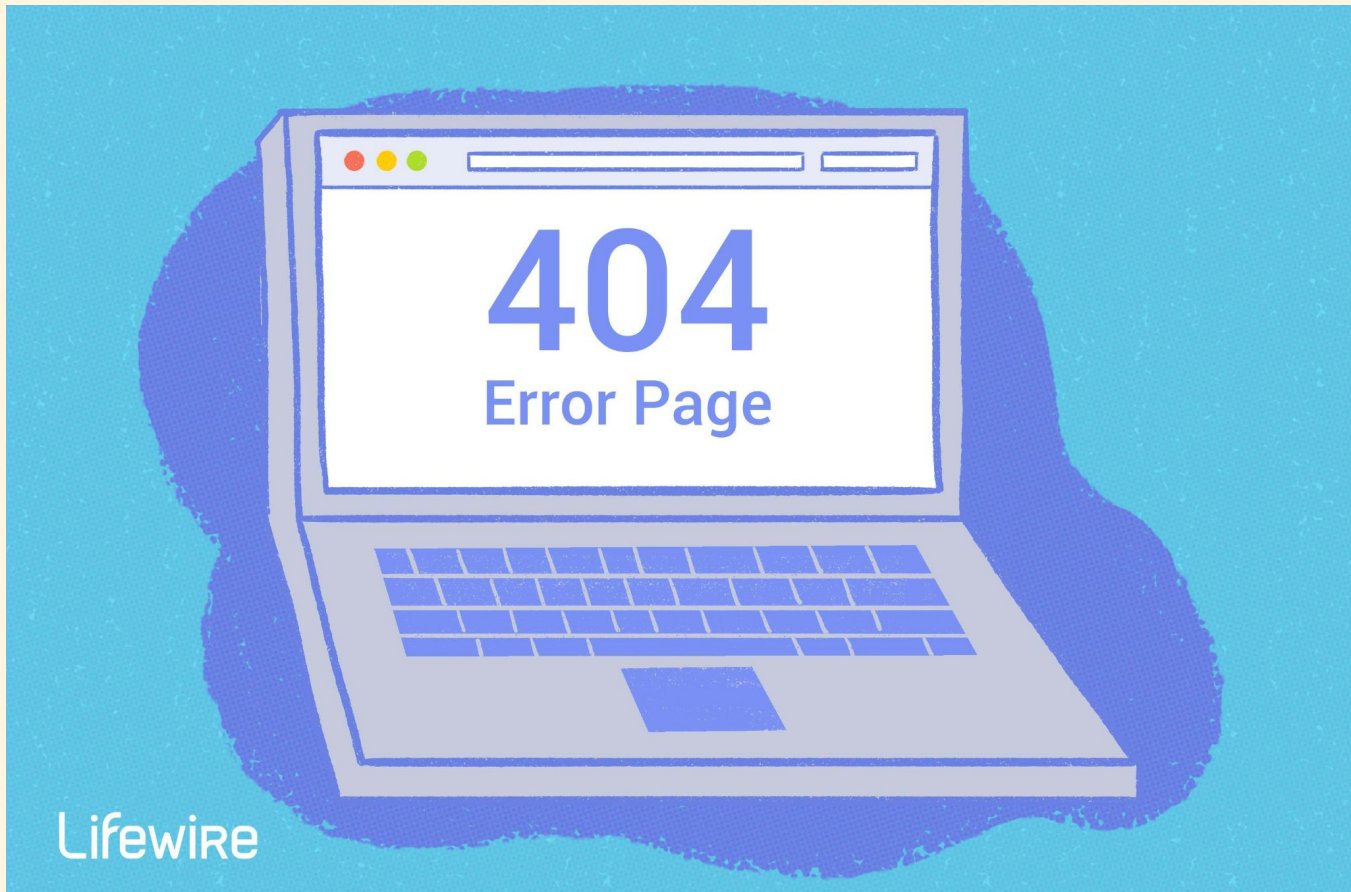
transaction (編集済み)

ブロックチェーンの今後

Bitcoin年表



マイクロペイメントの実現



Lifewire

マイクロペイメントの実現

Http 402 payment reauired

MDN Web Docs

References

Guides

Plus

Curriculum NEW

Blog

Play

AI Help BETA

Theme

References > HTTP > HTTP response status codes > 402 Payment Required

Filter

304 Not Modified

307 Temporary Redirect

308 Permanent Redirect

400 Bad Request

401 Unauthorized

402 Payment Required

403 Forbidden

404 Not Found

405 Method Not Allowed

406 Not Acceptable

407 Proxy Authentication Required

408 Request Timeout

402 Payment Required

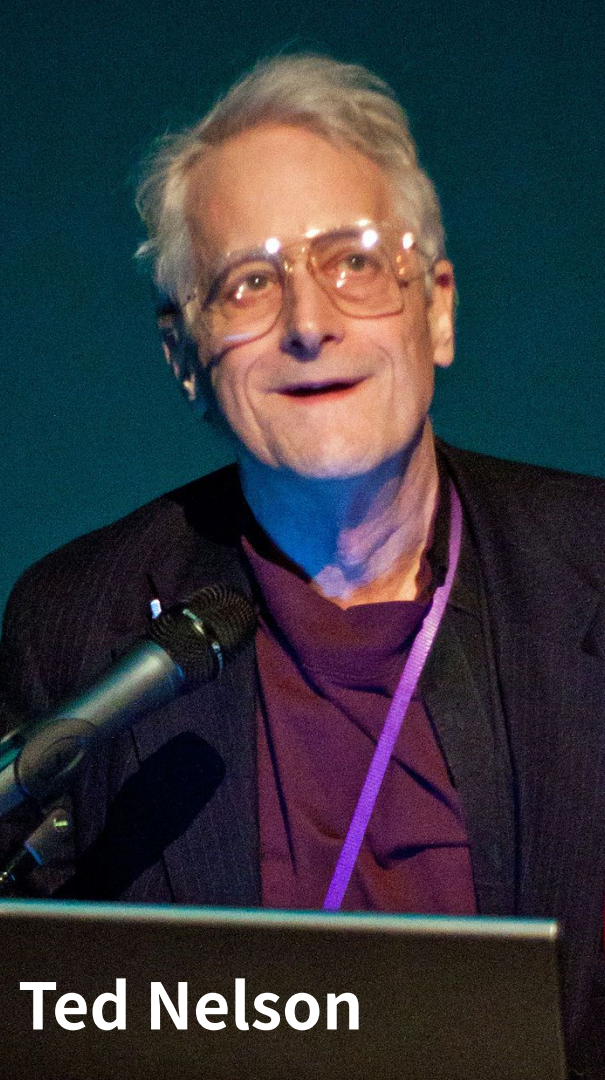


Experimental: This is an **experimental technology**.

Check the [Browser compatibility table](#) carefully before using this in production.

The HTTP **402 Payment Required** is a nonstandard response status code that is reserved for future use. This status code was created to enable digital cash or **(micro) payment systems** and would indicate that the requested content is not available until the client makes a payment.

Sometimes, this status code indicates that the request cannot be processed until the client makes a payment. However, no standard use convention exists and different entities use it in different contexts.



Ted Nelson



Tim Berners-Lee



Marc Andreessen

BSV処理能力 世界新記録

全銀ネットの18倍の処理 1億2000万TX/day



参考:全銀ネット
日平均約675万tx/day

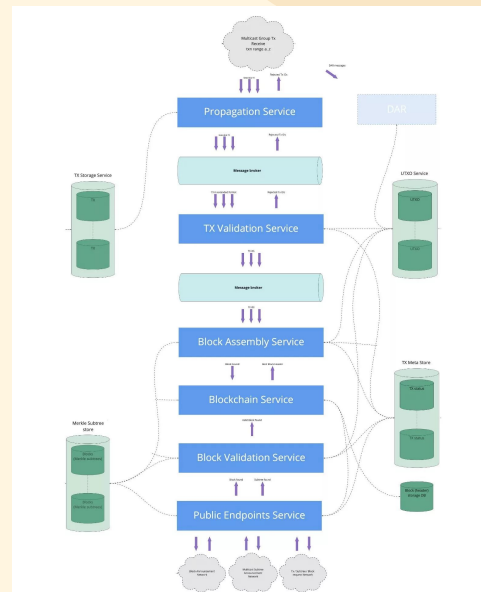
https://coinmystique.com/bsv-blockchains-record-breaking-128-million-transactions-have-been-natural-a-case-for-real-world-testing/?feed_id=1356

88...unique_id=6546b4cc2c27c

テストネットで300GB生成2024

Single thread vs 並列処理へ 毎秒百万txへの挑戦

The screenshot shows the BSV Blockchain website. At the top, there is a navigation bar with links for 'Learn', 'Build', 'Ecosystem', 'Network', 'Solutions', and 'Association', along with a 'Contact' button and a 'Get BSV' button. Below the navigation, there is a search bar with 'bsvblockchain' and 'Teranode' entered. The main heading is 'Teranode' in large blue letters. Below the heading, the text reads: 'Engineered for Scalability, Primed for Growth: Unleash Innovation with Uncompromised Data Integrity, Powered by Bitcoin SV's Teranode Technology.' To the right of the text is a 3D illustration of a blue cube labeled 'BSV Blockchain' with a blue ring around it, surrounded by various icons representing blockchain concepts.



Lightning に致命的なバグ

もしかしてそれは仕様ではありませんか？ 2023.10

10/24/2023 · 448 tuned in

第10回ライトニング開発者スペース



Koji Higashi
Host



Shigeyuki ✓
Speaker



yuya 🌱
Speaker



かな ⚡ 🛡️
Speaker



Shigeyuki Azuchi ✓

@techmedia_think

Develop with pleasure! CTO at chaintope, Inc.

Book (amzn.to/3xjNYXH)

npub1km5zgre7f5vxr6jgf32x055xlk3gjwrj5s4aedeyz6gr8l2yw0s8mmmlp

「資金をルーティング中に奪われる攻撃です。綺麗にごっそり取られてします。緩和策があるけど根本的に防ぐことができない。」
プロトコル変えれば？

「プロトコルを変えて、解決する問題でもないようだ。」

「攻撃を成功するためには、サンドイッチのように攻撃者を挟み込んで、おこなる。受取人 プレイメージを公開しないと、タイムアウトする。」

タイムアウトした後で、もらえるはずの回収するお金が、競合するトランザクションがネットワークに送信され、手数料が高く設定すれば、そちらに取り込まれてしまう。H TLCが奪取される可能性がある
さらに、被害者の上流も送金分の資金を全部奪われる可能性ある。」

https://twitter.com/Coin_and_Peace/status/1716771594377494633

Lightning is Dead!

Bitcoin core 開発者の告白 2023.10



Udi Wertheimer
@udiWertheimer

"I consider LN a done deal. The reasons were briefly posted on twitter already but since twitter account is deleted I'll provide them again here.

1) Serious LN dev is hard and time consuming, I no longer have time or

custodial one in UX terms and historically we see that majority of remaining users consistently choose convenience over control. This makes developing end-user non-custodial LN solutions feel like the most thankless thing in the world"

- Anton Kumaigorodski, developer of the first mobile lightning wallet

[DeepLで翻訳する](#)

7:40 AM · Oct 31, 2023 · 233.1K Views

113

191

603

122



<https://twitter.com/udiWertheimer/status/1719122153155473492>



Ken Sato (佐藤研一朗) @Uncle_Nakamoto · Oct 22

Lightning is finally officially dead after five times of 18 months later?

[DeepLで翻訳する](#)

WhaleWire @WhaleWire · Oct 21

BREAKING:

One of the top #Bitcoin developers recently discovered a massive security risk in the Lightning Network, which triggered him to announce his departure from the project....

[Show more](#)

- previous message: [bitcoin-dev] [lightning-dev] [core lightning] [CVE-2023-40232 / CVE-2023-40233 / CVE-2023-40234 "All your mempool are belong to us"]
- Next message: [bitcoin-dev] OP_Expire and Coinbase-Like Behavior: Making HTLCs Safer by Letting Transactions Expire Safely
- Messages sorted by: [date] [thread] [subject] [author]

Hi,

After writing the mail reply on the economics of sequential malicious replacement of honest HTLC-timeout, I did write one more test to verify the behavior on core mempool, and it works as expected.

<https://github.com/ariard/bitcoin/commit/30f5d5b270e1ff195e8dcbef6b7ddcc5f6a>

Responsible disclosure process has followed the lines of hardware issues affecting operating system, as documented for the Linux kernel, while adapted to the bitcoin ecosystem:

<https://docs.kernel.org/6.1/process/embargoed-hardware-issues.html>

https://twitter.com/Uncle_Nakamoto/status/1715884413836538276

クリプトの今後

今後、業界の大整理 2023.11



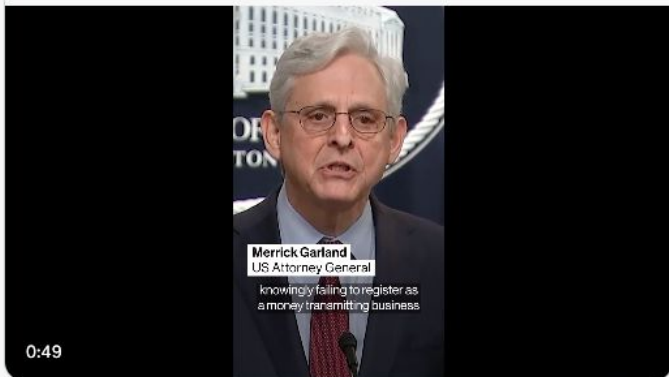
shu @shu_BSV · 7h

【速報】バイナンスとそのCEOであるCZは、反マネーロンダリングおよび米国制裁違反の刑事責任を認め、40億ドル以上の罰金を支払うことに同意したと、メリック・ガーランド米司法長官が発表した。

Bloomberg Crypto @crypto · 7h

Binance and its CEO Changpeng Zhao pleaded guilty to criminal charges for anti-money laundering and US sanctions violations and agreed to pay over \$4 billion in penalties, US Attorney General Merrick Garland said bloom.bg/49KtNox

[DeepLで翻訳する](#)



0:49

🔄 3 ❤️ 16 🗨️ 858 📌 ↑

https://twitter.com/shu_BSV/status/1727093495981294063



CZ @cz_binance

Craig Wright is not Satoshi.

Anymore of this sh!t, we delist!

[DeepLで翻訳する](#)

Bitcoin Magazine @BitcoinMagazine · Apr 12, 2019

An attack against one is an attack against all. #WeAreAllHodlonaut

Artwork: @CryptoScamHub

[DeepLで翻訳する](#)



https://twitter.com/cz_binance/status/1116563034476957699

BTCのバグから生まれたNFT

Bitcoin系共通のトークン規格 Ordinals



How Taproot Enabled The Ordinals Protocol



Trust Machines
2,270 followers

+ Follow

July 12, 2023

Effectively, it removed the script size limit of 10000 bytes. Scripts are now only limited by the block size limit of 1vMB, equivalent to roughly 4MB in size.



Ordinals NFT

UTXO系の共通規格

The screenshot shows the Ordinals Wallet interface. At the top, there is a navigation bar with 'Ordinals Wallet' on the left, a Bitcoin icon with a dropdown arrow, and buttons for 'Home', 'Inscribe', and 'Market'. On the right side of the navigation bar, there is a search bar, a notification bell, a 'Trade BTC' button, and a user profile icon with the address 'bc1p...67s4'.

The main content area features a dark background with a grid of colorful, pixelated NFT images on the right. On the left, the text reads: 'Collection [Share](#)', 'Pixel Pepes [Twitter](#) [Discord](#)', and 'The first ever airdrop on the Bitcoin network. 1563 rare Pixel Pepes airdropped to users who had made a transaction on ordinalswallet.com before block 777888.' Below this text are two data points: 'Floor [0.118](#)' and 'Total volume [148.8587](#)'. A prominent blue 'Trade now' button is located at the bottom left of the collection card.

1 Sat Ordinals

BSVのOrdinals NFT

Inscribe Market

Inscription Preview

Broadcast to finalize.

```
010000001c52abe4620285df76da3741463b0fe71a792f3d28c9e27e951e622819e9ebb9e010000006b483045022100fdadbf05dbaa0bfd20b2e68dc4c1f497282b0f2c316cc6c8ce8dc1c74d6865f202207599cb5d765864fd4094f2e9e110bea68d4029e6fab61f76349ce7b828ff7379412103475c34618fee3e0ea629863754a2f607f7fd47d65c475ac4e628527bb2fd1ecdTransaction ID@00000000fd2c2676a914da15fbc88645b0400003c21fa160790ce3f3a0080ac0863036f7264510a69606167652f
```

f9d402ae8e9640427d0fd7f2766ea1bccb49d192991112a6b34a32803354163e

1 Inputs	2 Outputs
Size	9.74 KiB
Network Fee	8,882 Satoshis
Network Fee USD	\$0.01
Fee Rate	0.89043 sat/B

Broadcast \$0.01

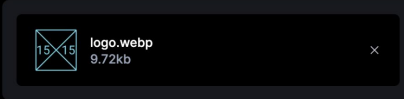
Copy Raw Tx Download

Start Over

Ordinals Wallet Home Inscribe Market Search

Inscribe Ordinals

Inscribe ordinals to Bitcoin



Select network fee **Medium 26 sats/byte**

26

Sats In Inscription:	546 sats	~\$0.28
Network Fee:	71656 sats	~\$37.17
Service Fee:	1999 sats	~\$1.04
Fee by Size:	3313 sats	~\$1.72
=	5312 sats	~\$2.76
Estimated Total:	76968 sats	~\$39.93

By clicking "Inscribe", you agree to the Ordinals Wallet [Terms of Service](#).

Your ordinals will be minted to your connected wallet

Inscribe

デジタルトレーディングカードゲーム

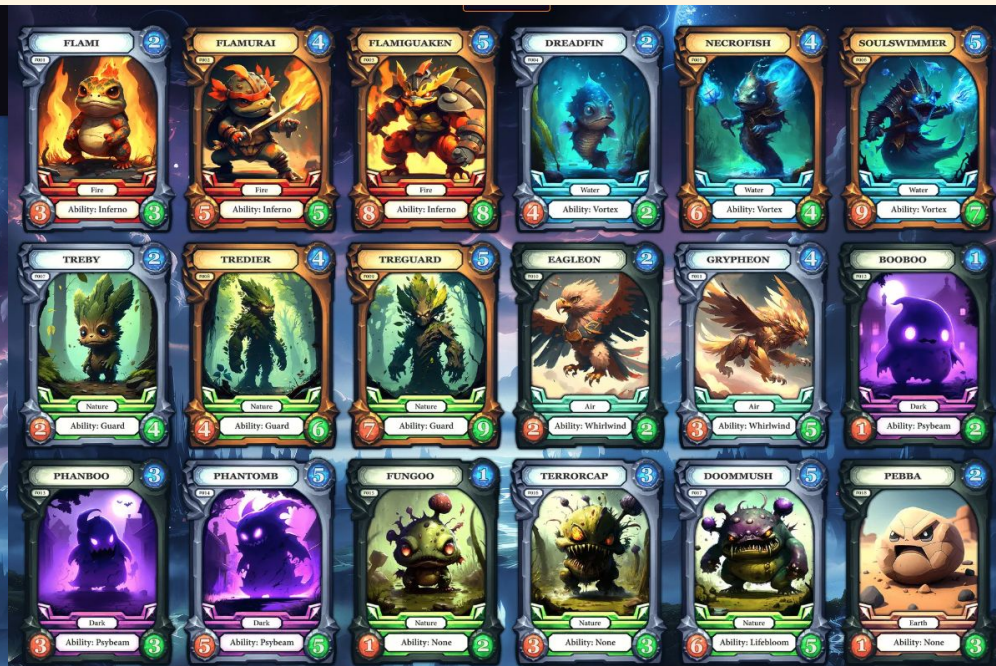
Champions TCGの日本での取扱 1 sat Ordinals



世界初の本格的なデジタルトレーディングカードゲーム

異世界の魔法のチャンピオン 公式ウェブサイト

Champions TCG



1 Sat Ordinals

BSVのOrdinals NFT

 **KURO'** @PhotoKuro_ · Feb 14
Bitcoin SV 



Phoenixer Blue

BSV ordinals collection

 **ninnin**  @ninnin_nft · 15h
BSV Ordinals Collection 
『Reverb/残響』 No.27
[DeepLで翻訳する](#) 



デジタルトレーディングカードゲーム

Champions TCGの日本での取扱



開発デモ画面

Market Place Top > Dashboard Search... ぺんだー

Dashboard ▾ Latest Posts 8件のポスト

Featured 「子」の中身
陽子の内部の様子を完全再現した最新の映像がヤバすぎる
Video **これに成功!?**

Price: \$2.00
Status: Active

YENPoint ¥33

支払う

株高 31947円

Featured 【定時上がりは効】 4E9ND エンス地獄の残業エピソード
Video

Price: \$3.00
Status: Active

YENPoint ¥33

Featured スーパー持ち込み禁止 読者のロコミ エンス読者のロコミ
Video

Price: \$3.00
Status: Active

YENPoint ¥33

Featured 【成功哲学】 最も才能のある人は、必ずしもラッキーな人が成功することを経験的に証明したイグノーベル賞研究
Video

Price: \$5.00
Status: Active

YENPoint ¥33

Featured 【成功哲学】 最も才能のある人は、必ずしもラッキーな人が成功することを経験的に証明したイグノーベル賞研究
Video

Price: \$50.00
Status: Active

YENPoint ¥33

Featured 天才! 日本人のIQは世界トップクラスなのに不幸なワケ
Video

Price: \$50.00
Status: Active

YENPoint ¥33

Featured その保険 その保険!!!
Video

Price: \$1.00
Status: Active

YENPoint ¥33

Featured TEst Image
Image

Price: \$11.00
Status: Active

YENPoint ¥33

Profile



プロフィールページ

販売コンテンツの一覧や、投げ銭や、質問箱など、クリエイターとファンが直接やりとりできるコミュニケーション機能

2円からの投げ銭が受けられます。

Market Place



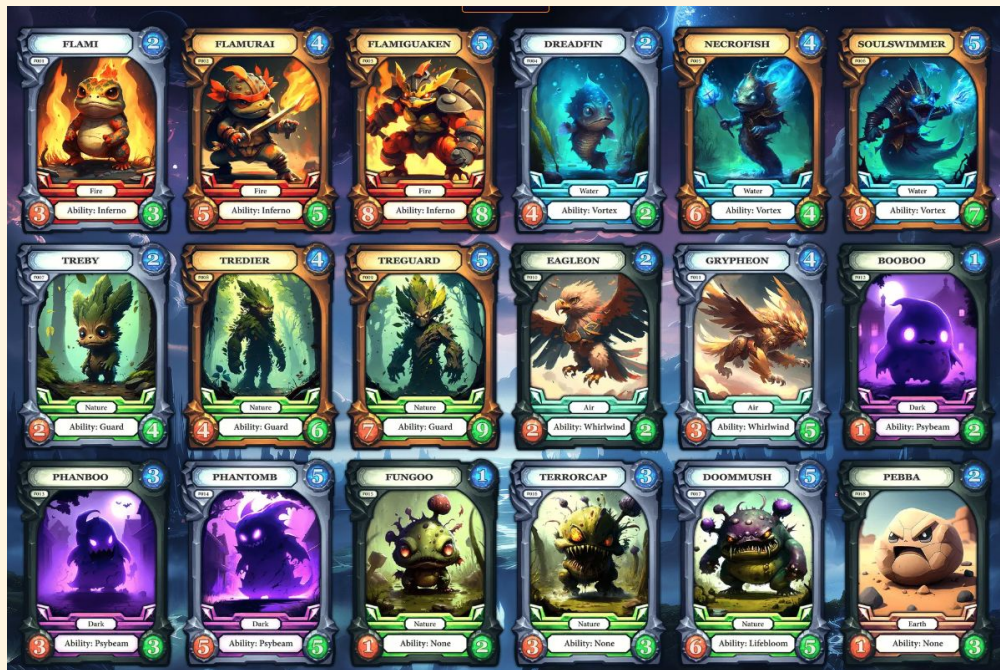
マーケットプレイス

100円以下のデジタルコンテンツを簡単に販売できるオンラインプラットフォームです。

コンテンツクリエイターは、手軽な価格設定で自身の作品を販売し、新たな収益機会を得ることができます。

プレゼント企画

このQRコードからサインアップしてくれた人に
Champions TCGのカードパックをプレゼント



Thanks



Xでフォロー

Contact

Ken Sato

ken@yenpoint.jp