THE BITCOIN LAYER

ZINES!

https://satsie.dev/zines

booklets about bitcoin tech

@SATSIE
SATSIE.DEV/ZINES
IMAGES: HERECOMESBITCOIN.ORG

open source

Always available to read online for free.

Thai translation made by the community!

Satsie's Pocket Guide to Taproot

Download the printable PDF here

Need help assembling? Check out these instructions.

What is the Taproot upgrade?

Taproot is a set of improvements that allow Bitcoin to be used in more scalable and private ways.

Activation date: November 2021
Block height: 709,632.

Taproot enables some cool features

Key and signature aggregation (MuSig)

If you have public keys A, B, and C, they can be combined into one. The same is true for the corresponding signatures.

This means complex multisignature spends can look like ones that only involve 1 key.

pg. 2

Batch signature validation

Validating digital signatures usually requires a lot of effort from a computer's CPU. Now transaction signatures can be grouped together and validated as one unit, instead of one by one.

Better privacy while spending

Bitcoin allows you to specify multiple ways to spend a coin. Prior to Taproot, all these ways had to be made public when the coin was spent. This is bad for privacy, especially for coins with unique spending rules, making them easy to identify.

pg. 3

Previous Next

Satsie's Pocket Guide to BIPs

Download the printable PDF here

Need help assembling? Check out these instructions.

There is also a Thai version 🇹🇭 made available by aekasitt.

But that's just the beginning...

How do BIPs get accepted and deployed into Bitcoin?

This is up to the community to decide. It's on the BIP author + its supporters to champion the idea. They need to spark interest and rally support.

> "The BIP author is responsible for building consensus in the community and documenting dissenting opinions" — from BIP-2

The beautiful thing about Bitcoin is it's decentralized. Anyone can make a BIP! But that also means no one has the authority to tell others how to allocate their time + resources. Nobody has to review your BIP, or even engage with it.

pg. 6

Sometimes you have to be patient. Some now popular BIPs sat around for months before anyone noticed them.

Why don't some BIPs move forward? Why don't they make it into Bitcoin?

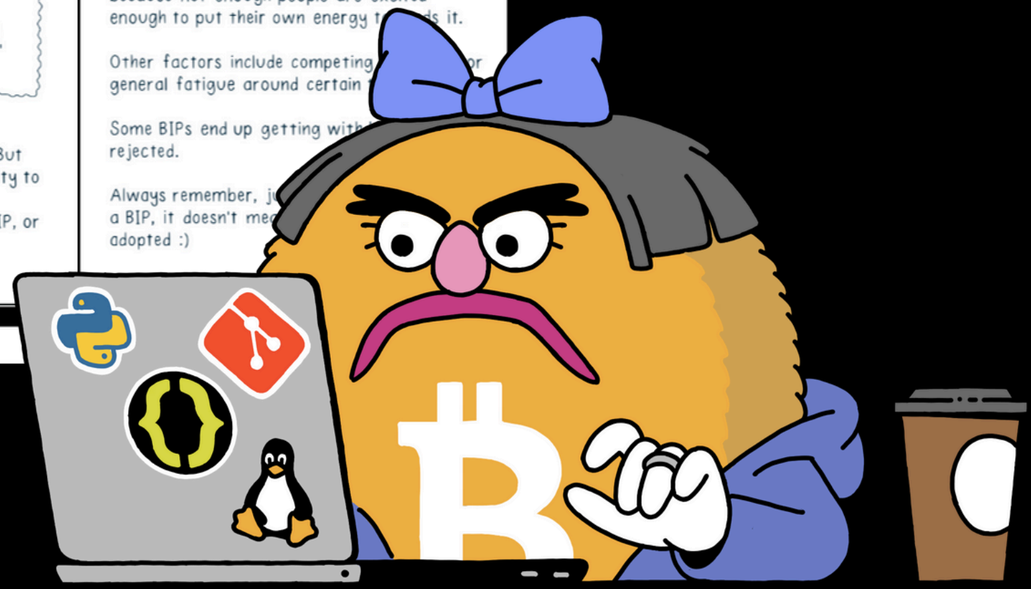
Oftentimes, while the community may not necessarily oppose a BIP, it doesn't progress because not enough people are excited enough to put their own energy t… …ds it.

Other factors include competing … or general fatigue around certain …

Some BIPs end up getting with… rejected.

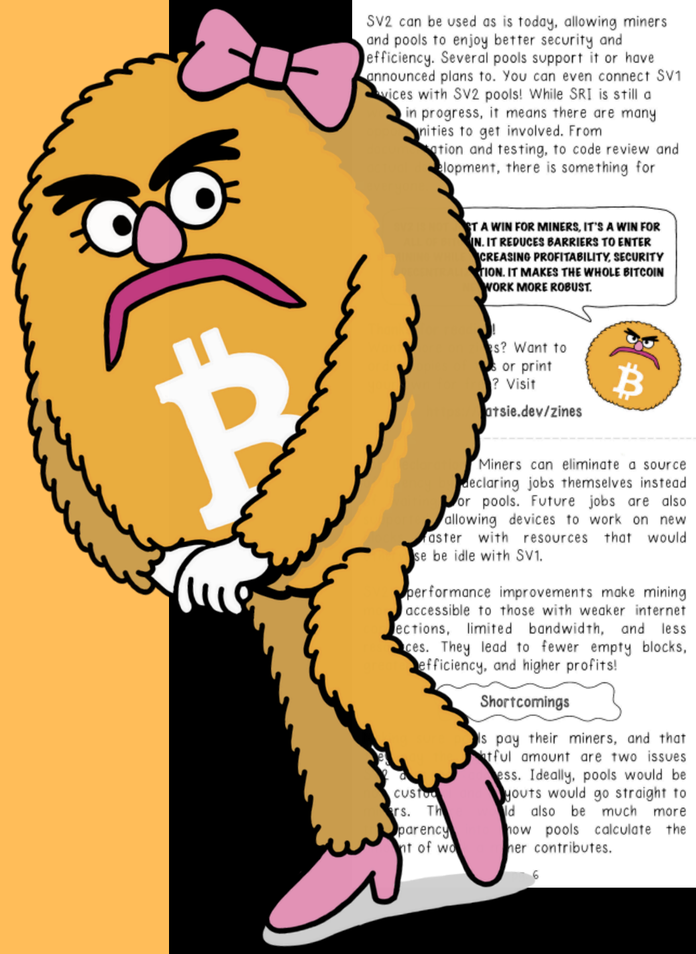
Always remember, j… a BIP, it doesn't mea… adopted :)

Previous



@SATSIE
SATSIE.DEV/ZINES
IMAGES: HERECOMESBITCOIN.ORG

short and sweet



SV2 can be used as is today, allowing miners and pools to enjoy better security and efficiency. Several pools support it or have announced plans to. You can even connect SV1 ...vices with SV2 pools! While SRI is still a ... in progress, it means there are many ...nities to get involved. From ...ation and testing, to code review and ...elopment, there is something for

...T A WIN FOR MINERS, IT'S A WIN FOR ...IN. IT REDUCES BARRIERS TO ENTER ...CREASING PROFITABILITY, SECURITY ...TION. IT MAKES THE WHOLE BITCOIN ...WORK MORE ROBUST.

...s? Want to ... or print ...? Visit ...atsie.dev/zines

... Miners can eliminate a source ...declaring jobs themselves instead ...or pools. Future jobs are also ... allowing devices to work on new ...aster with resources that would ...se be idle with SV1.

...performance improvements make mining ... accessible to those with weaker internet ...ections, limited bandwidth, and less ...ces. They lead to fewer empty blocks, ...efficiency, and higher profits!

Shortcomings

...s pay their miners, and that ...ntful amount are two issues ...ess. Ideally, pools would be ...payouts would go straight to ...rs. Th... ...d also be much more ...parency ...now pools calculate the ...nt of wo... ...ner contributes.

satsie's pocket guide to

STRATUM V2

A zine about the latest update to Bitcoin's mining protocol

APRIL 2024

By 2019 the mining landscape had drastically evolved. Late that year, the spec for Stratum V2 (SV2) was released.

Why is SV2 great?

✡ Decentralization ✡

In SV1, pools decide what transactions go into a block. If just a few of the largest pools collude, transaction censorship is possible. With the **Job Declaration (JD)** feature, SV2 flips this dynamic, letting miners pick the transactions. While pools can still reject blocks from miners, SV2 makes it easy for a miner to switch pools or solo mine. This incentivizes pools to avoid censorship, otherwise they risk losing miners.

JD also helps decentralize mining infrastructure. In addition to pools, miners and third parties can now construct block templates. This leads to more Bitcoin nodes, strengthening the network's peer-to-peer layer.

Stratum is a messaging protocol that miners and pools use to talk to each other

As a way to stabilize revenue, most Bitcoin miners join pools. Stratum is a protocol (set of communication rules) that allows individual mining devices ("**devices**") to talk to pools and the Bitcoin network. Stratum clients and servers form a communication layer above Bitcoin, facilitating the easy exchange of data between devices, Bitcoin nodes, and pools. It's used for things like connecting to, receiving jobs from, and submitting work to pools.

History

Slush (Marek Palatinus) proposed Stratum in late 2011. While initially intended for Electrum, a lightweight Bitcoin client, it was repurposed for mining. It quickly gained industry adoption and enjoyed years of success.

✡ Standardization ✡

Despite widespread use, SV1 was never standardized. Parts of the spec are open to interpretation, resulting in inconsistent SV1 implementations that aren't guaranteed to be compatible. This defeats the purpose of a protocol!

In contrast, SV2 has a well defined spec maintained by an independent, open source working group. It's more developer friendly and has a large, growing community.

✡ Security ✡

In SV1, communications between miners and pools are unauthenticated and unencrypted. Messages are plain text and available for anyone to read! Miners are vulnerable to an attack called hashrate hijacking. When a miner sends the work they have done to a pool, an attacker can intercept the message and take all the credit.

Timeline

November 2019 The SV2 spec by Pavel Moravec, Jan Capek, Matt Corallo, + other industry experts is published.

January 2021 Work begins on a community based, open source implementation of SV2, The Stratum Reference Implementation (SRI).

April 2020 Braiins releases the first (partial) implementation of SV2.

October 2022 SRI is released. Additional releases followed April 2023 and March 2024.

Today ✡ While SV2 has come a long way, development is far from over! There is still code in progress for things like monitoring, testing, and general usability. Even when SV2 is fully implemented, there are hurdles to overcome before complete adoption.

SV2 fixes this by adding authentication and encryption, a simple addition with a huge security impact.

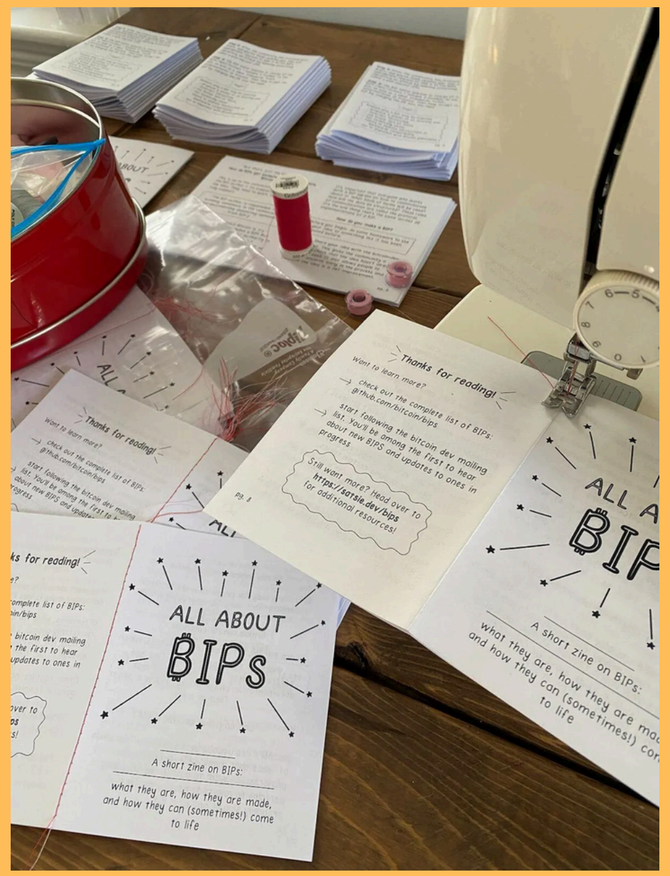
✡ Performance ✡

Messaging: By making network messages smaller and less frequent, SV2 is more efficient and uses less bandwidth. Instead of JSON RPC, a popular yet verbose format, SV2 uses binary. Compared to SV1, the average message is over 50% smaller!

Pooled Connections: In SV1, the TCP connections between devices and pools are one-to-one.* With SV2's new mining proxy, messages are collected and forwarded to and from the pool as one big unit, reducing bandwidth, CPU load, and infrastructure costs. This message aggregation lowers the total amount of data sent by reducing overhead and redundancy.

* at least officially. there are non standard ways to get around this

@SATSIE
SATSIE.DEV/ZINES
IMAGES: HERECOMESBITCOIN.ORG

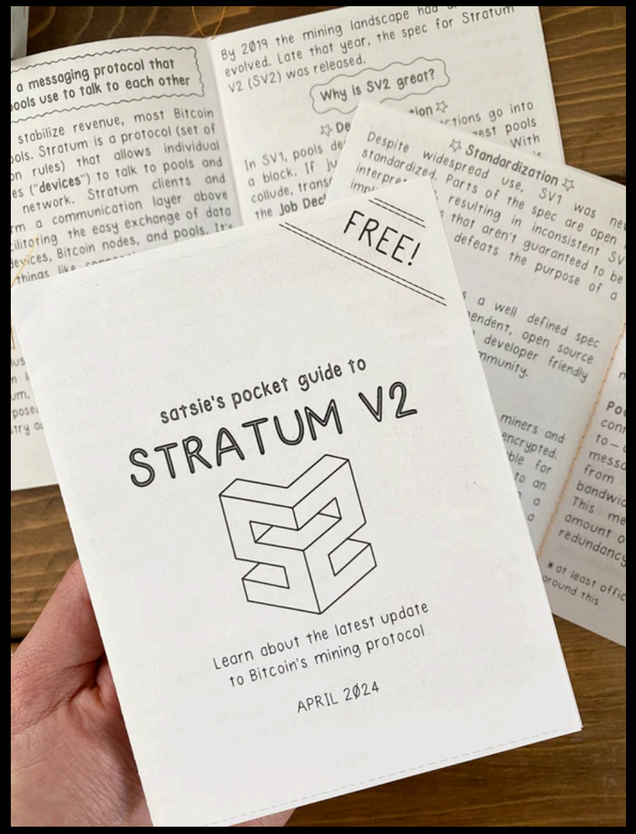


1. Print

2. Cut

3. Stack

4. Fold



print at home

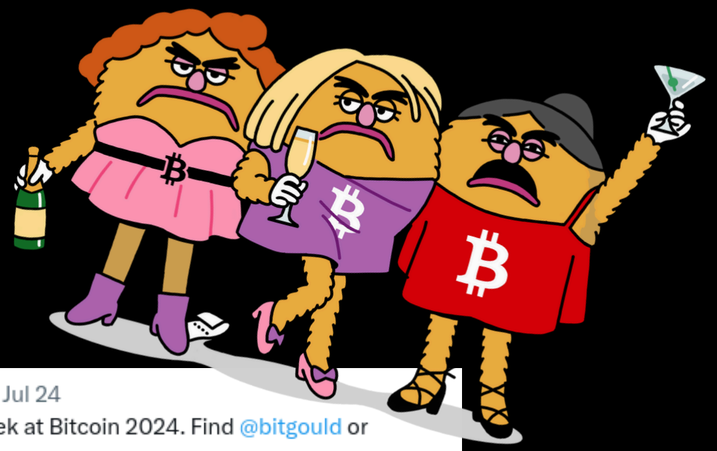
@SATSIE
SATSIE.DEV/ZINES

share with friends

Haley Berkoe @HBerkoe · Jun 6

Love these! Thanks @satsie 🧡

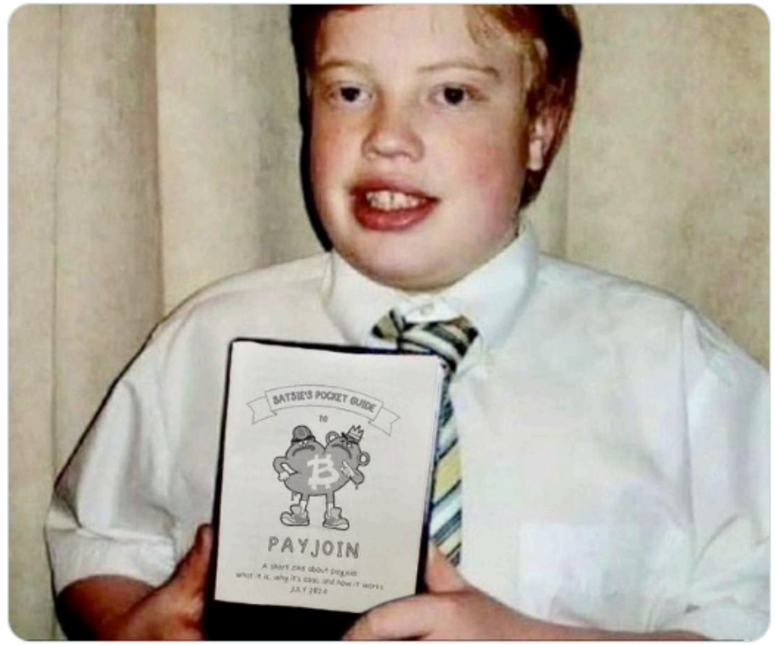
satsie.dev/zines



I identify as a layer 2 @satsie · Jul 24

New payjoin zine drops this week at Bitcoin 2024. Find @bitgould or @brandonstlucas for a copy!

I'm attaching a photo of them so you know who to look for.



Denver BitDevs @DenverBitDevs · Apr 6, 2023

BIP goodies for attendees tonight - thanks @satsie!

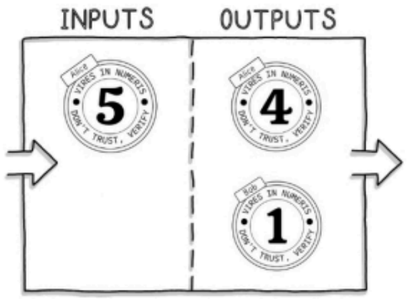
@SATSIE
SATSIE.DEV/ZINES
IMAGES: HERECOMESBITCOIN.ORG

Payjoin is a technique for batching Bitcoin transactions while preserving privacy and block space.

Recall that:

1. Bitcoin uses the UTXO model, and
2. coins (transaction inputs and outputs) can be of any value

Pretend Alice has 5 BTC in her wallet and she sends 1 BTC to Bob. The transaction (tx) looks like this:



pg. 2

How BIP-77 works

Bob: I want to start using payjoin. Can I have a mailbox?

Directory Server: Sure! Here's your address.

Bob: Hey Alice, anytime you want to send me BTC, use my mailbox so we can make it a payjoin.

Alice: Ok. I want to send you BTC. I've started a transaction, and am putting it in your mailbox. Add your input and it will be a payjoin.

Bob: Look! I have a payjoin transaction in my mailbox! Let me add my input and put it back in the mailbox.

Alice: My turn to check the mailbox. The payjoin transaction is in there and it's complete. Now I can broadcast it to the network!

pg. 7

new zine about payjoin

@SATSIE
SATSIE.DEV/ZINES
IMAGES: HERECOMESBITCOIN.ORG

satsie.dev/zines

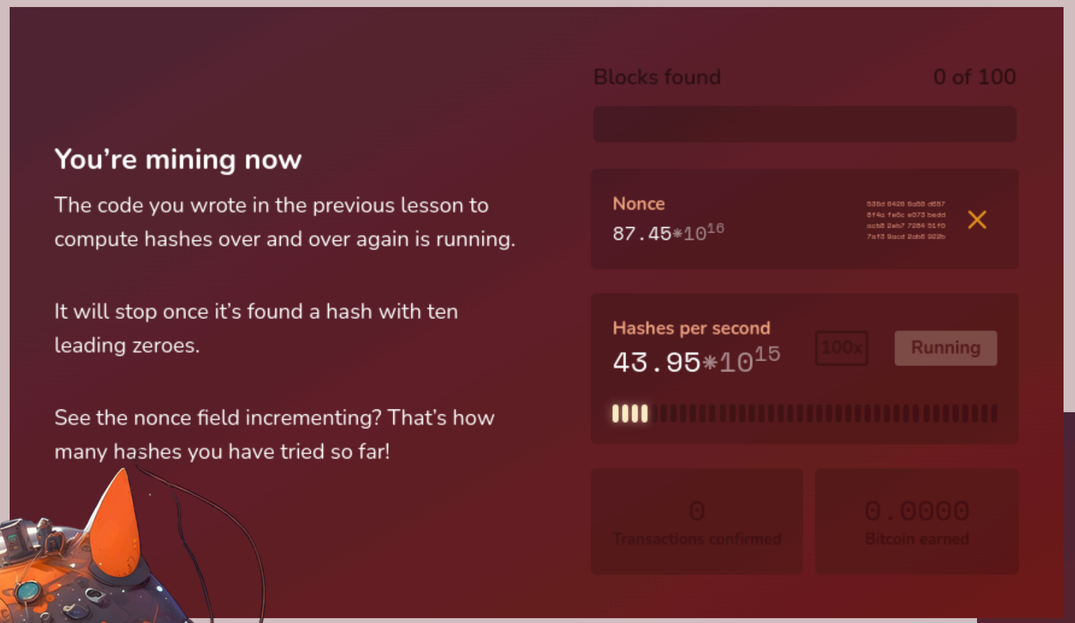

SAVING
SATOSHI
SAVINGSATOSHI.COM

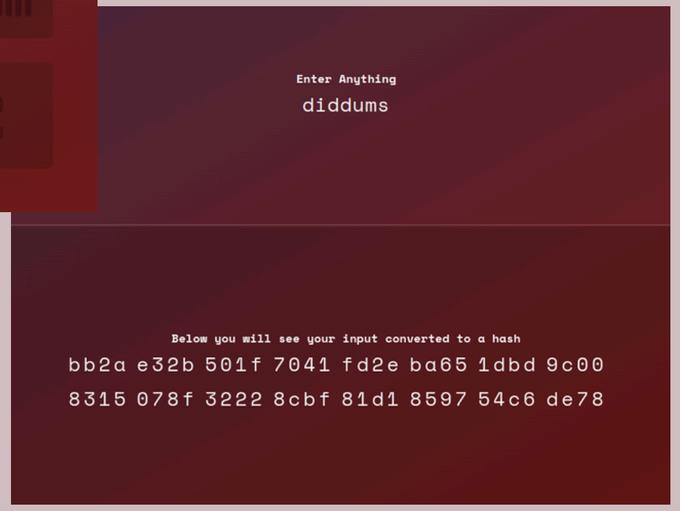
A FUN, GENTLE WAY TO LEARN HOW BITCOIN WORKS

A beautiful, student focused game. A sci-fi epic.

A welcoming entry point into bitcoin tech.

Reflective of the best parts of bitcoin.



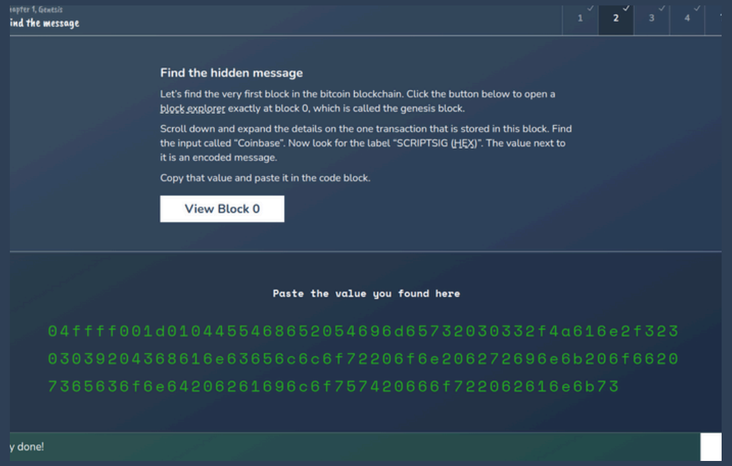


MADE TO INSPIRE A NEW GENERATION TO FALL IN LOVE WITH BITCOIN

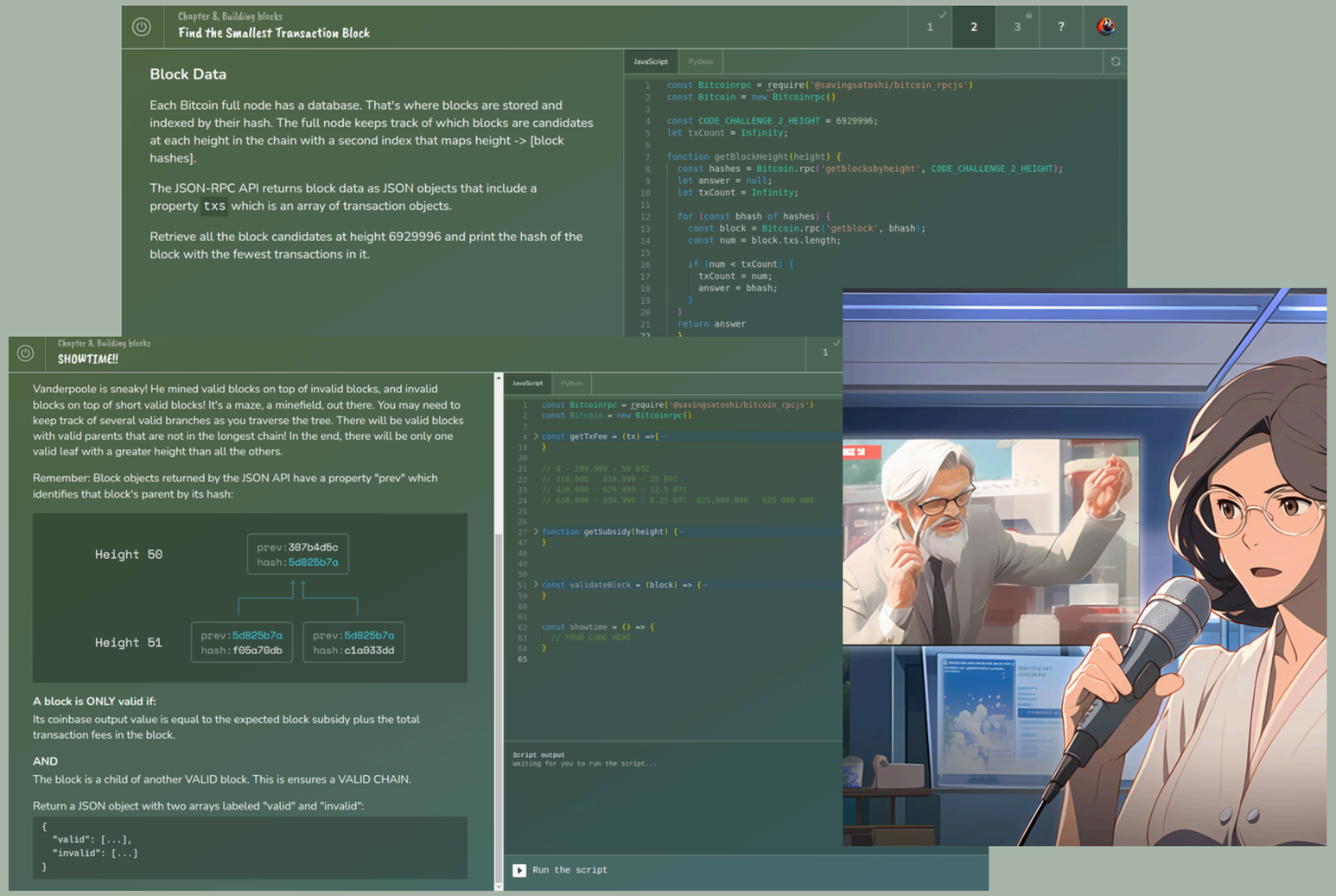
Understanding from a technical standpoint seals the deal.

The learning should be as cool and unique as the technology.

Complements existing resources.



FOR EDUCATORS AND THE TECHNICALLY CURIOUS, REGARDLESS OF BITCOIN BACKGROUND



Teachers and their students

Those struggling to progress in their bitcoin journey

All levels

Bitcoiners and non-Bitcoiners alike

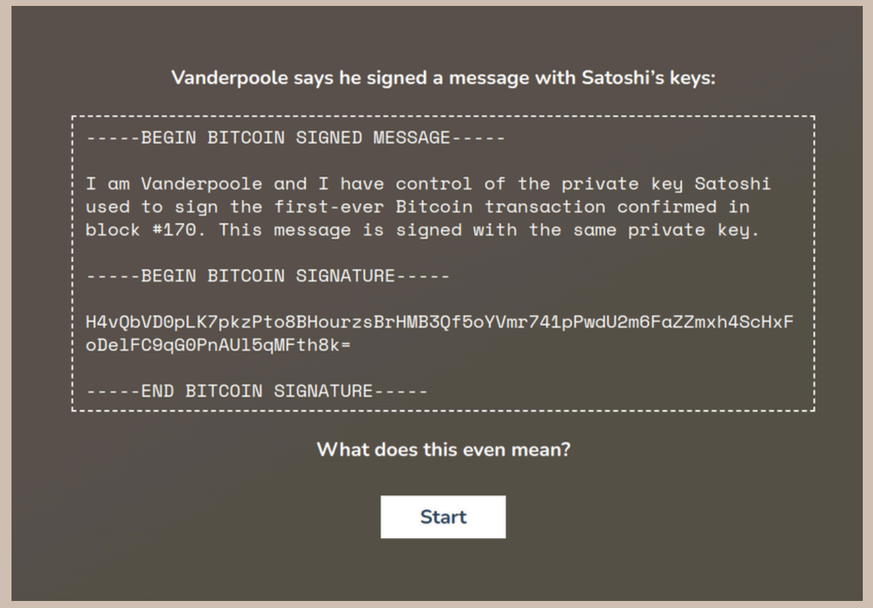
REAL LEARNING THAT HELPS YOU UNDERSTAND, EXPLAIN, AND USE BITCOIN BETTER

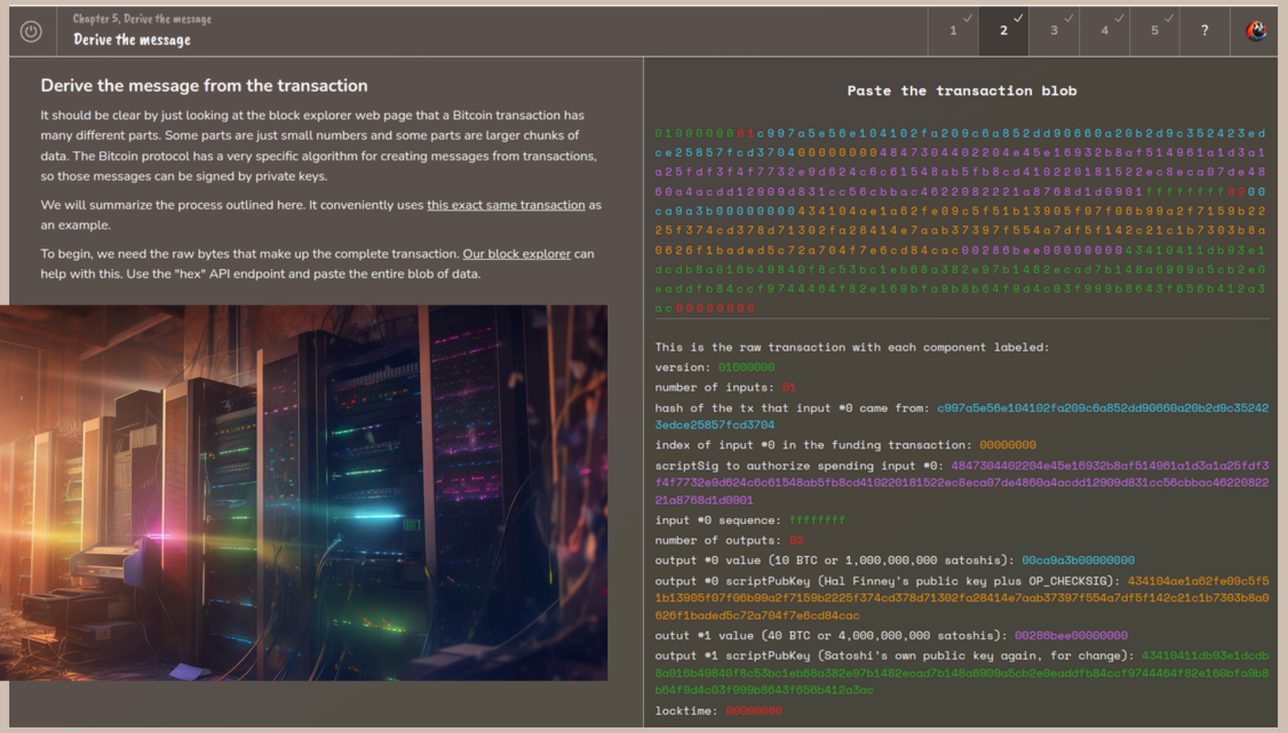
It's ambitious. You're ambitious.

Bitcoin is not inevitable. It's under attack.

Bitcoin is for everyone

You care about Bitcoin and all the things that make it special





Chapter 7, Building blocks

Assemble a block

You can make the following assumptions to complete your mission:

- All transactions in the mempool have already been verified as valid.
- The coinbase transaction, and the weight it contributes to the block, can be ignored.

You can view the entire raw mempool JSON file here.

Or browse an excerpt of the file in this table for some basic patterns:

Transaction ID	Fee Satoshis	Weight Weight units (WU)	Ancestors
b27f86d3	43430	2020	
c27b4d2e	30168	1676	bd1d83ca f29aec75
18725711	5520	1840	3c64a457 3c8abf73
92b1ecf5	24302	1676	398695a6 10025d80
8e8c8624	8990	1160	01f6094b
5f6c9a80	13716	1524	64121ab1
e140fa46	13020	1488	7675c31c
d7066e71	16416	1152	
88016f17	15200	1600	5e518bbe
8fa820d5	20221	1108	38a62dcc

View the json file here for the rest of the transaction data

JavaScript | Python

```
const json = require('./mempool.

class MempoolTransaction {
  constructor(json) {
    this.txid = json.txid;
    this.weight = json.weight;
    this.fee = json.fee;
    this.parents = json.parents;
  }
}

// Fix this!
function assembleBlock(mempool)
  const block = [];
  for (const tx of mempool) {
    block.push(tx.txid);
  }
  return block;
}

function importMempoolFromJson(j
  const mempool = [];
  for (const tx of json) {
    mempool.push(new MempoolTransaction(tx));
  }
  return mempool;
}

function run() {
  const mempool = importMempoolFromJson(json);
  const block = assembleBlock(mempool);
  return block;
```

Script output

Waiting for you to run the script...

Run the script

A LABOR OF LOVE

An expression of our love for Bitcoin

Our contribution towards making Bitcoin the best it can be

Scratch your own itch

SAVINGSATOSHI.COM