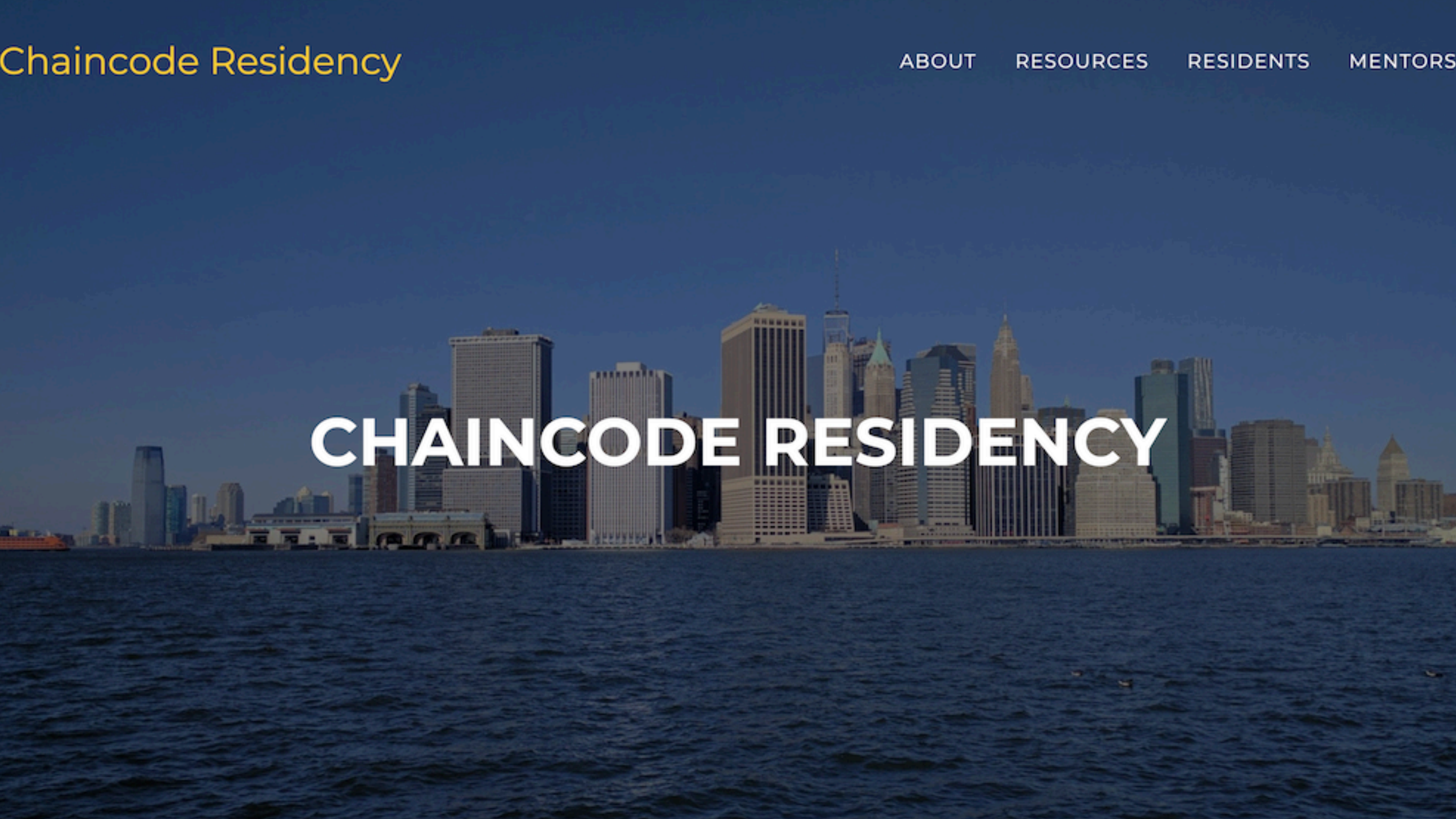
# schnorr & taproot in 20 minutes

laBITconf - 13th Dec 2019

John Newbery, Chaincode Labs


chaincode


Chaincode Residency
ABOUT
RESOURCES
RESIDENTS
MENTORS
CHAINCODE RESIDENCY

# Bitcoin Optech Newsletter #73

Nov 20, 2019

This week's newsletter announces a new minor version release of LND, notes downtime on the development mailing lists, describes some recent updates to Bitcoin services and clients, and summarizes recent changes to popular Bitcoin infrastructure projects.

## Action items

- **Upgrade to LND 0.8.1-beta:** this release fixes several minor bugs and adds compatibility for the upcoming Bitcoin Core 0.19 release.

## News

- **Mailing list downtime:** the Bitcoin-Dev and Lightning-Dev mailing lists both experienced downtime last week due to an unannounced server migration. Both lists are functional again as of this writing.

## Changes to services and client software

*In this monthly feature, we highlight interesting updates to Bitcoin wallets and services.*

- **Bitfinex bech32 send support:** In a recent blog post, Bitfinex has announced support on their exchange for sending to native bech32 addresses. While Bitfinex users could previously use P2SH-wrapped segwit addresses, they can now withdraw from the exchange to native segwit addresses.

- **Wasabi includes Bitcoin Core node:** As part of an ongoing effort to integrate Bitcoin Core, Wasabi has

# Bitcoin Optech Schnorr Taproot Workshop

Oct 29, 2019

En septiembre del 2019, Bitcoin Optech llevó a cabo talleres en San Francisco y Nueva York sobre las propuestas del soft-fork schnorr/taproot. Los objetivos de los talleres fueron:

1. compartir las ideas actuales a la comunidad open-source sobre las propuestas,
2. dar a los ingenieros la oportunidad de trabajar con la nueva tecnología a través de notebooks interactivos jupyter, y
3. ayudar a los ingenieros a participar en el proceso de retroalimentación de la comunidad.

Este artículo contiene todos los videos, diapositivas y notebooks de jupyter de estos talleres, para que los desarrolladores puedan aprender sobre estas nuevas y emocionantes tecnologías desde casa.

Los talleres se dividieron en 4 secciones:

1. Preparación y matemáticas básicas - muestra cómo configurar el entorno del notebook jupyter; ofrece ualización de las matemáticas básicas de la curva elíptica e introduce hashes etiquetados.
2. Firmas de Schnorr y MuSig - describe el esquema de firma bip-schnorr y cómo usar MuSig para

**Thanks to Bitso**

# Bitcoin Optech Schnorr Taproot Workshop

Oct 29, 2019

2019年9月、ビットコインオプテックはschnorr / taproot ソフトフォークの提案に関するワークショップをサンフランシスコとニューヨークで開催しました。 ワークショップを通じて、

1.提案に関するオープンソースコミュニティでの現在の考え方を共有し、 2.インタラクティブなJupyter Notebookを使用して、エンジニアに新しいテクノロジーを使用する機会を与え、 3.エンジニアがコミュニティのフィードバックプロセスに参加できるようにします。

このブログ投稿には、これらのワークショップのすべてのビデオ、スライド、およびJupyter Notebookが含まれているため、自宅にいながらこれらのエキサイティングな新技術について学ぶことができます。

ワークショップは4つのセクションに分かれています:

1. 事前準備、数学のベーシック-Jupyter Notebook環境のセットアップ方法、基本的な楕円曲線数学
ッシュの導入。
2. Schnorr署名とMuSig-bip-schnorr署名スキームと、MuSigを使用して複数の公開鍵 /部分署名を単
のpubkey /署名に集約する方法についての説明

Thanks to CryptoGarage

# Bitcoin Core PR Review Club



## A weekly review club for Bitcoin Core PRs

**What is this?** A weekly club for reviewing Bitcoin Core PRs at **18:00 UTC on Wednesdays** on IRC.

**What's it for?** To help newer contributors learn about the Bitcoin Core review process. The review club is *not* primarily intended to help open effect).

**Who should take part?** Anyone who wants to learn about contributing to Bitcoin Core. All are welcome to come and ask questions!

**What's the benefit for participants?** Reviewing and testing PRs is the best way to start contributing to Bitcoin Core, but it's difficult to kn many require a lot of contextual knowledge, and contributors and reviewers often use unfamiliar terminology. The review club will give you the in the Bitcoin Core review process on GitHub.

## How do I take part?

1. Clone the Bitcoin repository, check out and build the PR branch, and run all tests.
2. Review the code changes and read the comments on the PR.
3. Make a note of any questions you want to ask.
4. Join the #bitcoin-core-pr-reviews IRC channel on freenode at **18:00 UTC on Wednesday**.

# schnorr & taproot

johnnewbery.com/labitconf2019/

# why?

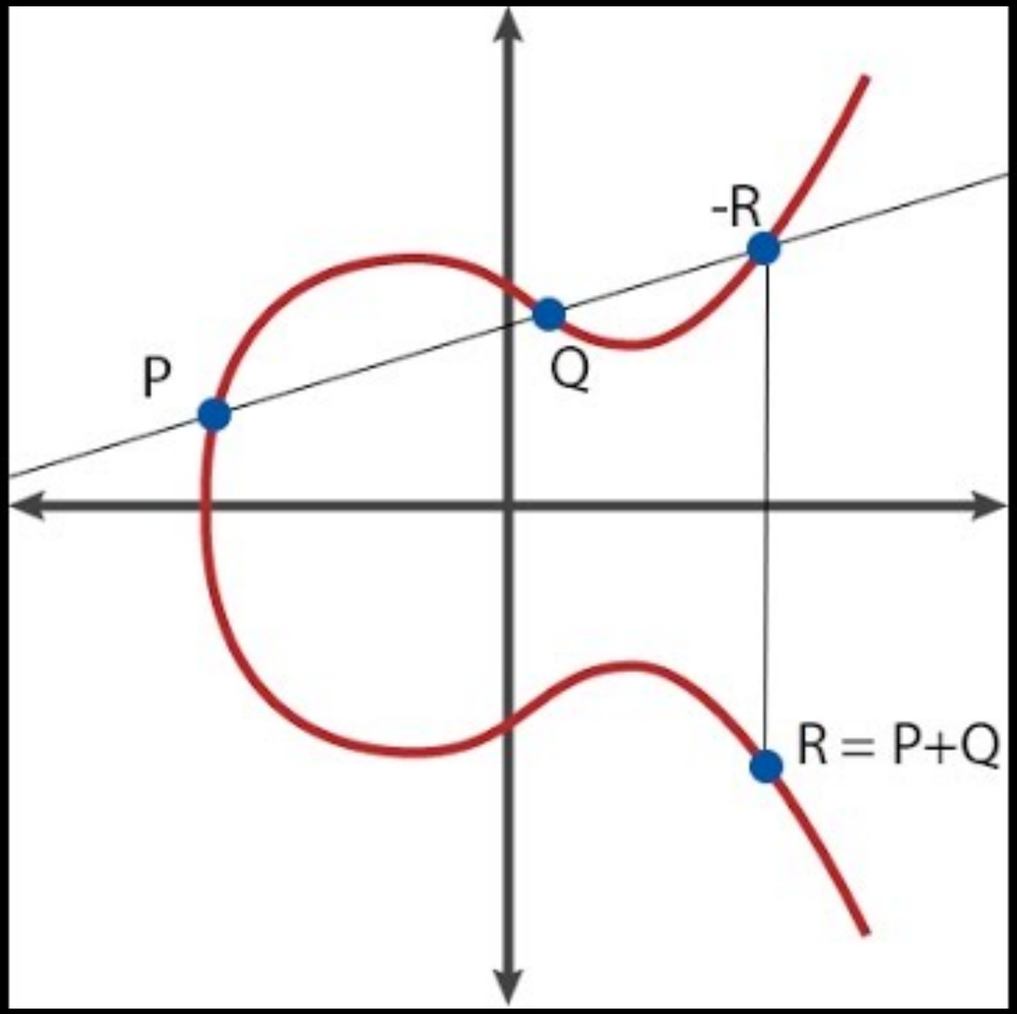
Privacy and fungibility

Scalability

Functionality

# What is a schnorr signature?

# Elliptic Curves



# Elliptic Curves

Addition: A + B = C *easy*

Subtraction: A - B = D *easy*

Multiplication: n x A = (A + A + …) = E *easy*

“Division”: A x ? = F *DIFFICULT!*


PATENTED
PATENTED
PATENTED

# United States Patent [19]

**Schnorr**

[11] **Patent Number: 4,995,082**

[45] **Date of Patent: Feb. 19, 1991**


[54] **METHOD FOR IDENTIFYING SUBSCRIBERS AND FOR GENERATING AND VERIFYING ELECTRONIC SIGNATURES IN A DATA EXCHANGE SYSTEM**


[76] Inventor: **Claus P. Schnorr,** Frankfurterstr. 81, 6350 Bad Nauheim, Fed. Rep. of Germany



[21] Appl. No.: **484,127**

[22] Filed: **Feb. 23, 1990**

[30] **Foreign Application Priority Data**

Feb. 24, 1989 [EP] European Pat. Off. ..... 89103290.6

[51] **Int. Cl.**[5] ..... **H04K 1/00**

[52] **U.S. Cl.** ..... **380/23;** 380/30; 380/25; 380/46

[58] **Field of Search** ..... 380/28, 30, 25, 46, 380/23



[56] **References Cited**

U.S. PATENT DOCUMENTS

on Public-Key Techniques", I.E.E.E., Communcations, vol. 25, No. 7, 1987, pp. 73-79.

Beth, T., "Efficient Zero-Knowledge Identification Scheme for Smart Cards", Advances in Cryptology--Eurocrypt, '80, pp. 77-84.



*Primary Examiner*—Thomas H. Tarcza
*Assistant Examiner*—David Cain
*Attorney, Agent, or Firm*—Hill, Van Santen, Steadman & Simpson



[57] **ABSTRACT**

In a data exchange system working with processor chip cards, a chip card transmits coded identification data I, v and, proceeding from a random, discrete logarithm r, an exponential value $x=2^r \pmod p$ to the subscriber who, in turn, generates and transmits a random bit sequence e to the chip card. By multiplication of a stored, private key s with the bit sequence e and by addition of the random number r, the chip card calculates a y value

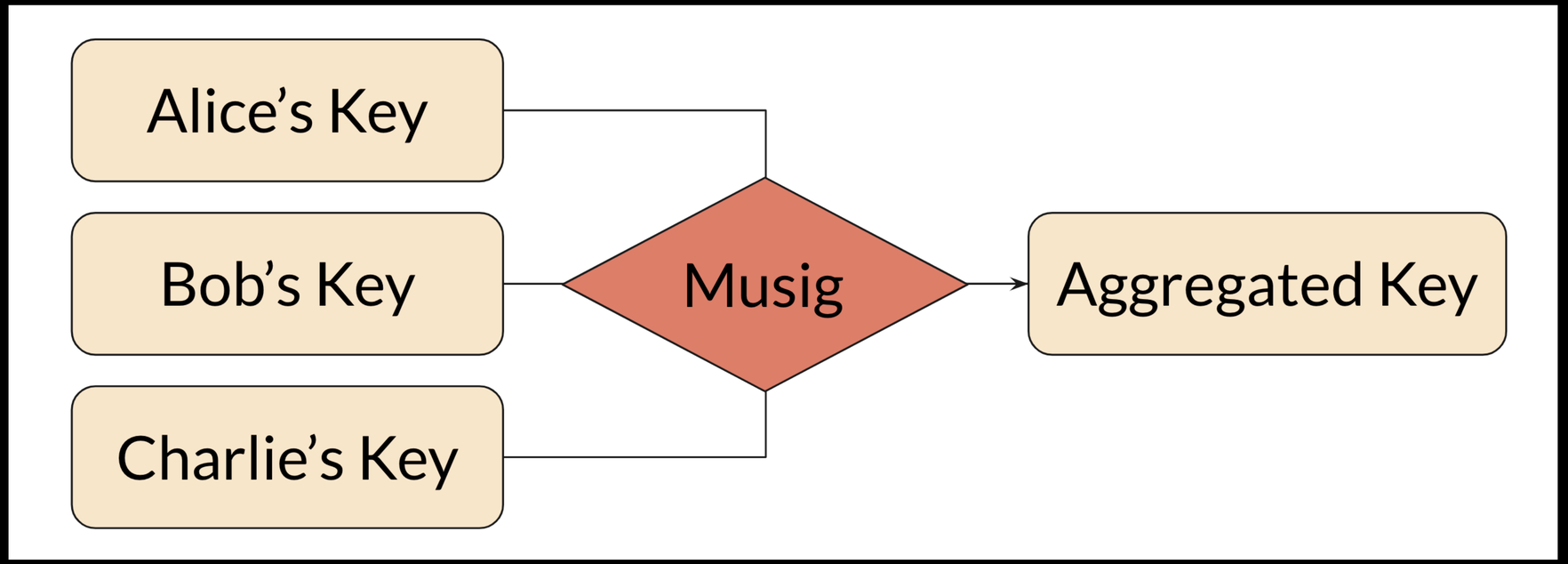
# Bitcoin: A Peer-to-Peer Electronic Cash System

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.

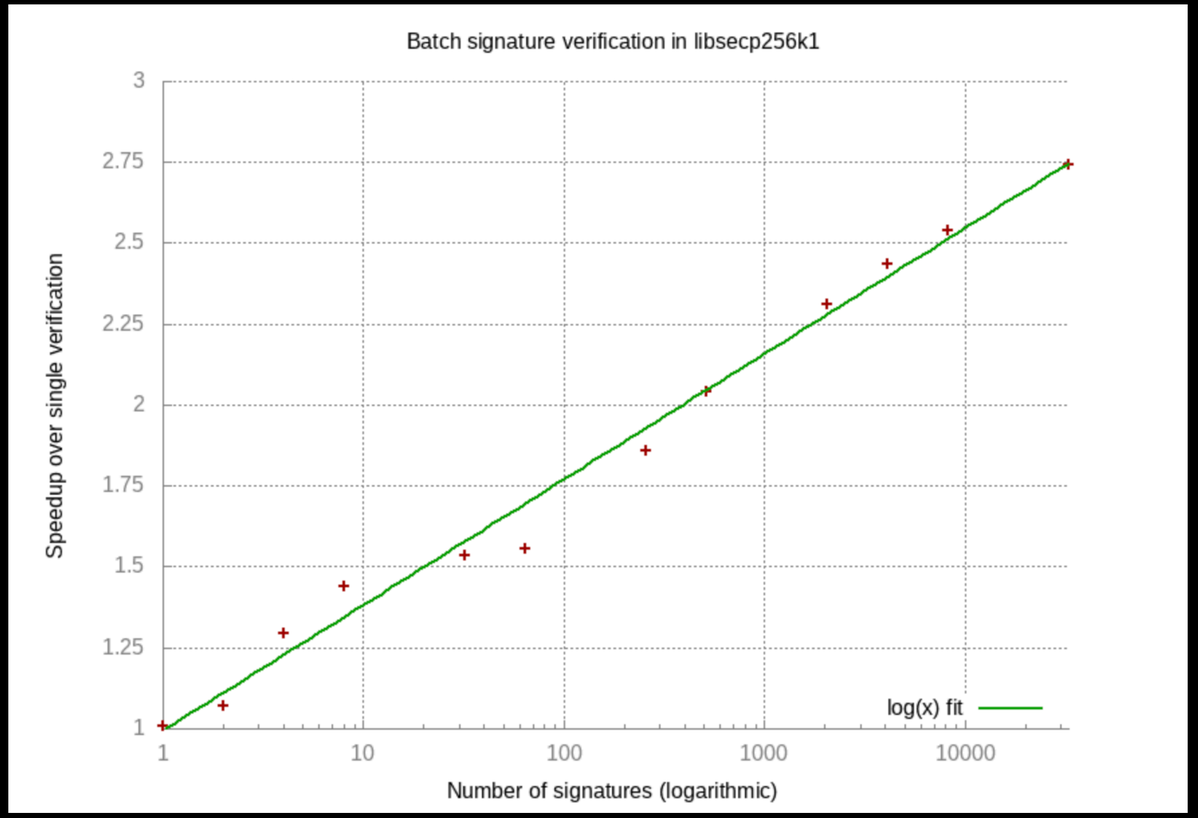
# how do schnorr signatures help privacy/fungibility?

# key aggregation



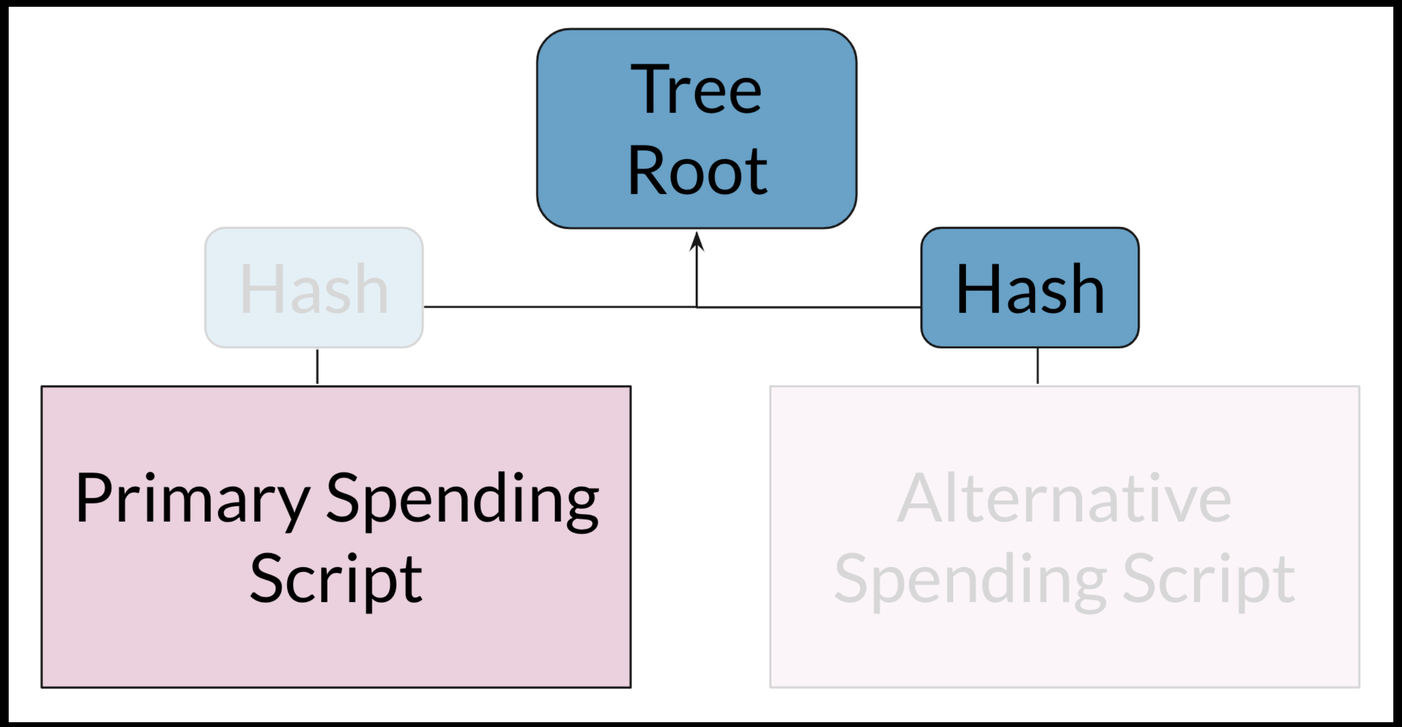
# how do schnorr signatures help scalability?

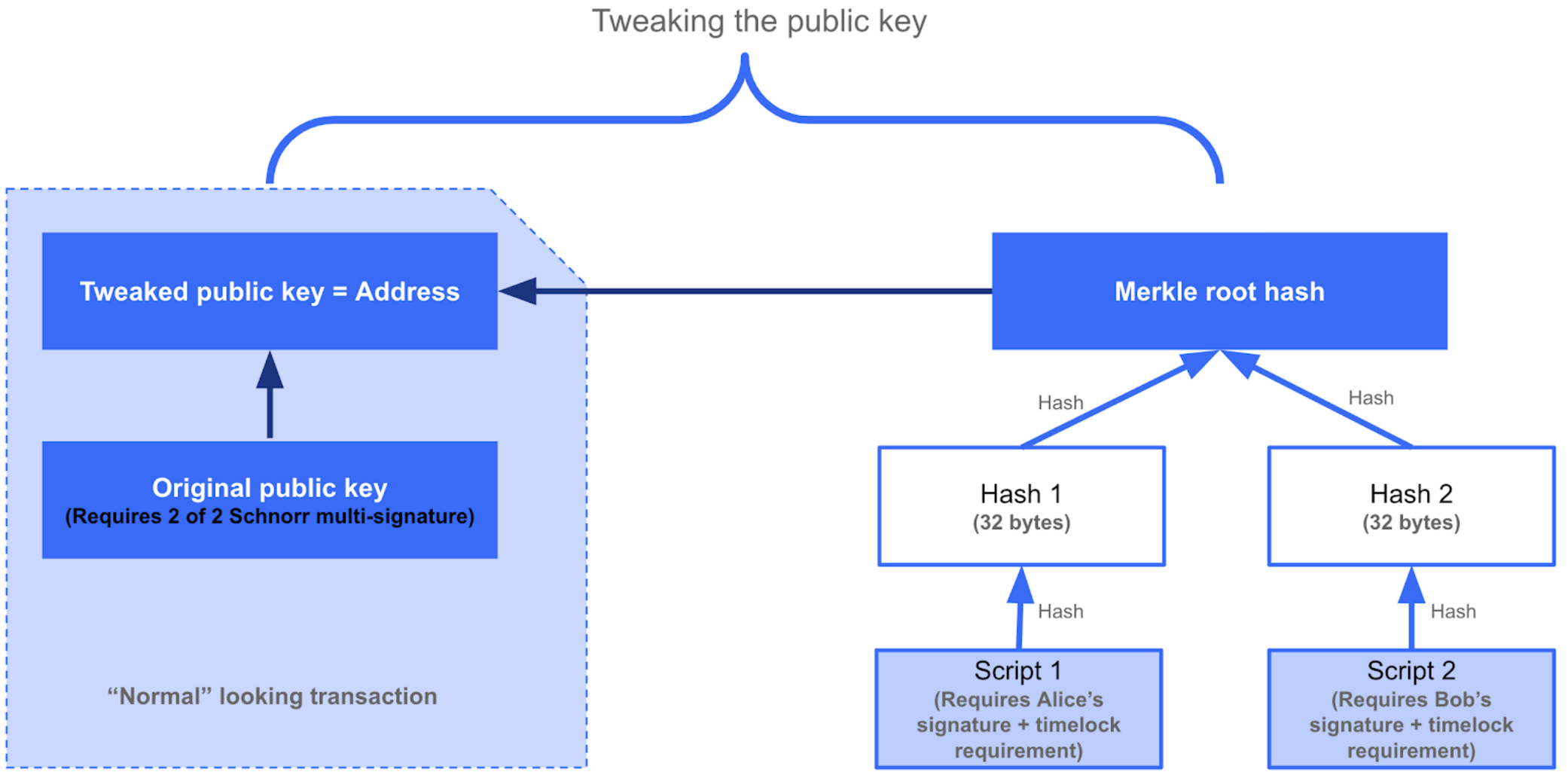
# batch validation



# what is taproot?

# script trees






# Thanks to BitMEX

# Taproot

Many spending conditions can be attached to an output

All outputs look the same

In the best case, only a single signature is revealed

In other cases, only the used spending path is revealed

# In summary

| | | |
|---|---|---|
| 1 | Scaling | • 30-75% savings on multisig<br>• 2.5x faster block validation |
| 2 | Fungibility | • All outputs and most spends indistinguishable |
| 3 | Script Innovation | • Very large k of n multisig<br>• Larger scripts, many scripts |

# Where do I find out more?

# Draft BIPs

https://github.com/sipa/bips/blob/bip-schnorr/bip-schnorr.mediawiki

https://github.com/sipa/bips/blob/bip-schnorr/bip-taproot.mediawiki

https://github.com/sipa/bips/blob/bip-schnorr/bip-tapscript.mediawiki

```
BIP: bip-taproot
Layer: Consensus (soft fork)
Title: Taproot: SegWit version 1 output spending rules
Author: Pieter Wuille <pieter.wuille@gmail.com>
Comments-Summary: No comments yet.
Comments-URI:
Status: Draft
Type: Standards Track
Created:
License: BSD-3-Clause
Requires: bip-schnorr
```

## Table of Contents

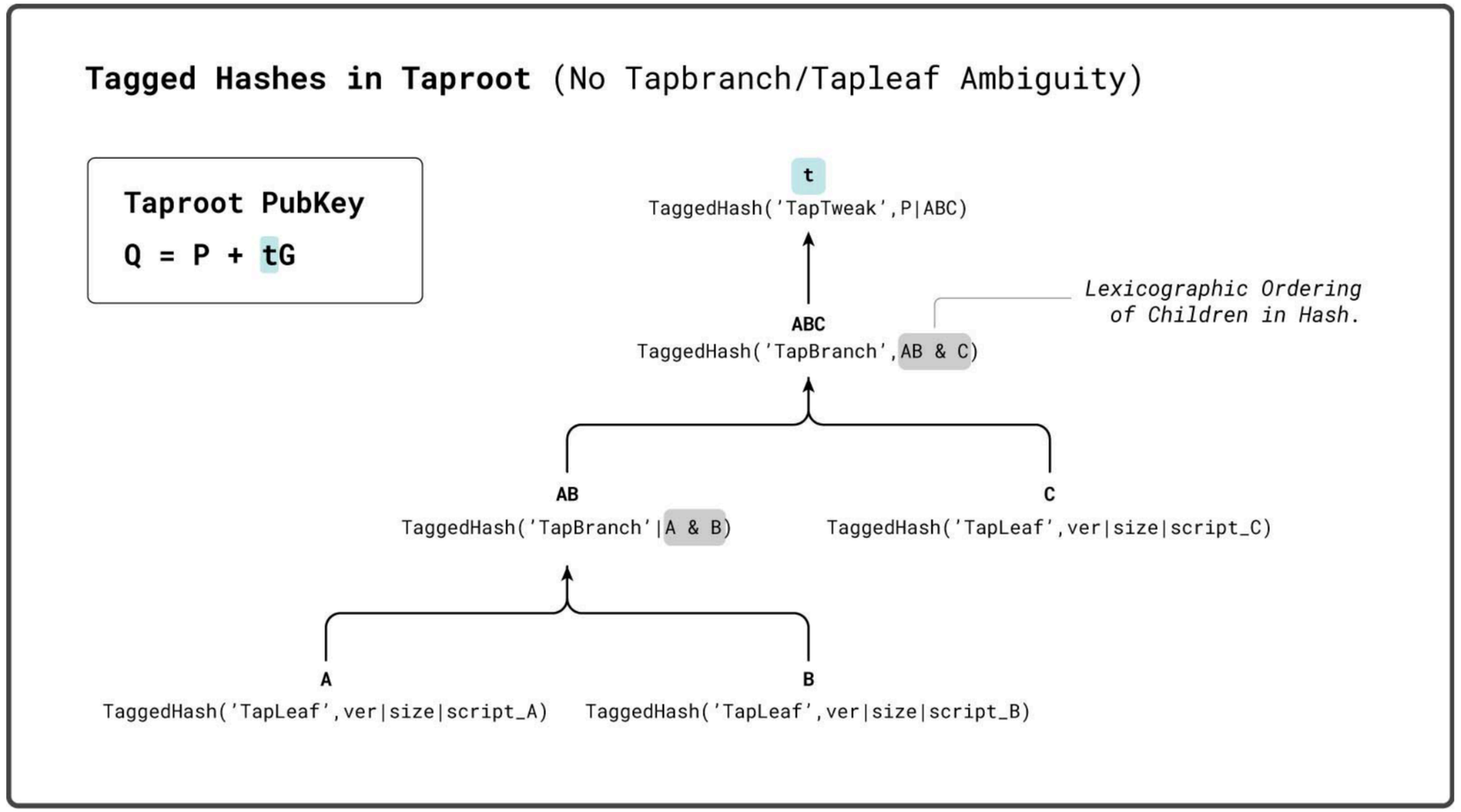
# Optech workshop

https://bitcoinops.org/en/schorr-taproot-workshop/

https://bitcoinops.org/es/schorr-taproot-workshop/

Internal nodes are called tapbranches, and are also computed with the `tagged_hash("Tag", input_data)` function.

Tagged hashes are particularly useful when building a taptree commitment. They prevent node height ambiguity currently found in the transaction merkle tree, which allows an attacker to create a node which can be reinterpreted as either a leaf or internal node. Tagged hashes ensure that a tapleaf cannot be misinterpreted as an internal node and vice versa.




### *Programming Exercise 2.4.1:* Compute a taptweak from a taptree

In the cell below, we will commit three pay-to-pubkey scripts to a taptweak and then derive the segwit address which can be spent by fulfilling these scriptpaths and the internal. We will use the same merkle tree structure as in the previous illustration.

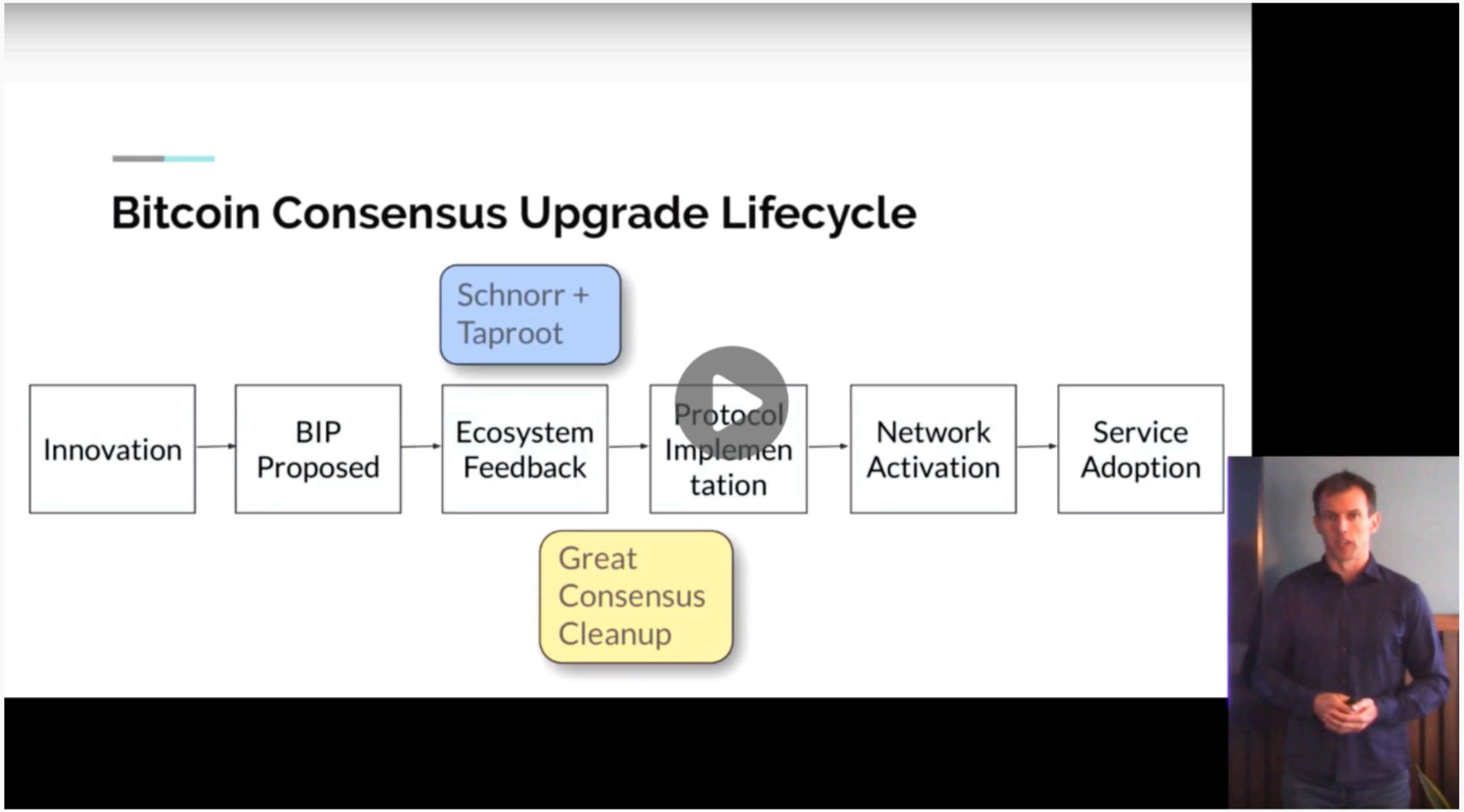
1. Compute TapLeaves A, B and C.
2. Compute Internal TapBranch AB.
3. Compute TapTweak

# Optech Executive briefing

https://bitcoinops.org/en/2019-exec-briefing/#the-next-softfork

# The Next Softfork

The final seminar was given by Bitcoin Optech contributor Steve Lee about potential future softforks in the Bitcoin Protocol.




Download slides

In his presentation, Lee describes the various phases of a soft fork from idea to proposal to implementation to

# Schnorr Taproot BIP review

https://github.com/ajtowns/taproot-review/

README.md

# Taproot BIP Review

## Pitch

The schnorr/taproot/tapscript BIPs are ready for review at this point, and we want to get as much in-depth review from as broad a range of people as we can before we go further on implementation/deployment. Reviewing the BIPs is hard in two ways: not many people are familiar with reviewing BIPs in the first place, and there are a lot of concepts involved in the three BIPs for people to get their heads around.

This is a proposal for a structured review period. The idea is that participants will be given some guidance/structure for going through the BIPs, and at the end should be able to either describe issues with the BIP drafts that warrant changes, or be confident that they've examined the proposals thoroughly enough to give an "ACK" that the drafts should be formalised and move forwards into implementation/deployment phases.

Benefits of participating:

- Deeply understand schnorr and taproot
- Be a stakeholder in Bitcoin consensus development
- Support/safeguard decentralisation of Bitcoin protocol development
- Have fun!

¡Muchas gracias!

Muito Obrigado!