b
UNIVERSITY
OF BERN

Beyond Software Families: Community-Driven Variability

Roman Bögli, Alexander Boll, Alexander Schultheiß, and Timo Kehrer

Software Engineering Group (SEG), University of Bern, Switzerland

FSE, 2025-06-23, Trondheim NO

Who rules bitcoin?

Source: bitcoin.org/en/choose-your-wallet

Operating System

Mobile

Desktop

Hardware

User type

New

Experienced

Criteria

Control

Validation

Transparency

Environment Not available

Privacy

Fees

Features

2FA

Bech32

Full Node

Hardware Wallet

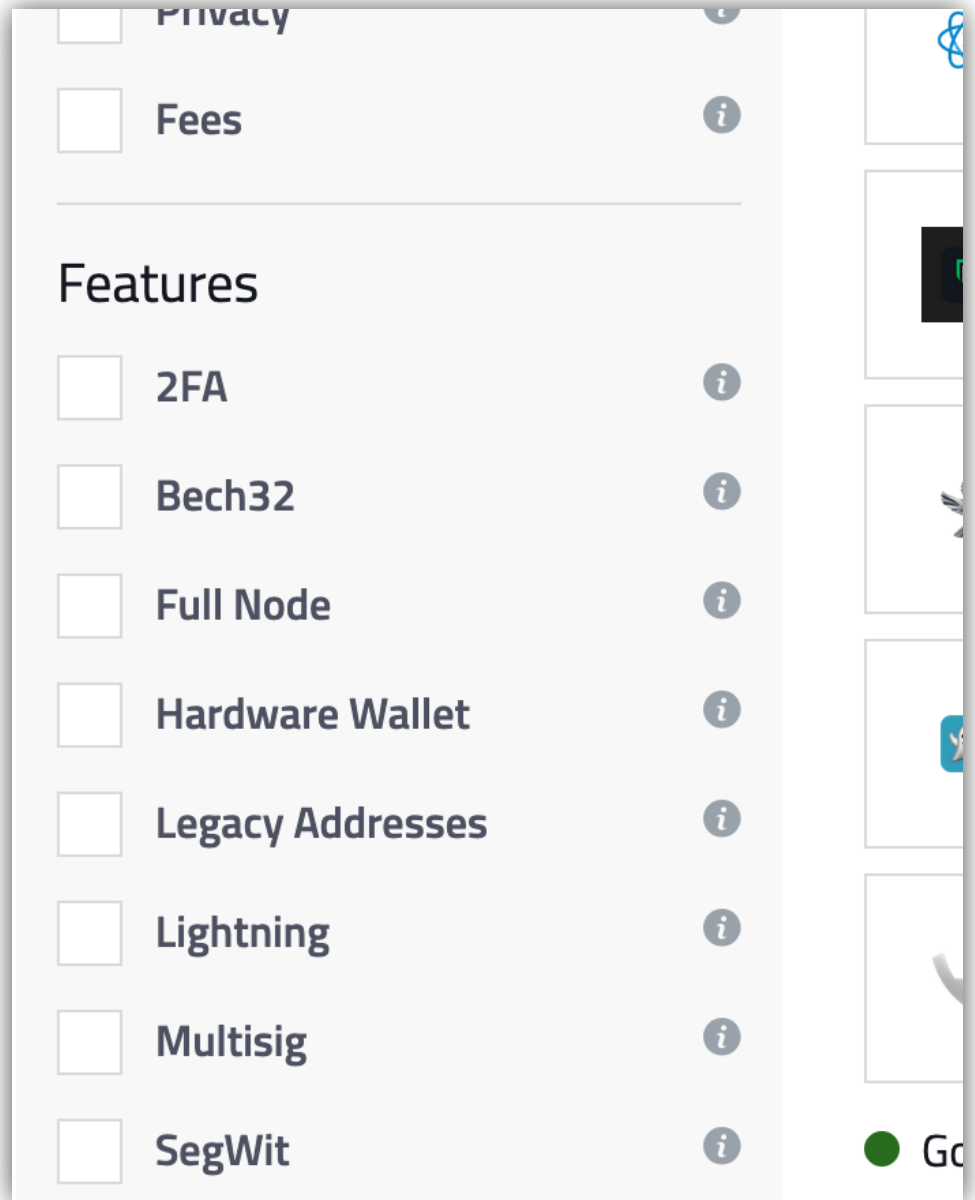
Legacy Addresses

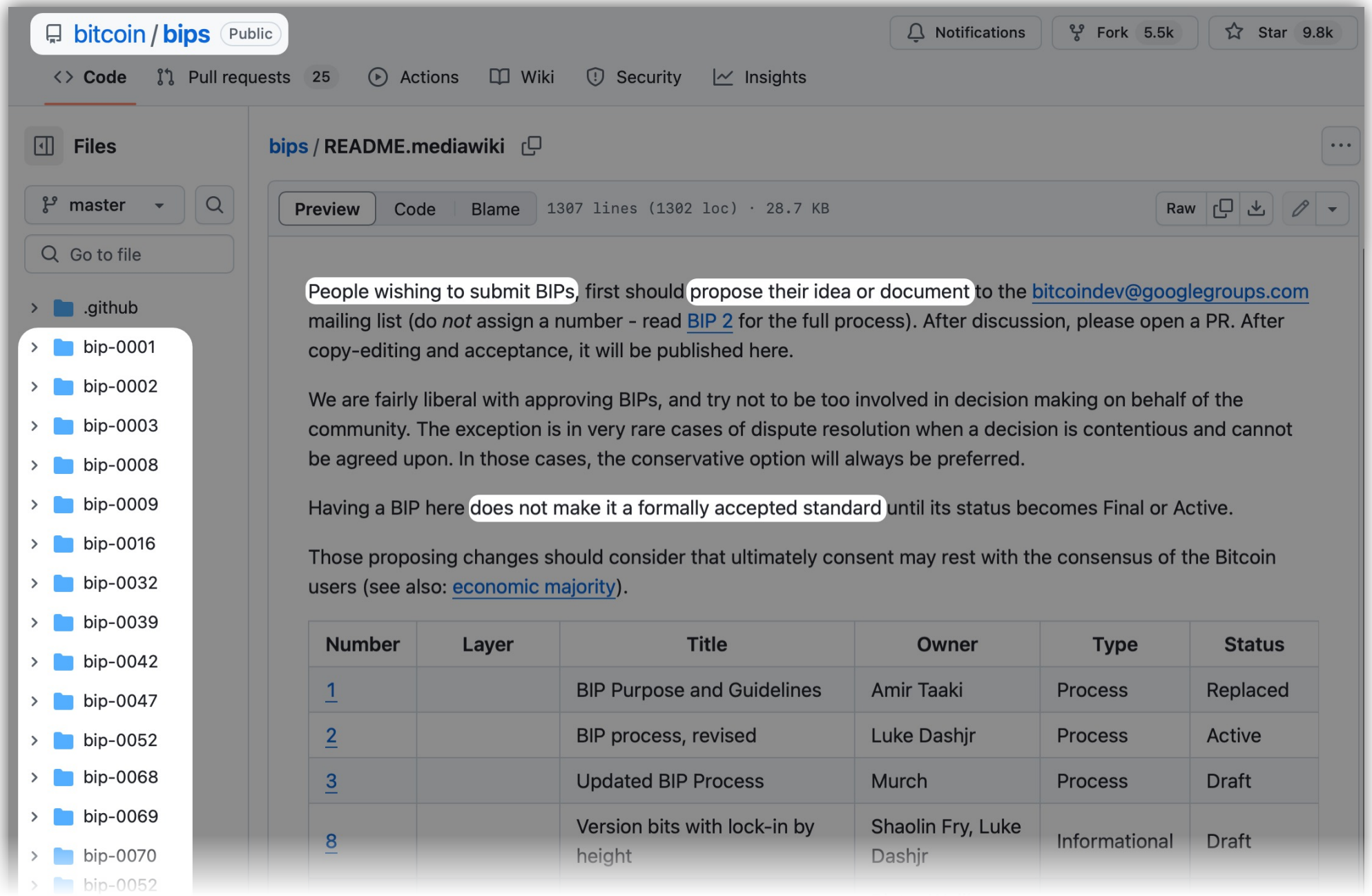
Below is a list of wallets available for your operating system

Linux Wallets	Control	Validation	Transparency	Environment	Privacy	Fees
Armory	●	●	◢	▲	●	●
Bitcoin Core	●	●	●	▲	●	●
Bitcoin Knots	●	●	●	▲	●	●
Bither	●	◢	◢	▲	◢	▲
BitPay	●	▲	◢	▲	◢	◢
Electrum	●	◢	●	◢	◢	●
Green	●	▲	◢	◢	◢	●
Sparrow	●	◢	◢	▲	●	●
Specter	●	●	◢	▲	●	●

Source: bitcoin.org/en/choose-your-wallet

bitcoin





Source: github.com/bitcoin/bips

bitcoin / bips Public

Notifications Fork 5.5k Star 9.8k

Code Pull requests 25 Actions Wiki Security Insights

Files

master

Go to file

- .github
- bip-0001
- bip-0002
- bip-0003
- bip-0008
- bip-0009
- bip-0016
- bip-0032
- bip-0039
- bip-0042
- bip-0047
- bip-0052
- bip-0068
- bip-0069
- bip-0070
- bip-0052
- bip-0068
- bip-0069
- bip-0070
- bip-0073
- bip-0075
- bip-0098
- bip-0114
- bip-0119
- bip-0122
- bip-0135
- bip-0144
- bip-0152
- bip-0156
- bip-0158
- bip-0174

bips / README.mediawiki

Preview Code Blame 1307 lines (1302 loc) · 28.7 KB Raw

People wishing to submit BIPs, first should propose their idea or document to the bitcoindev@googlegroups.com mailing list (do *not* assign a number - read BIP 2 for the full process). After discussion, please open a PR. After copy-editing and acceptance, it will be published here.

We are fairly liberal with approving BIPs, and try not to be too involved in decision making on behalf of the community. The exception is in very rare cases of dispute resolution when a decision is contentious and cannot be agreed upon. In those cases, the conservative option will always be preferred.

Having a BIP here does not make it a formally accepted standard until its status becomes Final or Active.

Those proposing changes should consider that ultimately consent may rest with the consensus of the Bitcoin users (see also: economic majority).

Number	Layer	Title	Owner	Type	Status
1		BIP Purpose and Guidelines	Amir Taaki	Process	Replaced
2		BIP process, revised	Luke Dashjr	Process	Active
3		Updated BIP Process	Murch	Process	Draft
8		Version bits with lock-in by height	Shaolin Fry, Luke Dashjr	Informational	Draft
9		Version bits with timeout and delay	Pieter Wuille, Peter Todd, Greg Maxwell, Rusty Russell	Informational	Final
10	Applications	Multi-Sig Transaction Distribution	Alan Reiner	Informational	Withdrawn
11	Applications	M-of-N Standard Transactions	Gavin Andresen	Standard	Final
12	Consensus (soft fork)	OP_EVAL	Gavin Andresen	Standard	Withdrawn
13	Applications	Address Format for pay-to-script-hash	Gavin Andresen	Standard	Final
14	Peer Services	Protocol Version and User Agent	Amir Taaki, Patrick Strateman	Standard	Final
15	Applications	Aliases	Amir Taaki	Standard	Deferred
	Consensus				

bips / bip-0173.mediawiki

Preview Code Blame 415 lines (340 loc) · 20.3 KB Raw

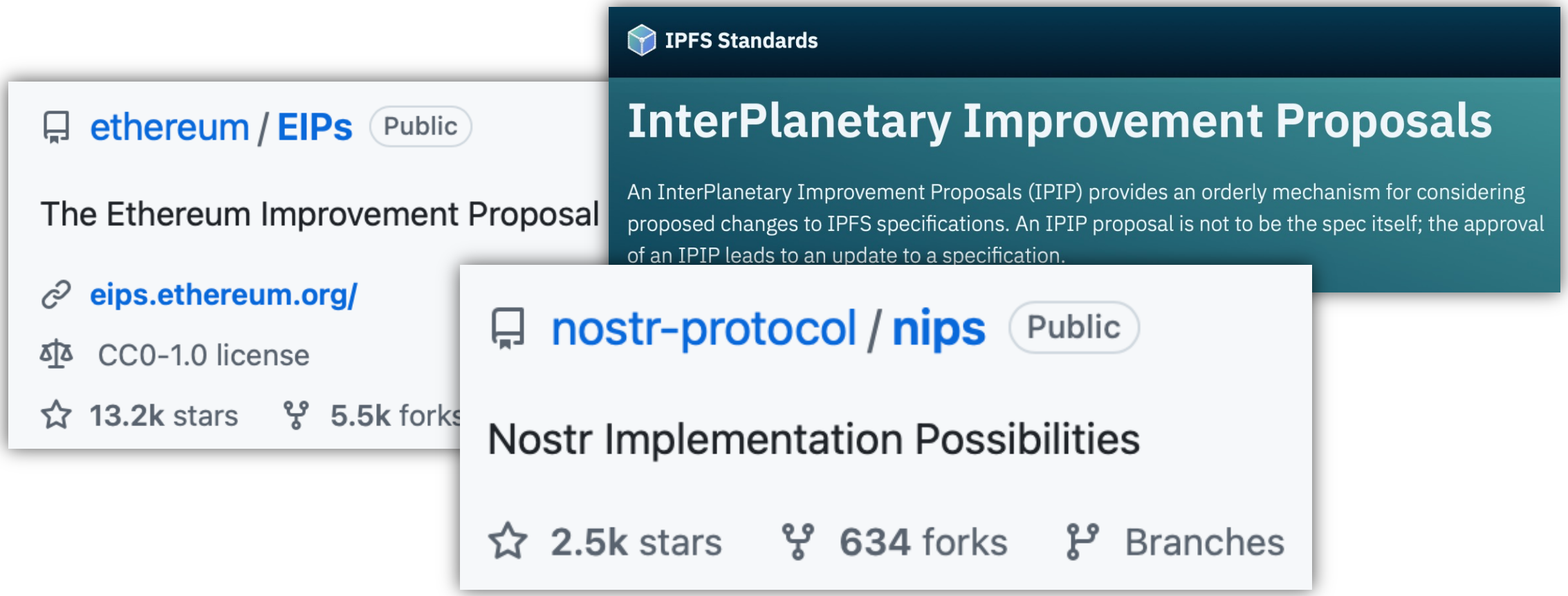
```
BIP: 173
Layer: Applications
Title: Base32 address format for native v0-16 witness outputs
Author: Pieter Wuille <pieter.wuille@gmail.com>
        Greg Maxwell <greg@xiph.org>
Comments-Summary: No comments yet.
Comments-URI: https://github.com/bitcoin/bips/wiki/Comments:BIP-0173
Status: Final
Type: Informational
Created: 2017-03-20
License: BSD-2-Clause
Replaces: 142
Superseded-By: 350
```

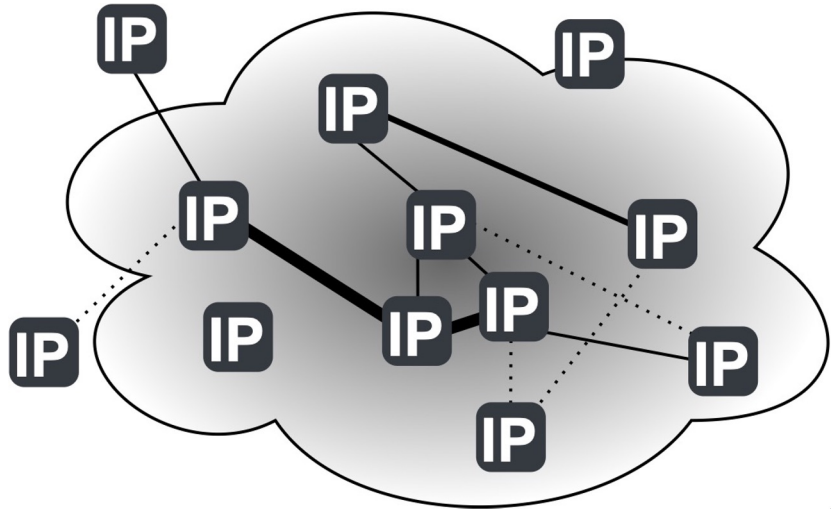
Table of Contents

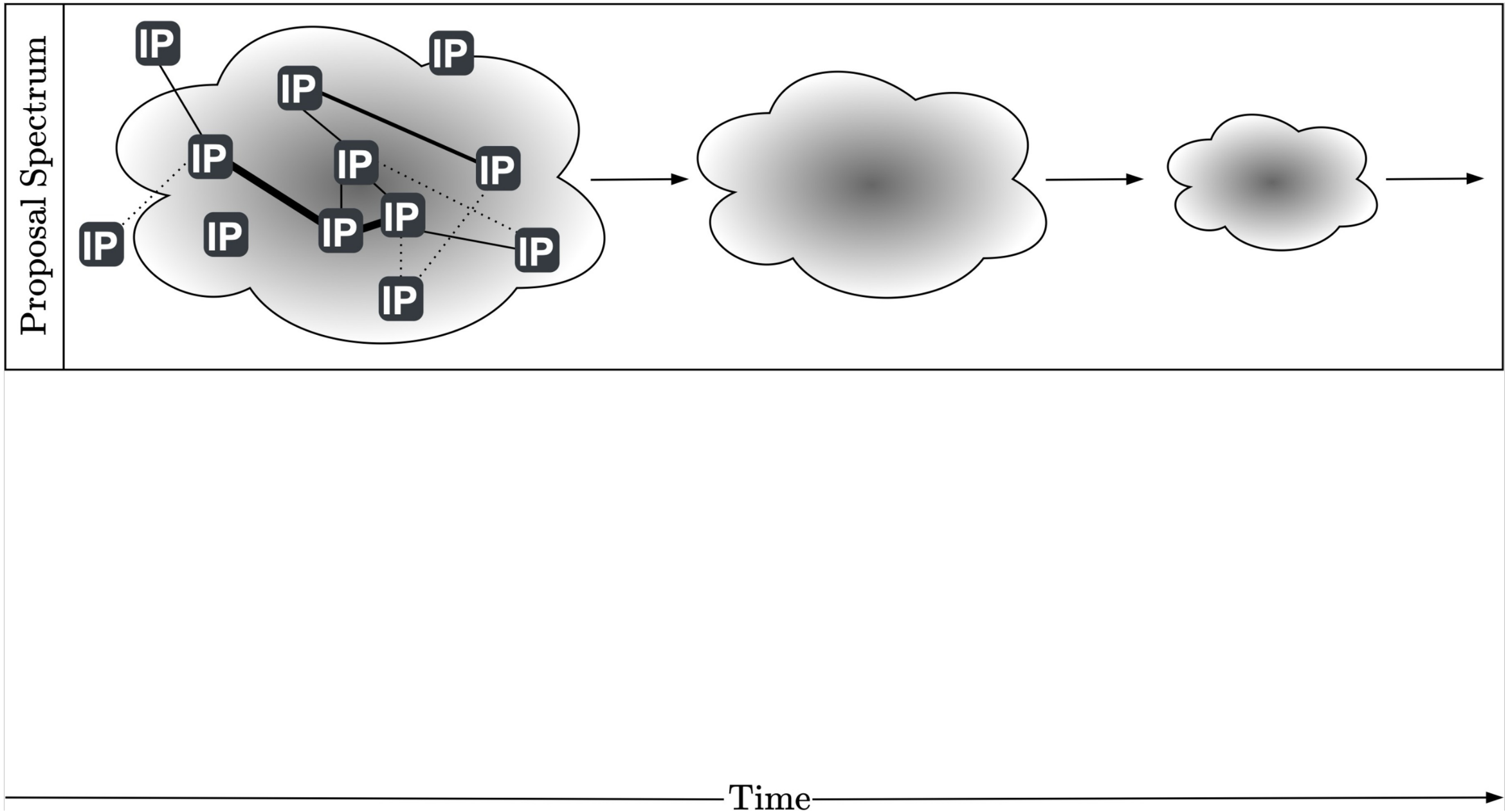
- Introduction
  - Abstract

Source: github.com/bitcoin/bips/...bip-0173

bitcoin


ethereum / EIPs
Public
The Ethereum Improvement Proposal
eips.ethereum.org/
CC0-1.0 license
13.2k stars
5.5k forks
IPFS Standards
InterPlanetary Improvement Proposals
An InterPlanetary Improvement Proposals (IPIP) provides an orderly mechanism for considering proposed changes to IPFS specifications. An IPIP proposal is not to be the spec itself; the approval of an IPIP leads to an update to a specification.
nostr-protocol / nips
Public
Nostr Implementation Possibilities
2.5k stars
634 forks
Branches

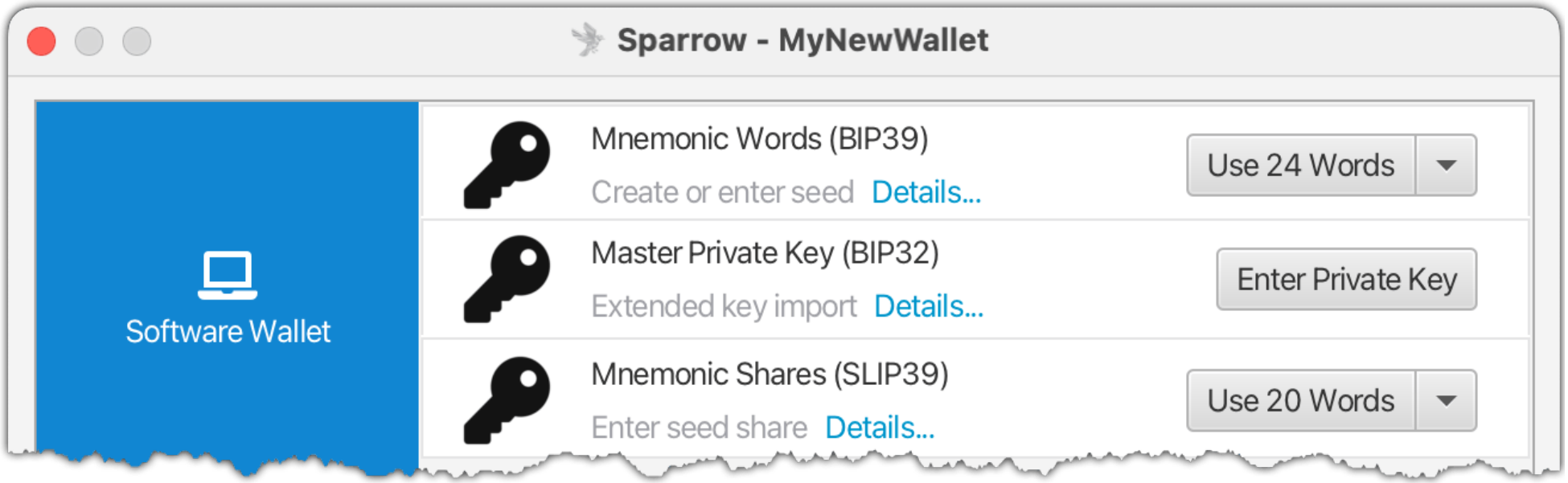

IP
IP
IP
IP
IP
IP
IP
IP
IP
IP
IP

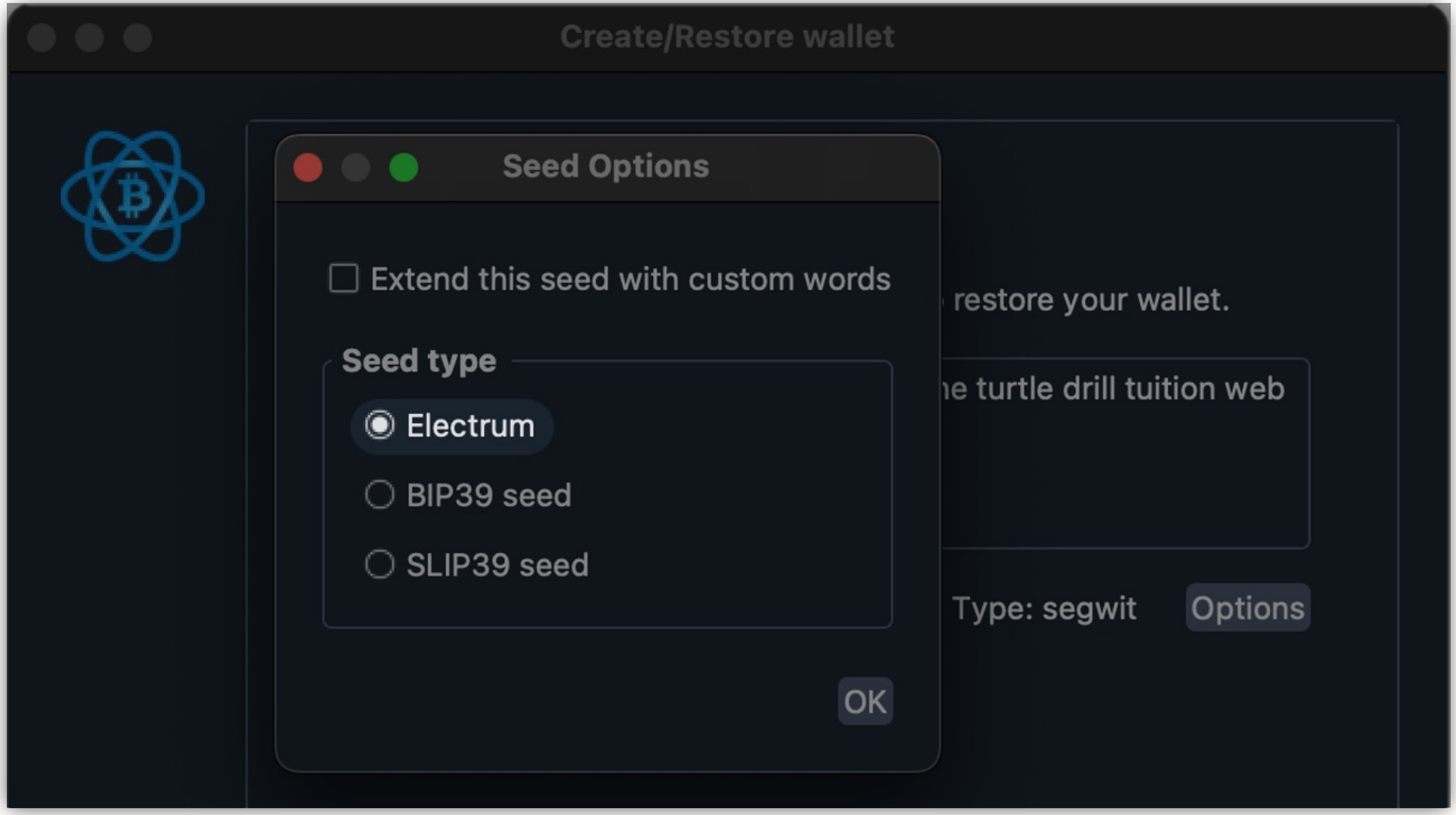

Proposal Spectrum
IP
IP
IP
IP
IP
IP
IP
IP
IP
IP
IP
Time

...but Standards Based

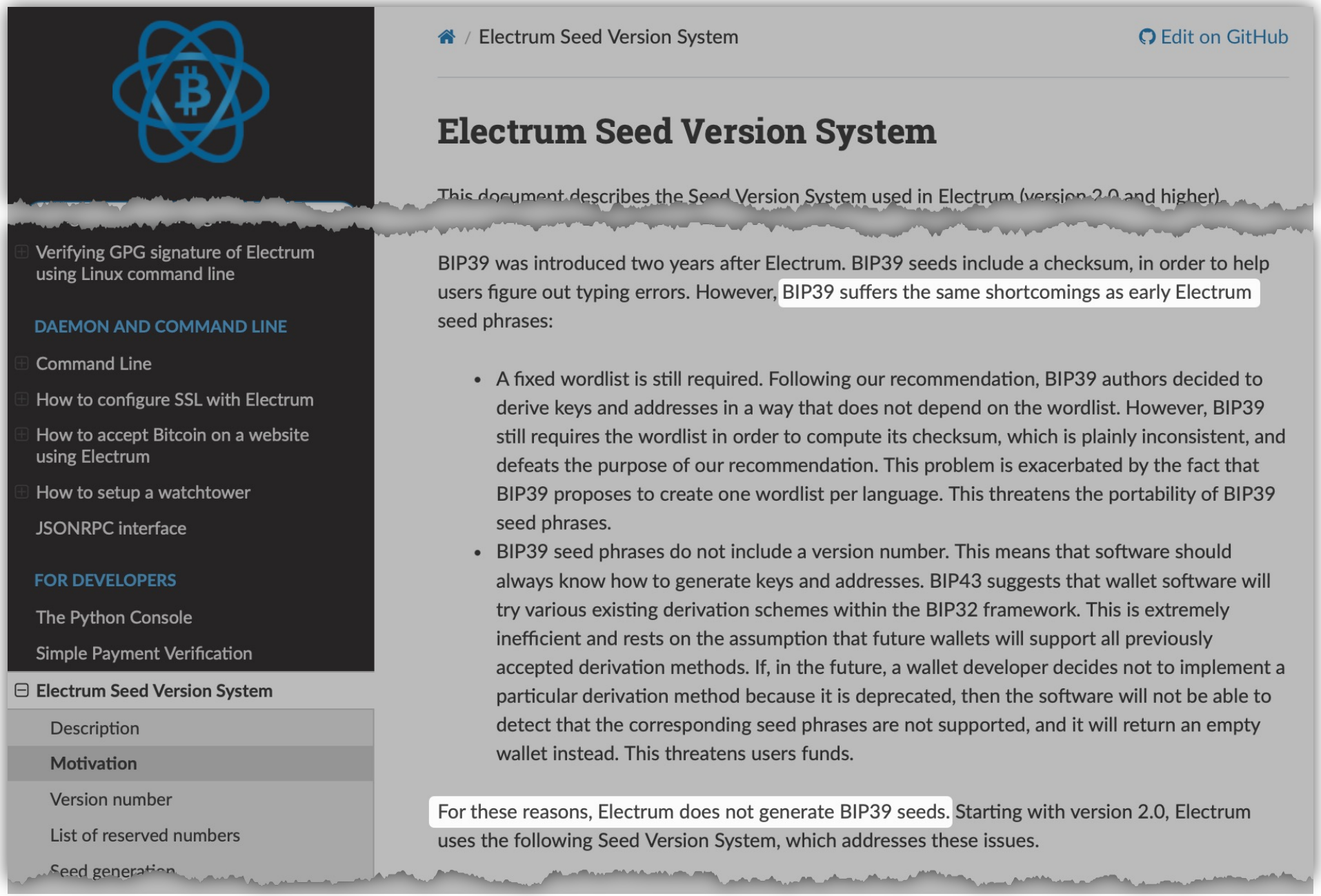
Sparrow tries wherever possible to adhere to commonly accepted standards in order to have as wide an interoperability as possible. In particular, it has been built to support Partially Signed Bitcoin Transactions (PSBTs) from the ground up, influencing everything from the keystore design to the transaction editor.

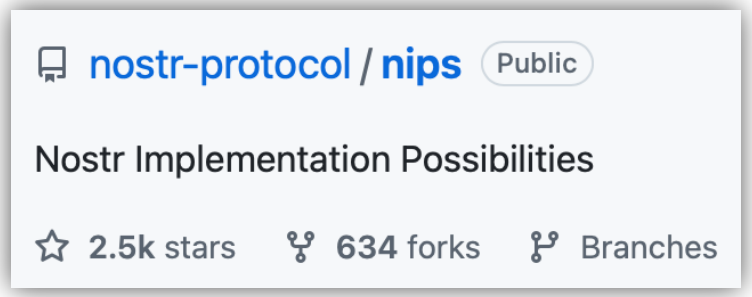
Source: sparrowwallet.com




Create/Restore wallet
Seed Options
Extend this seed with custom words
Seed type
Electrum
BIP39 seed
SLIP39 seed
OK
restore your wallet.
turtle drill tuition web
Type: segwit
Options

Source:
electrum.readthedocs.io





Clients

Source: github.com/.../awesome-nostr

- Agora Stars 17 - Follow your favorite topics in nostr-verse (and even posts from Mastodon, Reddit, Bluesky, and Twitter)
- Alexandria Stars 11 - A Knowledge Base and future eReader app. Focuses on the implementation of NKBIP-01
- algia-web Stars 11 - A small resource consumption oriented Nostr web client
- algia Stars 188 - A cli application for nostr.
- alphaama Stars 27 - alphaama is just a nostr fucking client
- Amethyst Stars 1.2k - An Android client for nostr written in Kotlin
- Anonostr Stars 14 - Anonostr allows users to send anonymous notes to the Nostr network without revealing their identity. For each note submission, the app generates a new key pair, sends the note through select relays, and then securely burns the key pair.
- ArcadeCity Stars 22 - Public group chats and P2P services (WIP) over nostr
- Asknostr.site - A Quora/StackOverflow Q&A site using the nostr network and #asknostr content
- Astral Stars 101 - a branle fork with global feed and UI makeover
- Attached Stars 26 - Open-Source ReactNative Expo app for Nostr (iOS, Android).
- badger Stars 0 - A NIP58 nostr badge client. Create Badges view Profile Badges and more.
- Beagle Stars 30 - Decentralized real-time Text/Audio/Video chat client for iOS, using nostr relays for users to share information and moments by posts of text, image and video.
- BlazeJump Stars 6 - A fast web client boilerplate written in C# / Blazor, that uses an in-browser SQLite database.
- Blowater - A desktop Web client focusing on chat with delightful UX

nostr-protocol / nips Public

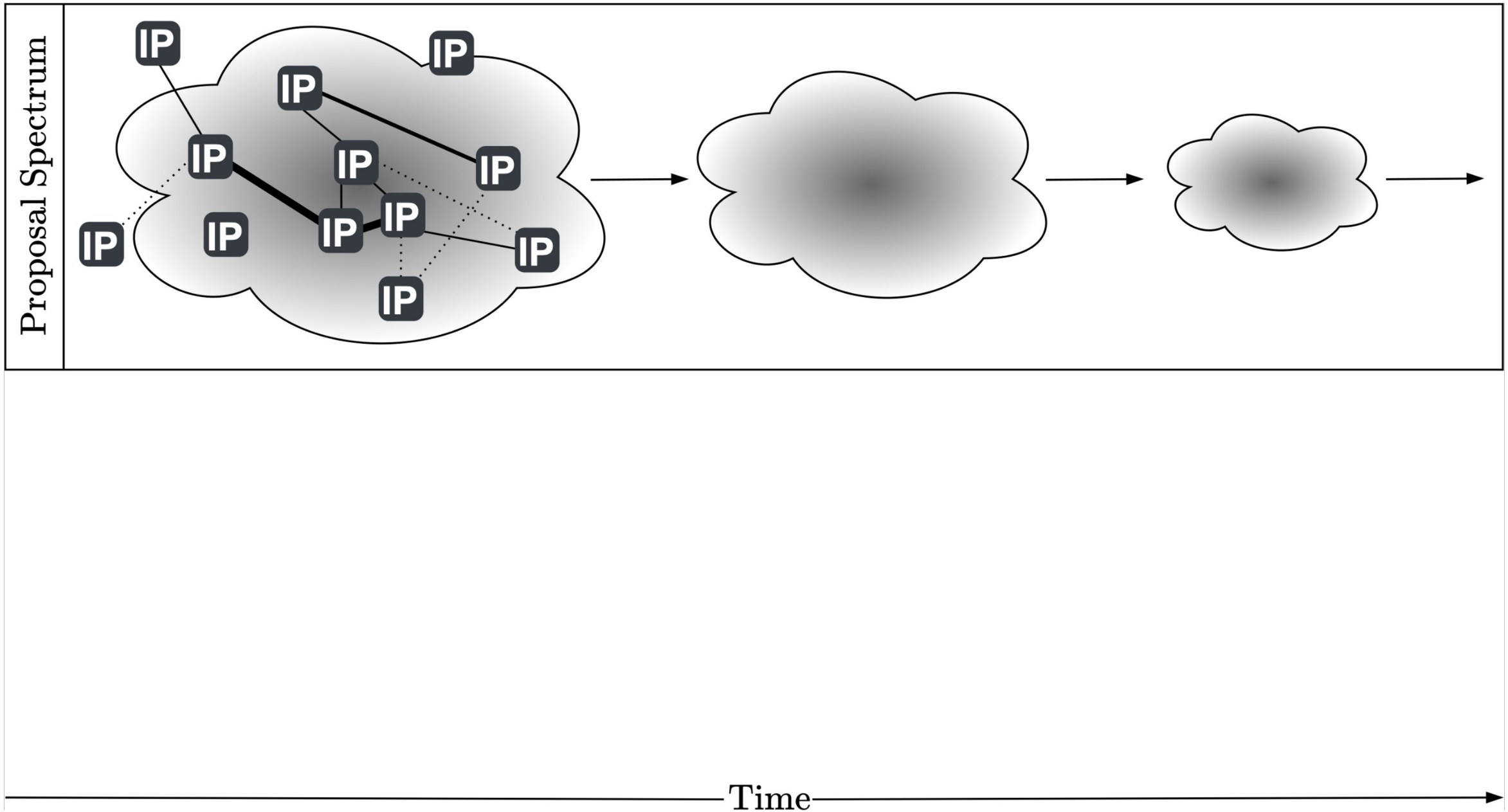
Nostr Implementation Possibilities

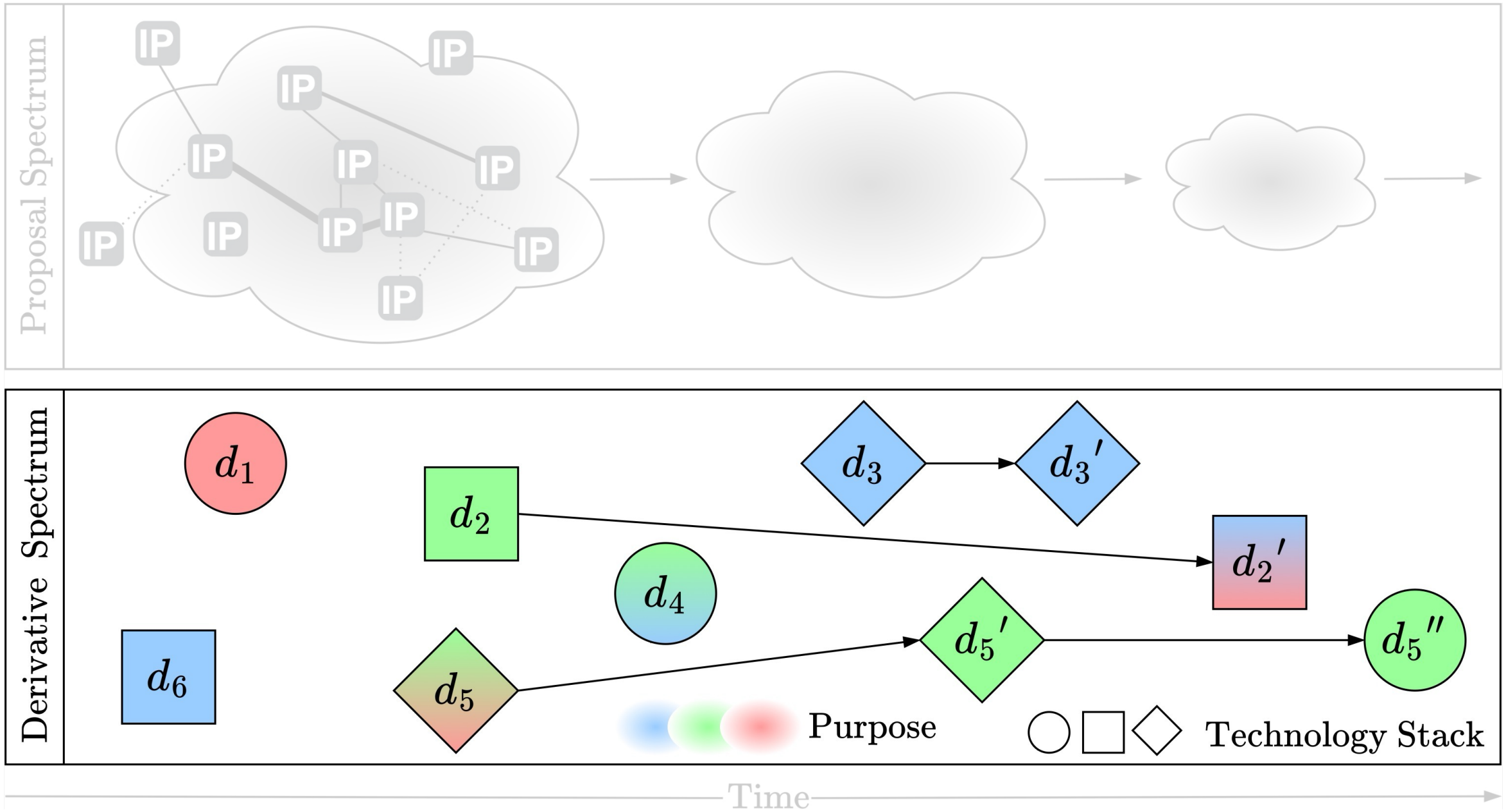
2.5k stars 634 forks Branches

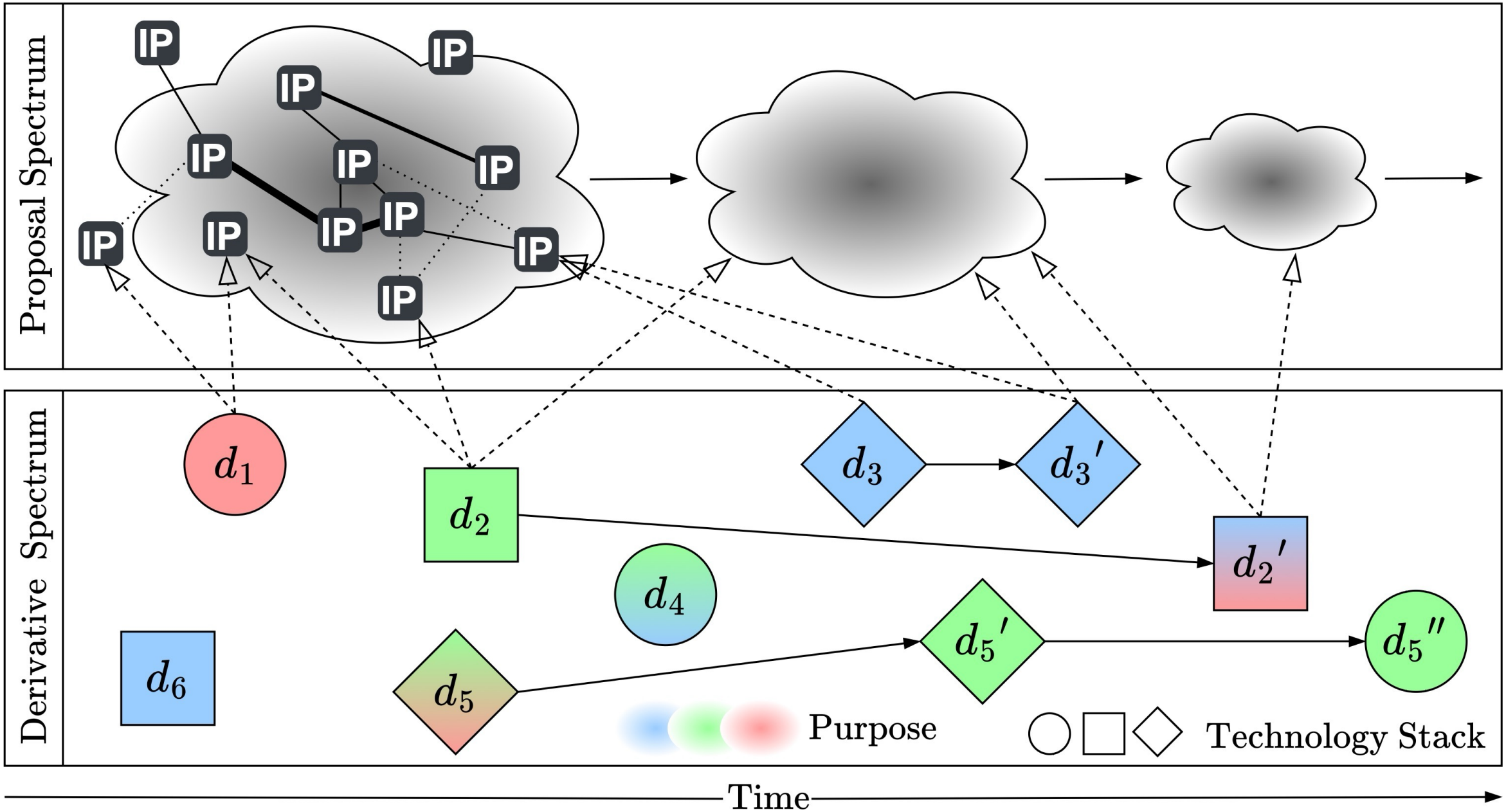
Clients

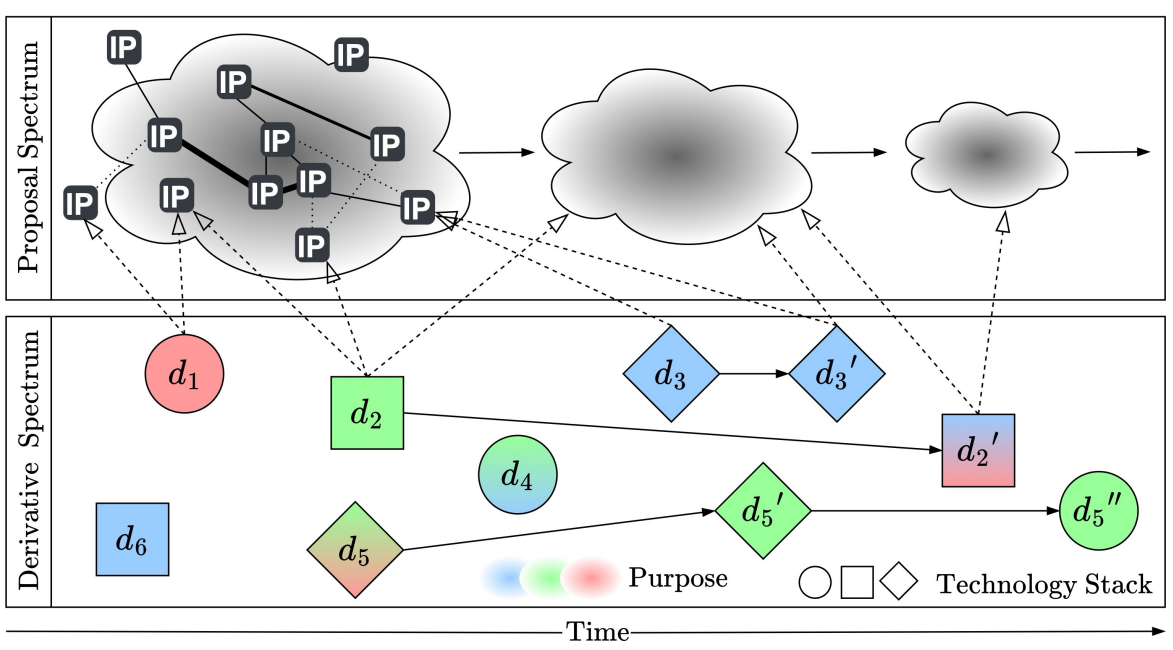
Source: github.com/.../awesome-nostr

- Agora Stars 17 - Follow your favorite topics in nostr-verse (and even posts from Mastodon, Reddit, Bluesky, and Twitter)
- Alexandria Stars 11 - A Knowledge Base and future eReader app. Focuses on the implementation of NKBIP-01
- algia-web Stars 11 - A small resource consumption oriented Nostr web client
- algia Stars 188 - A cli application for nostr.
- alphaama Stars 27 - alphaama is just a nostr fucking client
- Amethyst Stars 1.2k - An Android client for nostr written in Kotlin
- Anonostr Stars 14 - Anonostr allows users to send anonymous notes to the Nostr network without revealing their identity. For each note submission, the app generates a new key pair, sends the note through select relays, and then securely burns the key pair.
- ArcadeCity Stars 22 - Public group chats and P2P services (WIP) over nostr
- Asknostr.site - A Quora/StackOverflow Q&A site using the nostr network and #asknostr content
- Astral Stars 101 - a branle fork with global feed and UI makeover
- Attached Stars 26 - Open-Source ReactNative Expo app for Nostr (iOS, Android).
- badger Stars 0 - A NIP58 nostr badge client. Create Badges view Profile Badges and more.
- Beagle Stars 30 - Decentralized real-time Text/Audio/Video chat client for iOS, using nostr relays for users to share information and moments by posts of text, image and video.
- BlazeJump Stars 6 - A fast web client boilerplate written in C# / Blazor, that uses an in-browser SQLite database.
- Blowater - A desktop Web client focusing on chat with delightful UX


Proposal Spectrum
IP
IP
IP
IP
IP
IP
IP
IP
IP
IP
IP
Time


Proposal Spectrum
IP
Derivative Spectrum
d_1
d_2
d_3
d_3'
d_2'
d_4
d_5
d_5'
d_5''
d_6
Purpose
Technology Stack
Time


Proposal Spectrum
IP
Derivative Spectrum
d_1
d_2
d_3
d_3'
d_2'
d_4
d_5
d_5'
d_5''
d_6
Purpose
Technology Stack
Time



Community-Driven Variability (CDV)

Community-Driven Variability (CDV)

- **C1** Crowdsourcing
- **C2** Improvement Proposals
- **C3** Independent Derivatives
- **C4** Interoperability
- **C5** Decoupled Evolution

So what?

P1 Missing overview in proposal spectrum

P2 Missing overview in derivative spectrum

P3 IP change impact assessment

P4 Misalignment of proposal & derivative spectrum

P5 Level of derivative interoperability

P6 Ecosystem forks

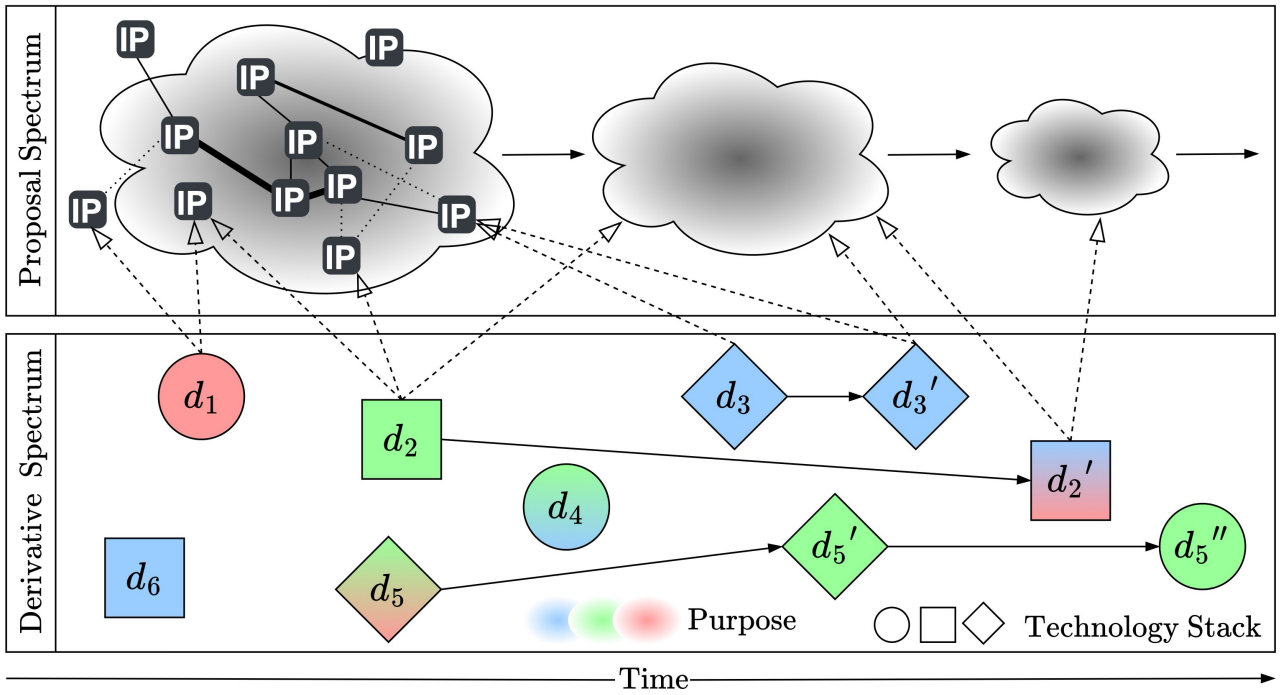
RG1 Systematic treatment of CDV in proposal spectrum

RG2 Supporting cohesive evolution of proposal and derivative spectrum

RG3 Methodical handling of derivative interoperability impairment

Community-Driven Variability

Preprint



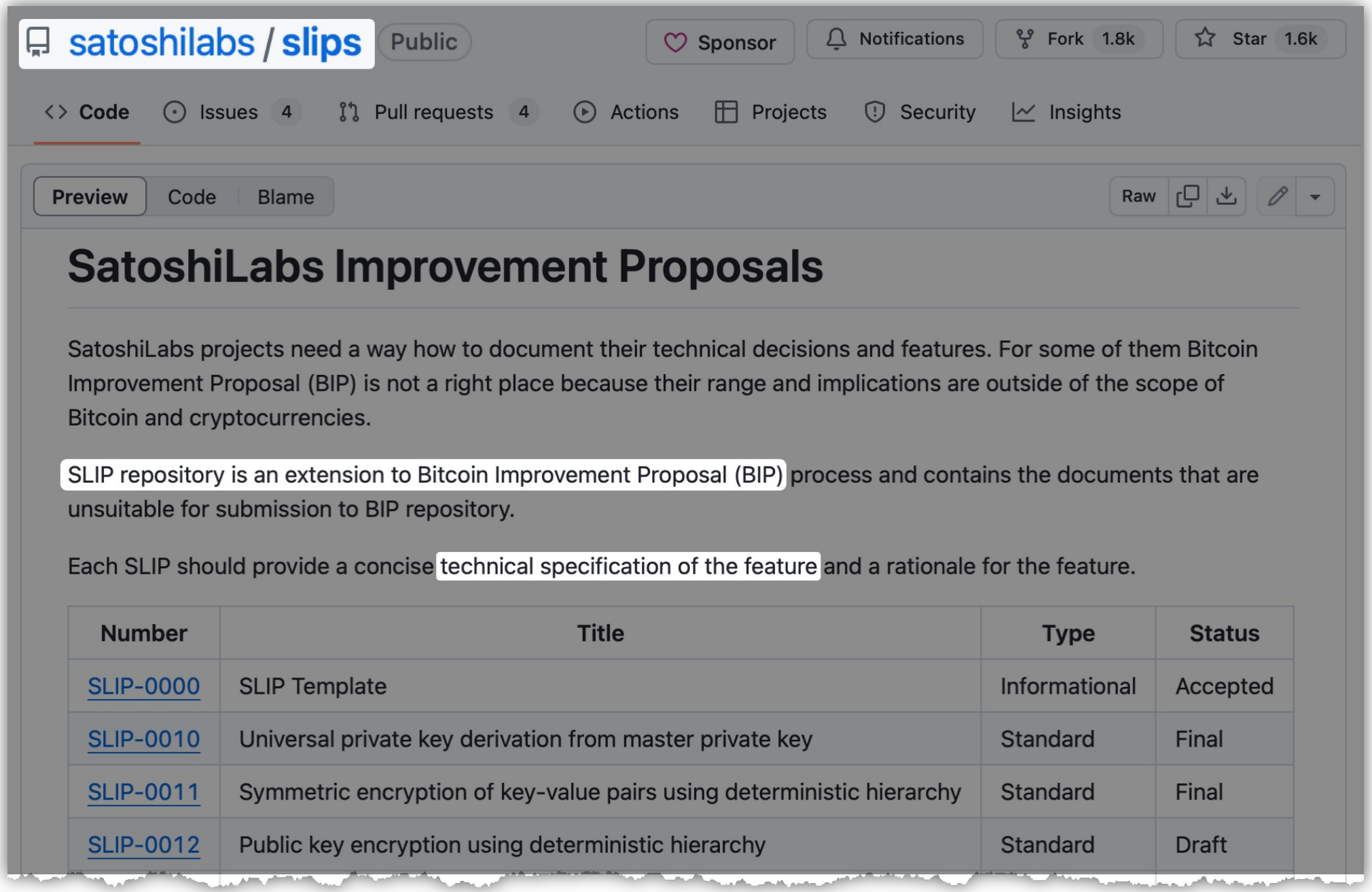
- **C1** Crowdsourcing
- **C2** Improvement Proposals
- **C3** Independent Derivatives
- **C4** Interoperability
- **C5** Decoupled Evolution

Boegli_2025_CDV_Preprint.pdf

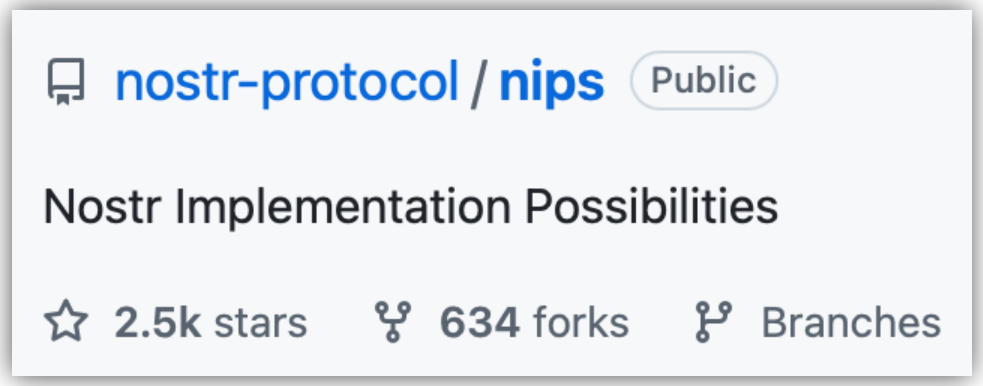
- **P1** Missing overview in proposal spectrum
- **P2** Missing overview in derivative spectrum
- **P3** IP change impact assessment
- **P4** Misalignment of proposal/derivative spectrum
- **P5** Level of derivative interoperability
- **P6** Ecosystem forks

- **RG1** Systematic treatment of CDV in proposal spectrum
- **RG2** Supporting cohesive evolution of proposal and derivative spectrum
- **RG3** Methodical handling of derivative inter-operability impairment

Appendix



Source: github.com/satoshilabs



§ NIPs

A Nostr Implementation Possibilty, or NIP for short, exist to document what MUST, what SHOULD and what MAY be implemented by Nostr-compatible relay and client software.

NIPs are the documents that outline how the Nostr protocol works.

Source: nostr.how

```
  BIP:               <BIP number, or "?" before being assigned>
* Layer:             <Consensus (soft fork) | Consensus (hard fork) |
                      Peer Services | API/RPC | Applications>
  Title:             <BIP title; maximum 44 characters>
  Author:            <list of authors' real names and email addrs>
* Discussions-To:    <email address>
  Status:            <Draft | Active | Proposed | Deferred | Rejected |
                      Withdrawn | Final | Replaced | Obsolete>
  Type:              <Standards Track | Informational | Process>
* Requires:          <BIP number(s)>
* Replaces:          <BIP number>
* Superseded-By:     <BIP number>
```

Figure 1: Excerpt of BIP preamble structure from BIP2 [29].

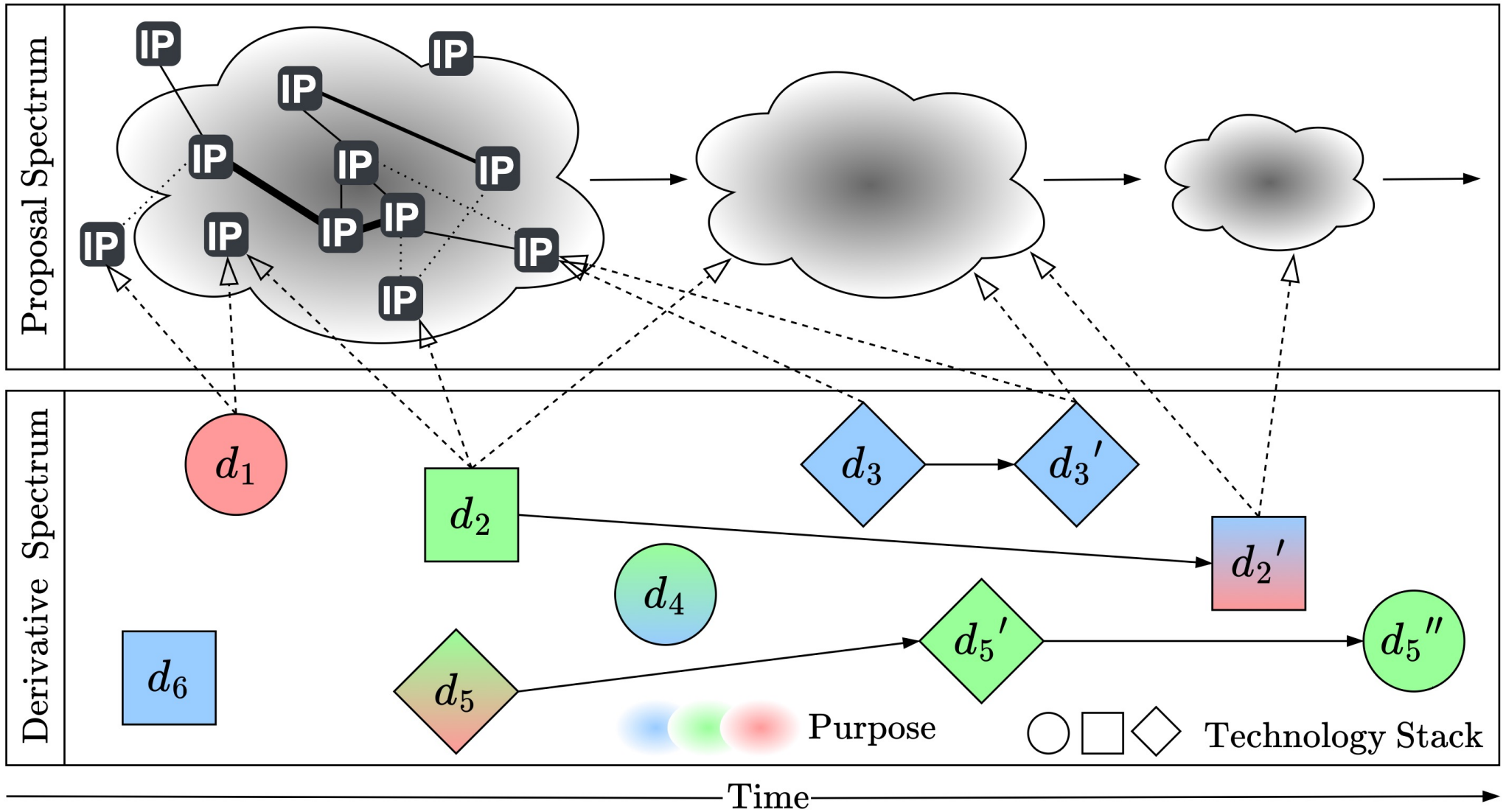


Figure 2: A schematic overview of the CDV landscape.

P1 & P2 – Missing overview of proposal and derivative spectrum: Due to the dynamics imposed by characteristics C1-C5, communities typically lack an overview of the entire ecosystem and its evolution. Consequently, involved actors lack orientation for guiding their decisions within the ecosystem. This missing overview is felt on both levels: the proposal spectrum (P1), and the derivative spectrum (P2). Realizing the need for an overview, the Bitcoin community already created a number of websites that monitor [10], compare [1, 24], or suggest [5] derivatives. We find these handcrafted ad-hoc monitoring efforts insufficient, but they underscore the richness of existing variability and, more importantly, the need to manage it effectively.

P3 – IP change impact assessment: The actors (C1) in the ecosystem face challenges during suggesting and updating IPs (C2), such as avoiding unforeseen side effects and change impact assessment (C4). For example, although on-boarding developer guidelines exist in Bitcoin [40], resources that document the interrelations between BIPs or their perceived feature impacts are missing.

P4 – Misalignment of proposal and derivative spectrum: There is a common interest to avoid a misalignment (C5) of derivatives and the proposal spectrum. However, developers (C3) lack the necessary guidance for alignment, while end users are unable to verify it, undermining trust in derivatives (C4) and into the ecosystem. This lack of guidance is exemplified in Electrum avoiding BIP39 [7], whereas Sparrow "tries wherever possible to adhere to commonly accepted standards in order to have as wide an interoperability as possible." [27]

P5 – Determining interoperability of derivatives: The shared interest in interoperability (C4) forces developers and end users to be aware of potential restrictions of derivative interactions. A lack of interoperability can lead to immense damage, such as permanent financial losses due to wallet recovery issues [14, 26] or incorrectly mined blocks [22]. Some communities already introduced partial solutions for this problem, e.g., *feature vectors* [4], a handshake, that tests what features the other derivative implements prior to actual interaction. However, users could place more trust into a more rigorous procedure, that is formally derived from and enforced through an ecosystem's variability model.

P6 – Ecosystem fork: The independent evolution of proposals and derivatives (C5) can lead to complex phenomena: As some IPs are embraced by the whole community, others may be rejected by a tight-knit part of the community (C3). This can lead to a split within the ecosystem into fractions or a complete detachment, as sub-communities drift further and further apart. Ultimately, such detachments provoke yet another variability source for both IPs (C2) and derivatives (C3), catalyzing the severity of P1-P5. In Bitcoin and related domains, for instance, this phenomenon is referred to as *fork* and has had occurred several times in the past (e.g., Bitcoin Cash, Gold, SV) [23].

Characteristics Encouraging CDV

C1 – Crowdsourcing: There exists an open de-facto standard in the ecosystem that is continuously shaped by independent actors with distributed authority.

C2 – Improvement Proposals: This de-facto standard defines how the system shall operate using a set of improvement proposals (IPs) that can have dependencies, varying levels of importance, and undergo different states.

C3 – Independent Derivatives: Developers choose a set of IPs from which they implement independent derivatives using different technology stacks and targeting different use-cases.

C4 – Interoperability: The ecosystem's value and flourishing substantially depends on and encourages direct or indirect derivative interaction.

C5 – Decoupled Evolution: The de-facto standard, its feature specification, and the derivatives evolve autonomously and detached from each other while following their own life cycles.

Figure 3: Characteristics Encouraging CDV.

Table 1: CDV characteristics of selected ecosystems/projects.

Paradigm	Ecosystem/Project	C1	C2	C3	C4	C5
CDV	Bitcoin [2, 43]; Lightning [3, 48]	●	●	●	●	●
	Nostr [12]	●	●	●	●	●
	Ethereum [8]	◒	●	●	●	●
	Tor Protocol [13, 30]; IPFS [9, 21]	◒	●	●	●	●
SPL	Linux Kernel [15, 33]	◒	◒	◒	○	○
	Eclipse [25, 60]	◒	◒	◒	◒	○
	BusyBox [46, 62]	◒	◒	◒	○	○
Clone & Own	ApoGames [36, 42]	○	○	◒	○	◒
	Marlin Forks [37, 38]	○	○	◒	○	◒
	Health Watcher [56, 57]	○	○	◒	○	○

RG1 – Systematic treatment of CDV in proposal spectrum: Our first research goal is threefold. First, we aim to develop a variability modeling formalism and notation that can adequately capture CDV ecosystems and their evolution, providing a structured, explorable representation of the proposal spectrum amenable to analysis (P1). Second, we want to support the automated extraction of CDV models from various resources, with a focus on deriving variability models directly from IP collections. Third, analysis techniques shall be developed to reason about the structure and constraints of CDV models, spotting anomalous IPs and interrelations. This includes methods for differential analysis of CDV models representing different proposal spectrum snapshots, facilitating change impact analyses in the proposal spectrum (P3, P6).

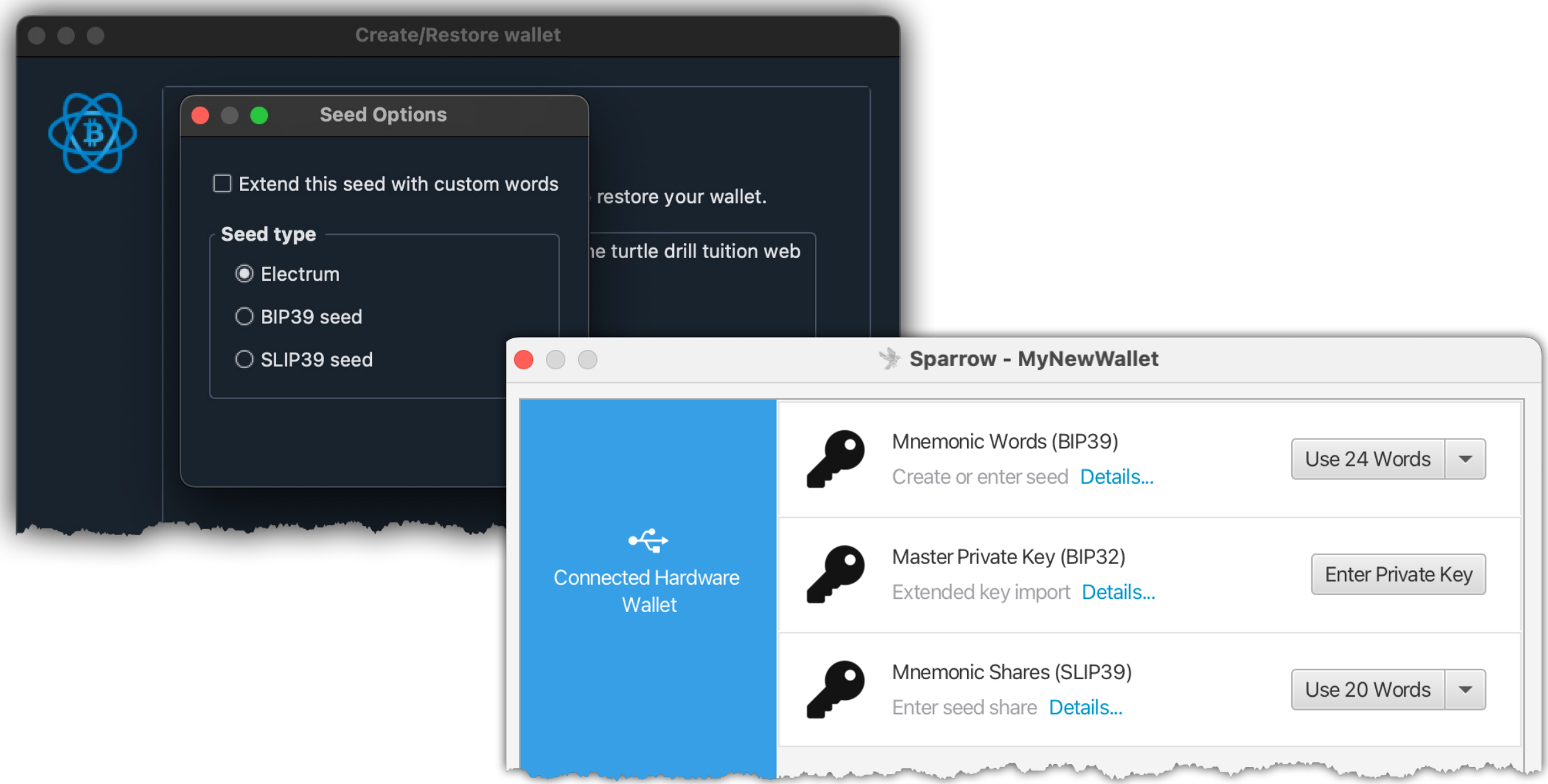
Impact: Holistic modeling of a CDV ecosystem's topology fostering comprehensibility and auditability.

RG2 – Supporting cohesive evolution of proposal and derivative spectrum: Given the autonomous evolution of these two spectra, our goal is to better understand and measure their cohesion (P4). This includes providing configuration support through CDV model-guided IP selection and first cohesion assessments by, e.g., checking a given set of IPs against a CDV model. However, the major endeavor pursued with this research goal is to support tracing of IPs from the proposal to the derivative spectrum, providing a better understanding of the derivative spectrum (P2) and facilitate further change impact analyses (P3). Besides IP traceability, we aim at mining CDV models from existing derivatives, enabling comparisons with those extracted from the IP spectrum (P4) and analyzing potential drift between community forks (P6).

Impact: Streamline the evolution of ecosystems by increasing the efficiency and effectiveness of future development endeavors.

RG3 – Methodical handling of derivative interoperability impairment: We dedicate our final research goal to address the challenges related to impaired interoperability within the derivative spectrum (P5), which boils down to handling and detecting undesired inter-derivative IP interactions. Anticipated interactions shall be documented and articulated through the CDV model, amenable to automatically validating derivatives wrt. proposal spectrum alignment (P4). Unanticipated interactions impairing interoperability shall be detected through systematic IP interaction testing, which must be both effective and efficient to be accepted in practice.

Impact: Reduce the effort and complexity of proper inter-derivative feature testing, further maximizing interoperability and positive user experience.


Create/Restore wallet
Seed Options
Extend this seed with custom words
Seed type
Electrum
BIP39 seed
SLIP39 seed
restore your wallet.
e turtle drill tuition web
Sparrow - MyNewWallet
Connected Hardware Wallet
Mnemonic Words (BIP39)
Create or enter seed Details...
Use 24 Words
Master Private Key (BIP32)
Extended key import Details...
Enter Private Key
Mnemonic Shares (SLIP39)
Enter seed share Details...
Use 20 Words

nostr-protocol / nips Public

Nostr Implementation Possibilities

2.5k stars 634 forks Branches

Source: next.nostr.watch

nostr.watch home relays operators monitors preferences

wss://nostr-relay.app/

A high-performance nostr relay, using PostgreSQL

Online
Last Seen 1 Hour Ago

Overview

Checks

NIP-11

Audit

Insights

Operator

Feed

NIP-11 last synced wtf? unknown

NIP-11 requires attention


```
{
    "name": "nostr-relay-nestjs",
    "version": "2.2.0",
    "description": "A high-performance nostr relay, using PostgreSQL",
    "pubkey": "8125b911ed0e94dbe3008a0be48cfe5cd0c0b05923cfff917ae7e87da8400883",
    "contact": "codytseng98@gmail.com
    "software": "git+https://github.c
    "git_commit_sha": "aab48b2",
    "supported_nips": [
        1,
        2,
        4,
        11,
        13,
        22,
        26,
        28,
        40,
        42
    ],
    "limitation": {
        "max_message_length": 131072,
        "max_subscriptions": 20,
        "max_filters": 10,
        "max_limit": 1000,
        "max_subid_length": 128,
```



```
"supported_nips": [
    1,
    2,
    4,
    11,
    13,
    22,
    26,
    28,
    40,
    42
```

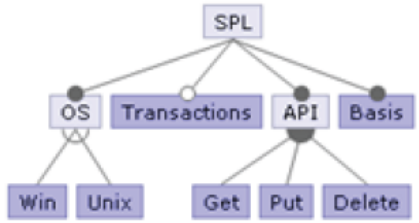
SPL

Problem Space

Solution Space

Domain Eng.

- Variability model (FMs)



map

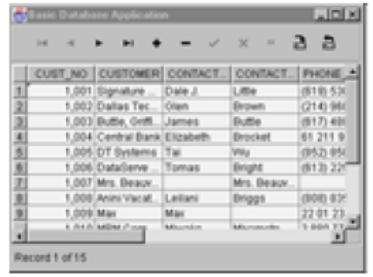
- Reusable implementation artifacts

App. Eng.

- Configuration (feature selection)

- Generated product

generate



CDV

Problem Space

Solution Space

Domain Eng.

- Collection of specification documents / improvement proposals / implementation possibilities
- BIPs, NIPs, EIPs, etc.

???

select

- [x] NIP-01: Basic protocol flow description
- [x] NIP-02: Contact List and Petnames
- [ ] NIP-04: Encrypted Direct Message
- [x] NIP-05: Mapping Nostr keys to DNS-based internet identifiers
- [x] NIP-06: Basic key derivation from mnemonic seed phrase
- [x] NIP-07: `window.nostr` capability for web browsers
- [ ] NIP-08: Handling Mentions

App. Eng.

implement

Clients

>> algia-web Stars 11 - A small resource consumption oriented Nostr we
>> Agora Stars 10 - Follow your favorite topics in the Nostr-verse (a posts from Mastodon, Reddit, Bluesky, and Twitter)
>> algia Stars 166 - A cli application for nostr.
>> Amethyst Stars 1.1k - An Android client for nostr written in Kotlin
>> ArcadeCity Stars 21 - Public group chats and P2P services (WIP) ove
>> Astral Stars 103 - a branle fork with global feed and UI makeover

Thanks

b
UNIVERSITY
OF BERN