# BitcoinのSoft Fork

BIP-9

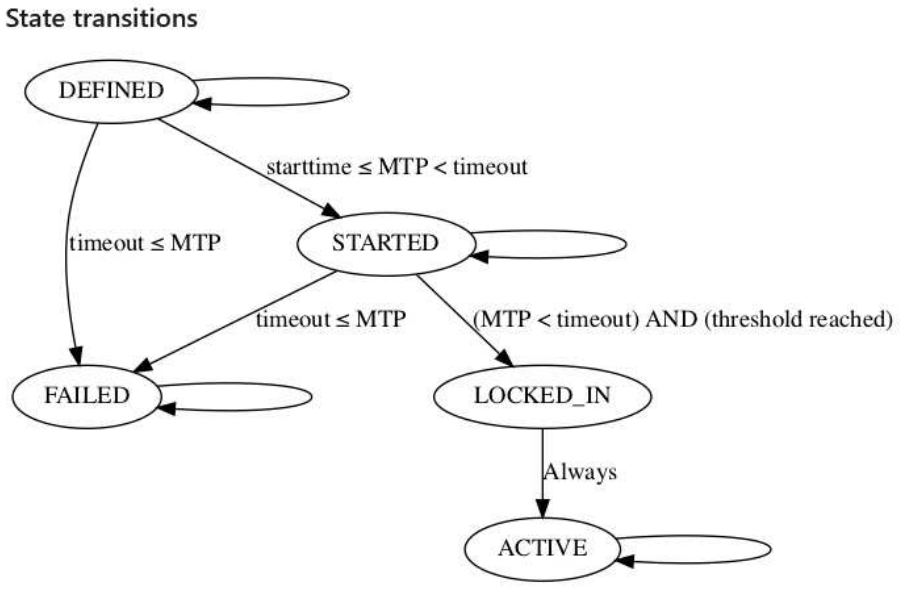
- BIP-9概要 - ChatGPT

### しくみの名前

VersionBits

### 概要

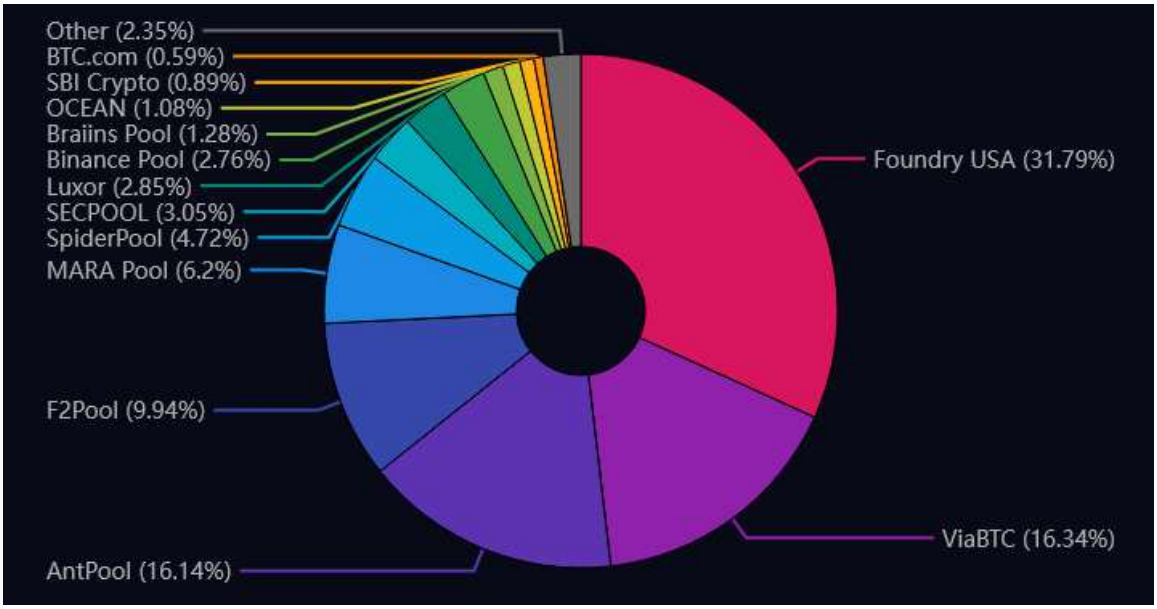
- Bitcoinのソフトフォークのアクティベーションを柔軟に行うための仕組み
- マイナーによる信号送信 を用いた 投票方式のソフトフォークのアクティベーション
- ブロックのバージョンフィールドを使って、マイナーが特定の機能の有効化に賛成しているかを示す




- 投票の状態が STARTED になって、承認率が閾値に達すると LOCKED_IN になり、次のタイイングで必ず ACTIVE になる
  - 投票：マイナーがブロックを作るとき、`version`フィールドにビットを立てておくと投票したことになる
    - つまり、マイニングに成功しないと投票できない
    - ビットは0〜28まである。今は0と1だけ使われた？ 過去の投票歴？
  - 承認率
    - 投票期間のブロック数
    - 最初は1年間で95%だったようだ

        - 2016ブロックの95%は1916で、
    - SegWitのときは満たせず、BIP-91で限定的に80%にした(なんだそりゃ？)
        - BitcoinのSoft Fork#a235c4
    - Taprootのときは Speedy Trial というのを使って 3ヶ月で 90%に達したのでよしとした
        - これはBIPにないものだそうだ。
        - メーリングリストなどで決まったらしく実験的に行ったそうだ。
- `version` のどのビットを使うかは開発者で決めるものだそうだ
    - Taprootのときは bit 2 を使ったそうだが、BIP-9の履歴に載っていない

## まとめ

- 基本的にSoftForkに関する投票はBIP-9に沿っている
    - 期間と投票による閾値と投票したことを示すビットを決める
        - BIP-9では閾値は固定だったが、最近は開発者で決めるなど曖昧なところがある
    - 投票は生成したブロックデータに載せる
        - ブロックヘッダの `version` にビットを立てると投票したことになる
    - 期間内のブロックが閾値以上投票すると、しばらくして自動で承認される
        - 元は1年だったが、これも自由に決めたそうだ
- 投票は内容を決めるのが開発者、実施するのはマイナー
    - ハッシュパワーが強いマイナーが投票でも権利を持ちやすいことになる
    - 95%とかなってくるとほとんどのマイナーが認めない限り難しいだろう
    - 


## segwit と taproot

それぞれ softfork 提案でもめた。

https://chatgpt.com/share/6854e758-4428-8001-b2ab-19431edc306f

segwit のときは、BIP9 シグナリングでやっていたが数年かかっても広まらなかった。
そこで、UASF(User Activated Soft Fork) という swegwit を強制的に有効にする提案をした。
「2017年8月1日以降、segwit 未対応のブロックを拒否する」という恐ろしい機能である。
結果として、それが発動される2017年7月に segwit は有効になった。UASF が圧力になったと言われている。

segwit が進まなかった理由として挙げられるのが、政治的な理由である。

- segwit によって ASICBoost と呼ばれる不正ではないが仕様上の不備を突いた技が塞がれるのを嫌がった
- ブロックサイズ拡大派が、segwit を認めるからブロックサイズ拡大も認めろ、みたいなことをやってた

taproot のときはその反省を元に、BIP9 ではなく BIP8 の一種である "Speedy Trial" という方式を使った。

### segwitのとき

- learn me a bitcoin
- Grok

私は知らなかったのだが、BIP-144で segwit対応ノードから非対応ノードに segwitトランザクションを展開する際には witness 関係の部分を取り除いて展開するというルールになっていたそうだ。
marker, flag の領域を vin_count として読み込むので無視される、と思っていたのだが、取り除くと scriptSig が空なので ANYONE CAN PAY という扱いだったらしい。