BitcoinのOP_CHECKSIGFROMSTACK

bips/bip-0348.md at master · bitcoin/bips
ChatGPT
Grok

スタックにあるデータと公開鍵を使ってスタック上にある署名を検証する。
(従来からある `OP_CHECKSIG` などは処理しているトランザクションに対する署名検証しかできない)
`OP_CHECKSIGFROMSTACKVERIFY` もある。

```
OP_CSFS
   <sig>
   <message>
   <pubkey>
   OP_CHECKSIGFROMSTACK
```

オフチェーンのデータやメッセージに対しての署名検証ができる。
トランザクションとは関係なく署名チェックする処理を付け加えることができる。

LN の revoked transaction close に対するペナルティをなくすことができる(そもそも展開できないようにする)らしいが、よくわからんかった。LN のしくみもある程度変更することで実現できるらしい。
そう Grok はいうのだが、ChatGPT は特にそういうことは告げなかった。
HTLC ではなく PTLC にできたりするのだとか。