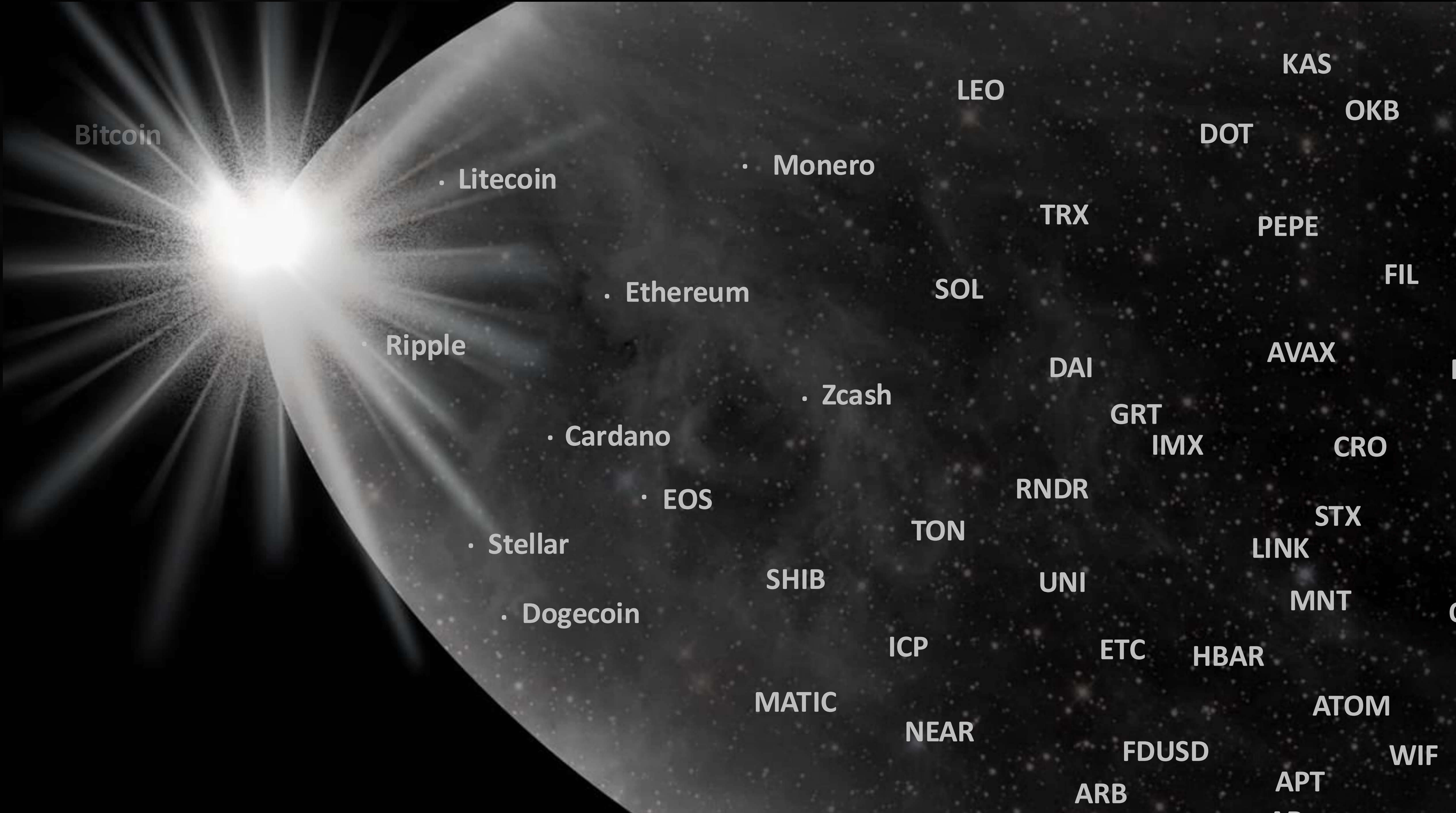
Bringing DeFi to Bitcoin

Dr. Owen Vaughan

Founder & CEO, Bitroots



Bitcoin

- Litecoin
- Monero
- Ethereum
- Ripple
- Zcash
- Cardano
- EOS
- Stellar
- Dogecoin

LEO

KAS

OKB

DOT

TRX

PEPE

FIL

SOL

AVAX

DAI

GRT

IMX

CRO

RNDR

STX

TON

LINK

SHIB

UNI

MNT

ICP

ETC

HBAR

MATIC

ATOM

NEAR

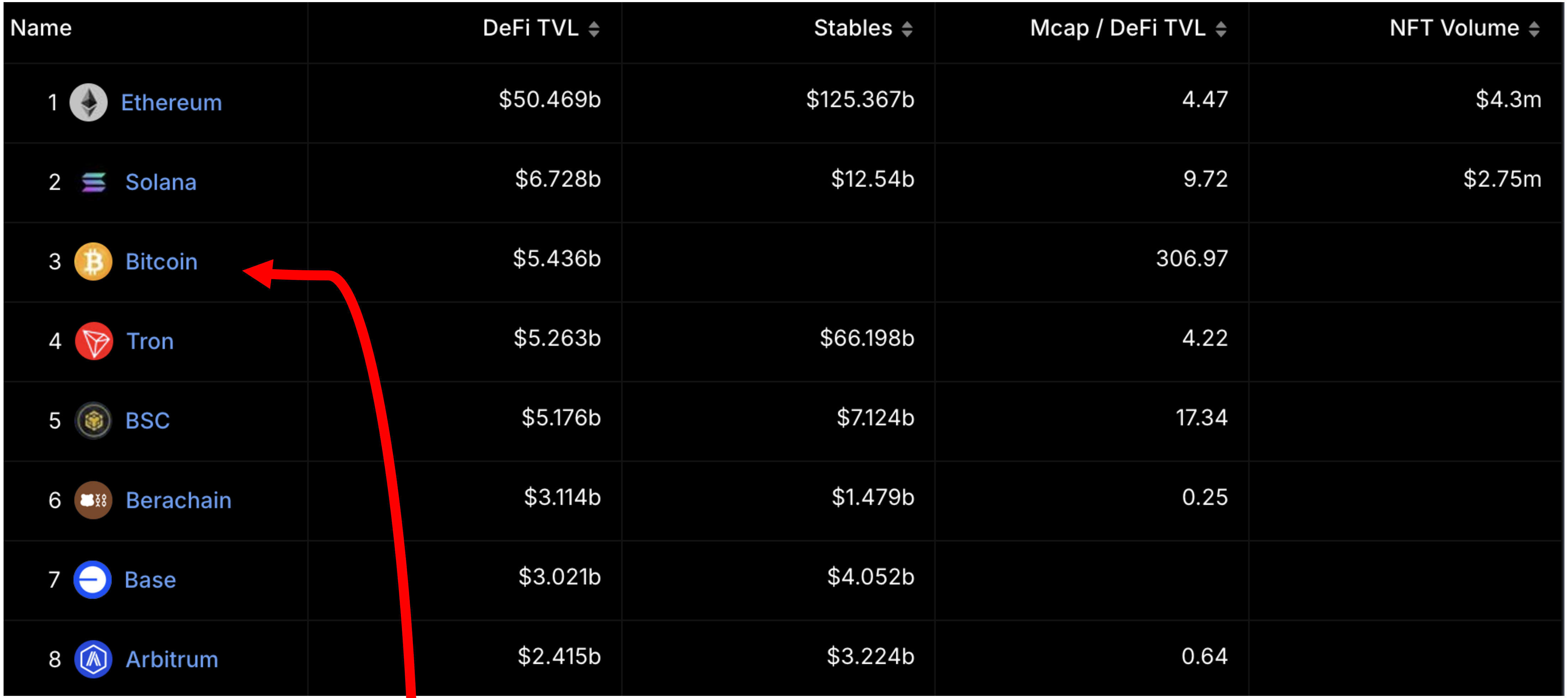
FDUSD

WIF

APT

ARB

DeFi platform ranking (TVL)

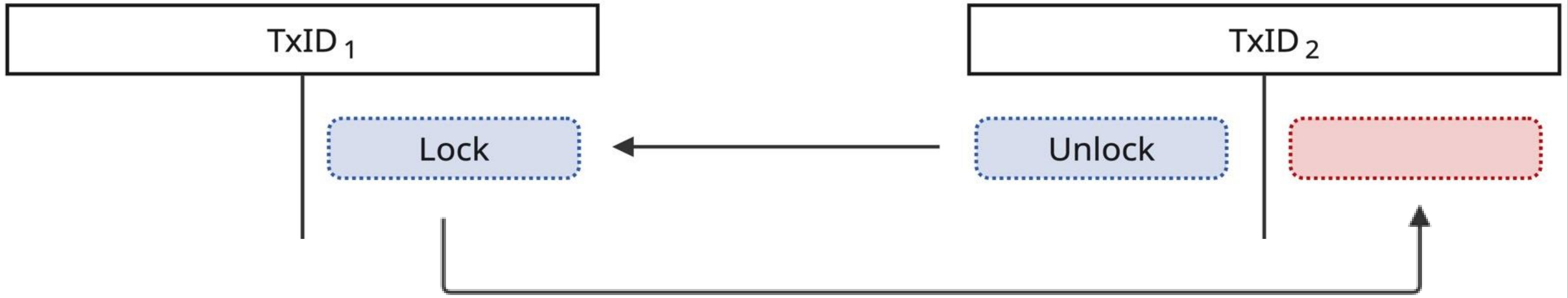


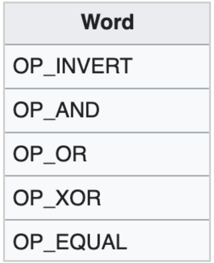
Name	DeFi TVL	Stables	Mcap / DeFi TVL	NFT Volume
1 Ethereum	$50.469b	$125.367b	4.47	$4.3m
2 Solana	$6.728b	$12.54b	9.72	$2.75m
3 Bitcoin	$5.436b		306.97	
4 Tron	$5.263b	$66.198b	4.22	
5 BSC	$5.176b	$7.124b	17.34	
6 Berachain	$3.114b	$1.479b	0.25	
7 Base	$3.021b	$4.052b		
8 Arbitrum	$2.415b	$3.224b	0.64	

Last year

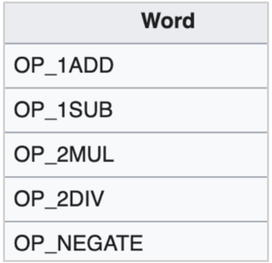
Source: DeFiLlama.com

Bitcoin opcodes

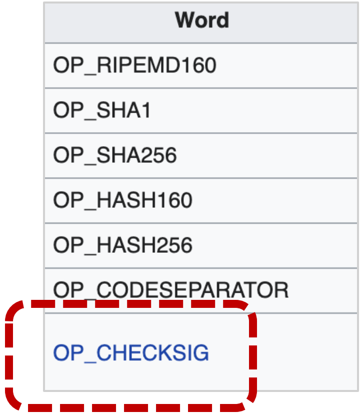




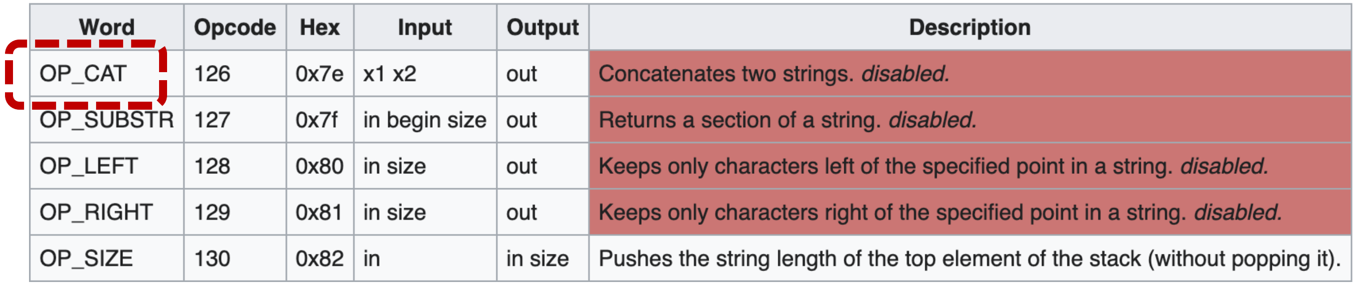
Word
OP_INVERT
OP_AND
OP_OR
OP_XOR
OP_EQUAL



Word
OP_1ADD
OP_1SUB
OP_2MUL
OP_2DIV
OP_NEGATE

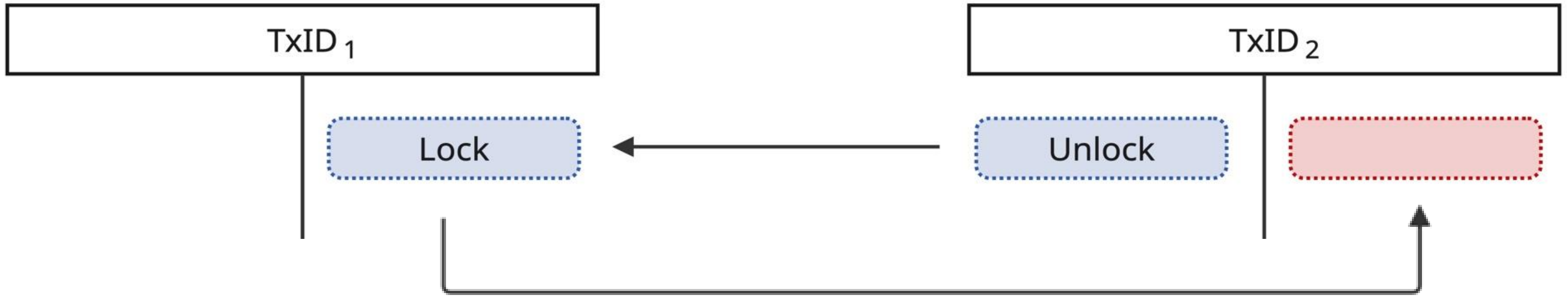


Word
OP_RIPEMD160
OP_SHA1
OP_SHA256
OP_HASH160
OP_HASH256
OP_CODESEPARATOR
OP_CHECKSIG



Word	Opcode	Hex	Input	Output	Description
OP_CAT	126	0x7e	x1 x2	out	Concatenates two strings. *disabled.*
OP_SUBSTR	127	0x7f	in begin size	out	Returns a section of a string. *disabled.*
OP_LEFT	128	0x80	in size	out	Keeps only characters left of the specified point in a string. *disabled.*
OP_RIGHT	129	0x81	in size	out	Keeps only characters right of the specified point in a string. *disabled.*
OP_SIZE	130	0x82	in	in size	Pushes the string length of the top element of the stack (without popping it).

Covenants



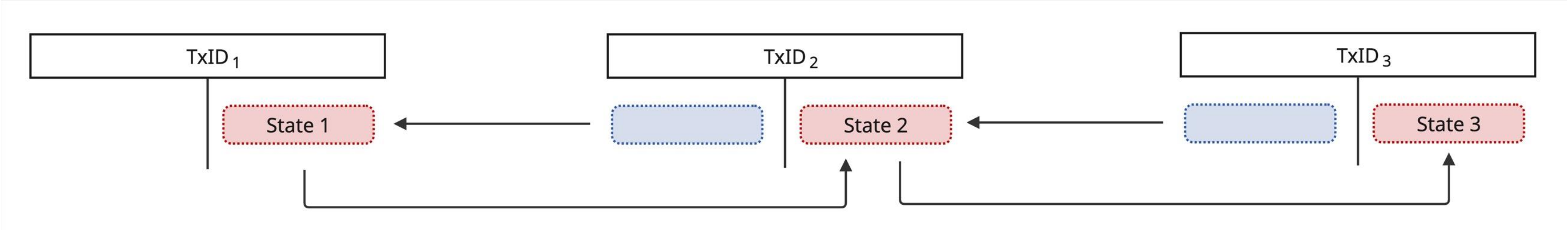
Inspect spending transaction by constructing a dummy signature in script!

$$s = k + xe \qquad e = H(Rx \,||\, Px \,||\, transaction)$$

Simply with $k = x = 1$

$$s = 1 + e$$

Smart Contracts



1. Unique ID can be propagated
2. Enables tokens (CAT-20)
3. Using recursive ZKPs to add sophisticated logic to

ZKPs

STARKWARE

STARK
11 Taproot transactions, 4MB, OP_CAT, Signet.

nChain

Groth16
1 transaction, 500KB, OP_CAT + more, BSV Mainnet.

bitcoinOS

STARK
Merkle-mesh on-chain structure. Specific DeFi. 100KB. Testnet.

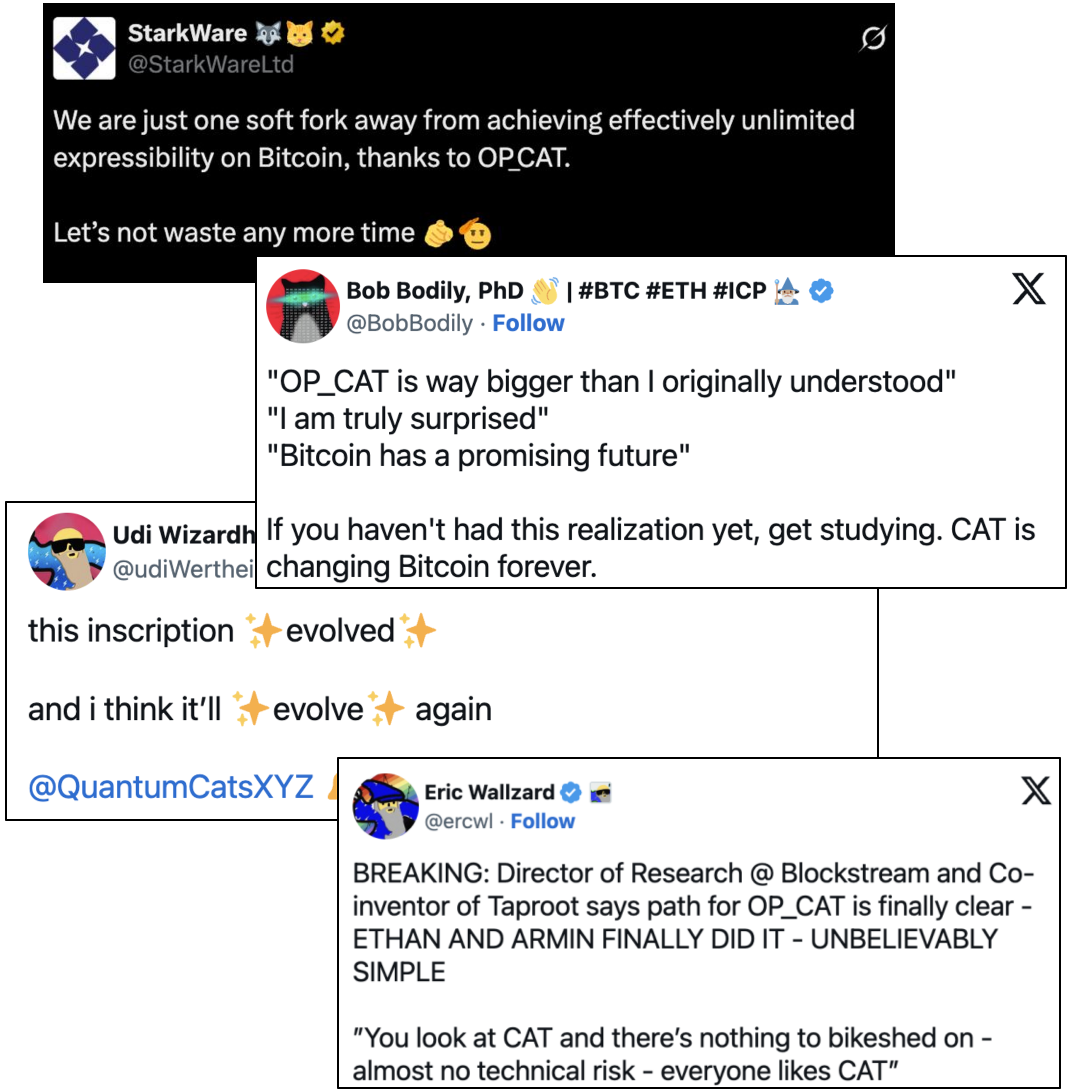
BitVMX

STARK + Groth16
Off-chain with on-chain fraud proofs. General VM. GBs memory. Testnet.

Reference: Wei Zhang nChain blog

Where are we now

Bitroots



StarkWare 🐺🐱
@StarkWareLtd

We are just one soft fork away from achieving effectively unlimited expressibility on Bitcoin, thanks to OP_CAT.

Let's not waste any more time 🫵🫡

Bob Bodily, PhD 👏 | #BTC #ETH #ICP 🧙
@BobBodily · Follow

"OP_CAT is way bigger than I originally understood"
"I am truly surprised"
"Bitcoin has a promising future"

If you haven't had this realization yet, get studying. CAT is changing Bitcoin forever.

Udi Wizardh
@udiWerthei

this inscription ✨evolved✨

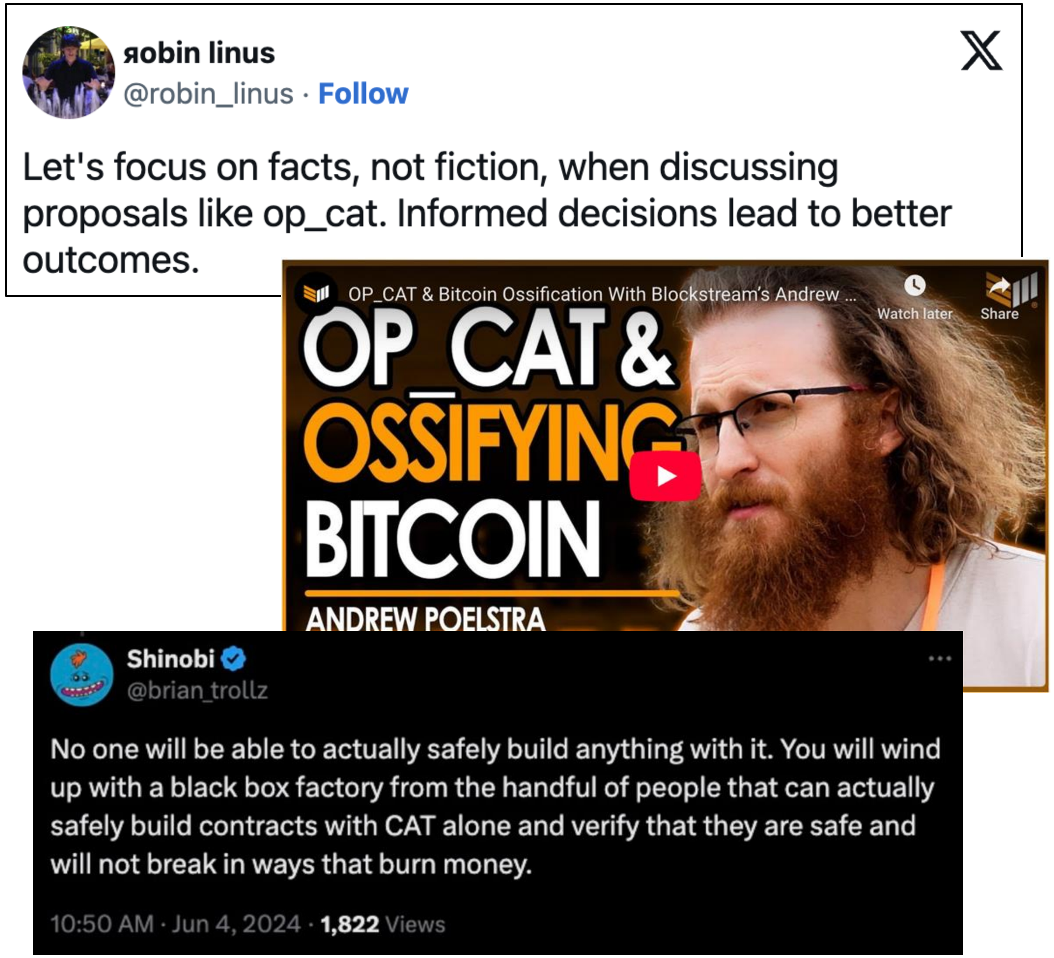
and i think it'll ✨evolve✨ again

@QuantumCatsXYZ

Eric Wallzard
@ercwl · Follow

BREAKING: Director of Research @ Blockstream and Co-inventor of Taproot says path for OP_CAT is finally clear - ETHAN AND ARMIN FINALLY DID IT - UNBELIEVABLY SIMPLE

"You look at CAT and there's nothing to bikeshed on - almost no technical risk - everyone likes CAT"



яobin linus
@robin_linus · Follow

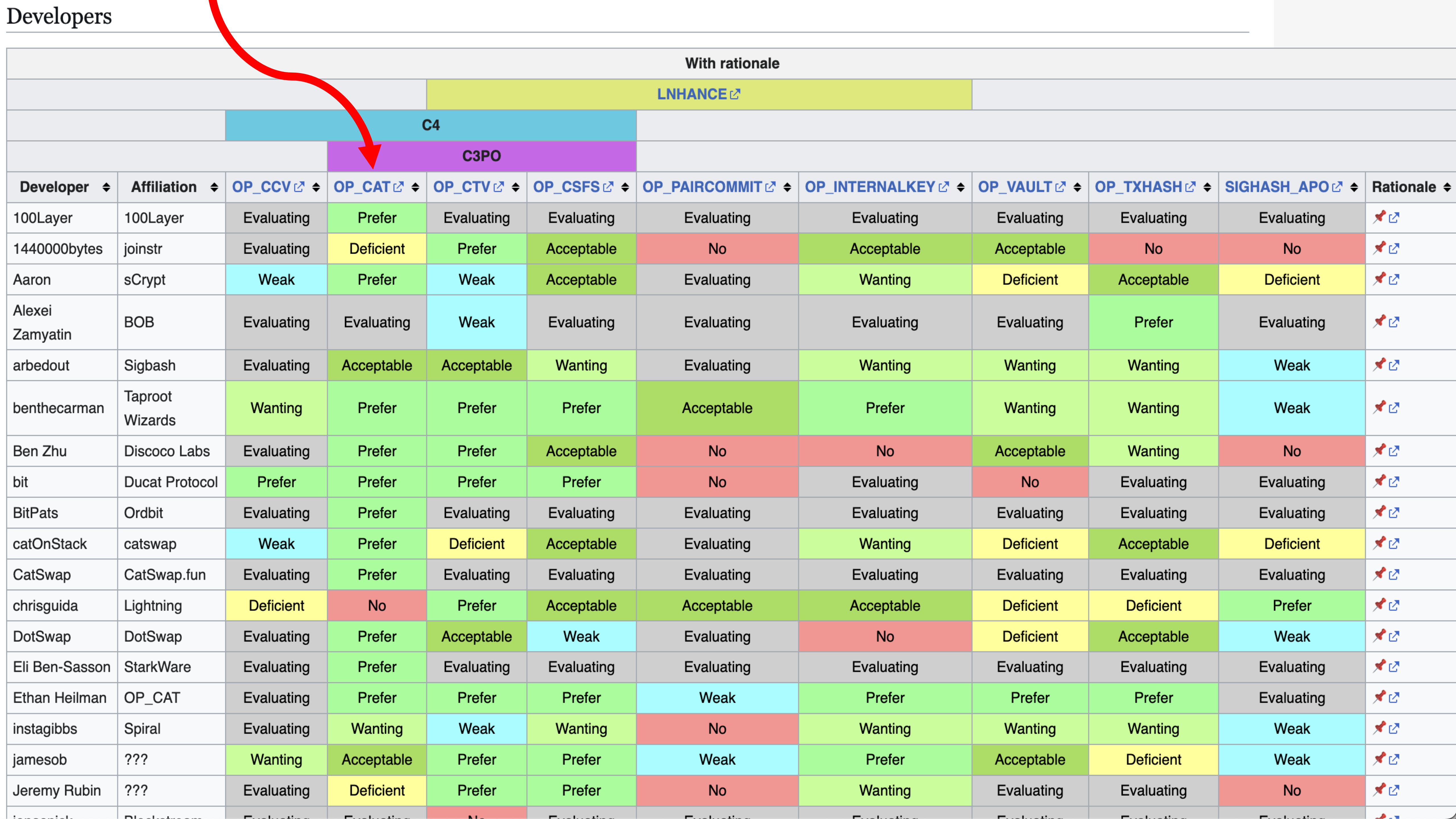
Let's focus on facts, not fiction, when discussing proposals like op_cat. Informed decisions lead to better outcomes.

OP_CAT & Bitcoin Ossification With Blockstream's Andrew ...

Shinobi
@brian_trollz

No one will be able to actually safely build anything with it. You will wind up with a black box factory from the handful of people that can actually safely build contracts with CAT alone and verify that they are safe and will not break in ways that burn money.

10:50 AM · Jun 4, 2024 · **1,822** Views



Developers

With rationale											
				LNHANCE							
		C4									
			C3PO								
Developer	Affiliation	OP_CCV	OP_CAT	OP_CTV	OP_CSFS	OP_PAIRCOMMIT	OP_INTERNALKEY	OP_VAULT	OP_TXHASH	SIGHASH_APO	Rationale
100Layer	100Layer	Evaluating	Prefer	Evaluating	Evaluating	Evaluating	Evaluating	Evaluating	Evaluating	Evaluating	📌 ↗
1440000bytes	joinstr	Evaluating	Deficient	Prefer	Acceptable	No	Acceptable	Acceptable	No	No	📌 ↗
Aaron	sCrypt	Weak	Prefer	Weak	Acceptable	Evaluating	Wanting	Deficient	Acceptable	Deficient	📌 ↗
Alexei Zamyatin	BOB	Evaluating	Evaluating	Weak	Evaluating	Evaluating	Evaluating	Evaluating	Prefer	Evaluating	📌 ↗
arbedout	Sigbash	Evaluating	Acceptable	Acceptable	Wanting	Evaluating	Wanting	Wanting	Wanting	Weak	📌 ↗
benthecarman	Taproot Wizards	Wanting	Prefer	Prefer	Prefer	Acceptable	Prefer	Wanting	Wanting	Weak	📌 ↗
Ben Zhu	Discoco Labs	Evaluating	Prefer	Prefer	Acceptable	No	No	Acceptable	Wanting	No	📌 ↗
bit	Ducat Protocol	Prefer	Prefer	Prefer	Prefer	No	Evaluating	No	Evaluating	Evaluating	📌 ↗
BitPats	Ordbit	Evaluating	Prefer	Evaluating	Evaluating	Evaluating	Evaluating	Evaluating	Evaluating	Evaluating	📌 ↗
catOnStack	catswap	Weak	Prefer	Deficient	Acceptable	Evaluating	Wanting	Deficient	Acceptable	Deficient	📌 ↗
CatSwap	CatSwap.fun	Evaluating	Prefer	Evaluating	Evaluating	Evaluating	Evaluating	Evaluating	Evaluating	Evaluating	📌 ↗
chrisguida	Lightning	Deficient	No	Prefer	Acceptable	Acceptable	Acceptable	Deficient	Deficient	Prefer	📌 ↗
DotSwap	DotSwap	Evaluating	Prefer	Acceptable	Weak	Evaluating	No	Deficient	Acceptable	Weak	📌 ↗
Eli Ben-Sasson	StarkWare	Evaluating	Prefer	Evaluating	Evaluating	Evaluating	Evaluating	Evaluating	Evaluating	Evaluating	📌 ↗
Ethan Heilman	OP_CAT	Evaluating	Prefer	Prefer	Prefer	Weak	Prefer	Prefer	Prefer	Evaluating	📌 ↗
instagibbs	Spiral	Evaluating	Wanting	Weak	Wanting	No	Wanting	Wanting	Wanting	Weak	📌 ↗
jamesob	???	Wanting	Acceptable	Prefer	Prefer	Weak	Prefer	Acceptable	Deficient	Weak	📌 ↗
Jeremy Rubin	???	Evaluating	Deficient	Prefer	Prefer	No	Wanting	Evaluating	Evaluating	No	📌 ↗
jonasnick	Blockstream	Evaluating	Evaluating	No	Evaluating	Evaluating	Evaluating	Evaluating	Evaluating	Evaluating	📌 ↗

Recap

OP_CAT > Covenants > Smart Contracts > ZKPs > DeFi

Thank you :)

owen@bitroots.io