
digital
currency
initiative

Vision

Create a future in which moving value across the Internet is as intuitive and efficient as moving information, to increase wellbeing for all people.

digital currency initiative

Layer 2

Currently used as an umbrella term for all operations that are performed “off chain”, and use blockchains to settle transactions.

digital currency initiative

Scale

Every node runs every step of every smart contract. This is unnecessary. Why not use verifiable computation techniques + on chain anchoring?

digital currency initiative

Smart contracts

- Example: payment conditional on external data
- In this example, Alice and Bob bet on tomorrow's weather. If it rains, Alice gets 1 coin. If it's sunny, Bob gets 1 coin
- Issue: The bitcoin blockchain unaware of the weather

digital currency initiative

Oracles

- For external state, need way to get it, usually called an "oracle“
- Oracles should not be able to **collude**, or **equivocate**
- Use cryptography to implement one such oracle – that’s what we’ve done

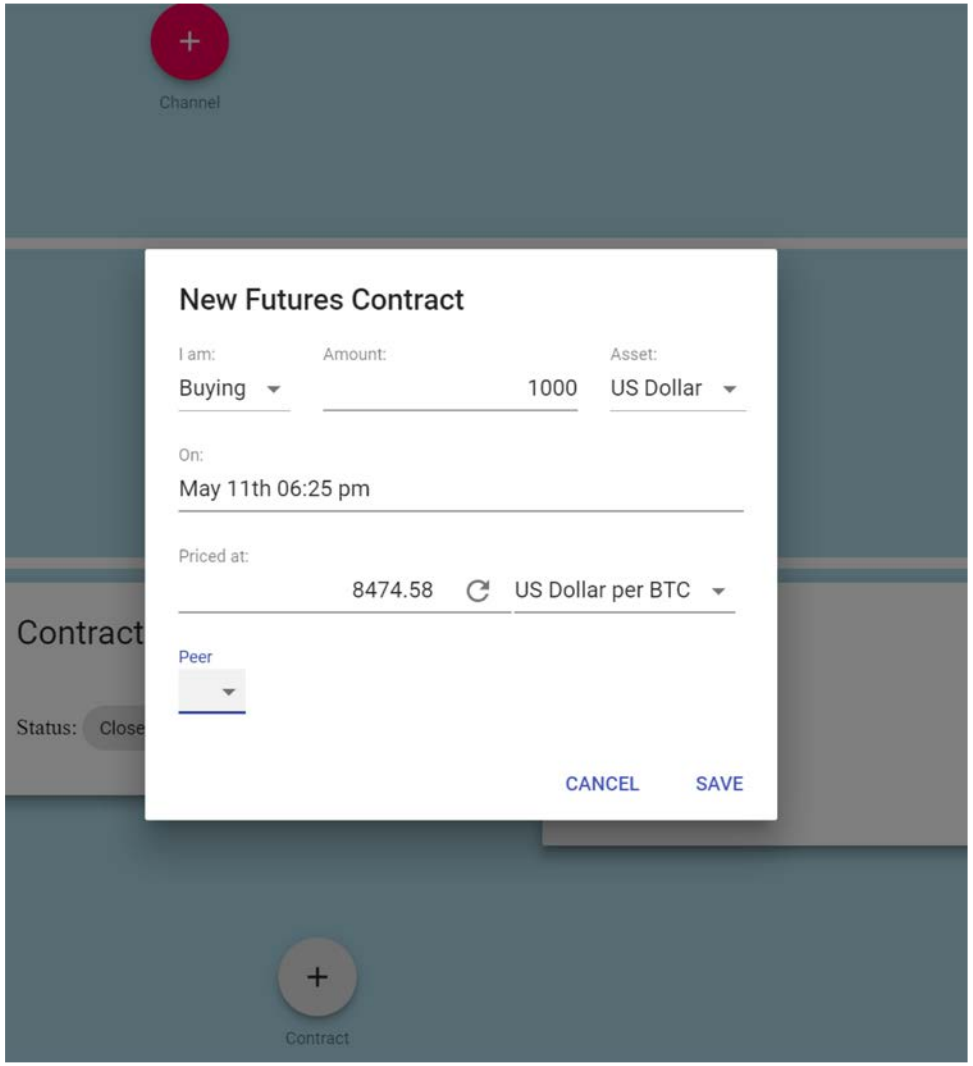
digital currency initiative

One example

- Bitcoin settled dollar futures
- Allows Alice to move the risk to Bob
- One way to address volatility for Alice

digital currency initiative

One example (cont.)



digital currency initiative

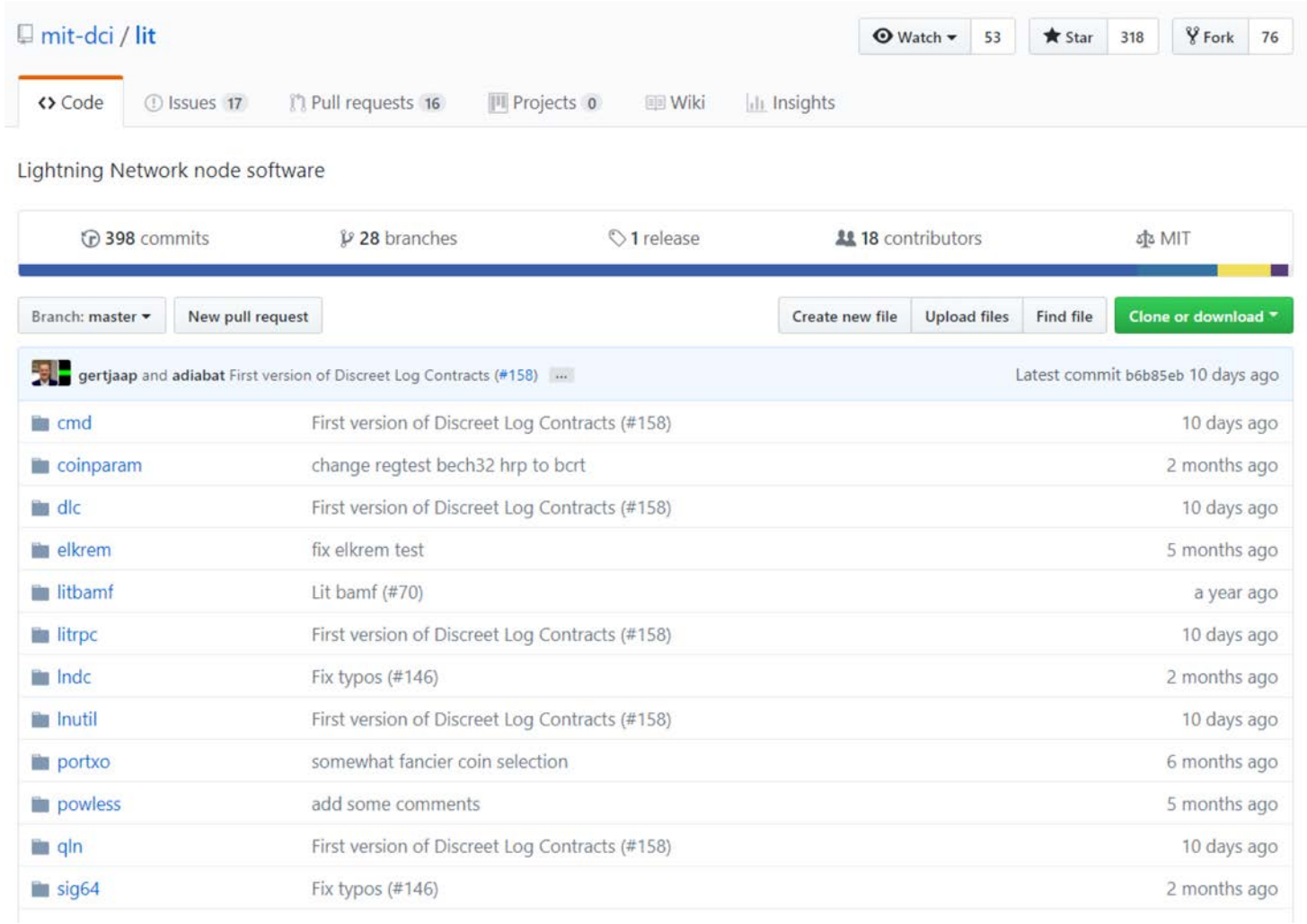
Other use cases?

- General: conditional payments based on any number or elements from predetermined set

- Weather?
- Stocks?
- Commodities?
- Sports?
- Insurance?

digital currency initiative

Check out our GitHub



mit-dci / lit

Watch 53 | Star 318 | Fork 76

Code | Issues 17 | Pull requests 16 | Projects 0 | Wiki | Insights

Lightning Network node software

398 commits | 28 branches | 1 release | 18 contributors | MIT

Branch: master | New pull request | Create new file | Upload files | Find file | Clone or download

gertjaap and adiabat First version of Discreet Log Contracts (#158) ... Latest commit b6b85eb 10 days ago

cmd	First version of Discreet Log Contracts (#158)	10 days ago
coinparam	change regtest bech32 hrp to bcrt	2 months ago
dlc	First version of Discreet Log Contracts (#158)	10 days ago
elkrem	fix elkrem test	5 months ago
litbamf	Lit bamf (#70)	a year ago
litrpc	First version of Discreet Log Contracts (#158)	10 days ago
lndc	Fix typos (#146)	2 months ago
lnutil	First version of Discreet Log Contracts (#158)	10 days ago
portxo	somewhat fancier coin selection	6 months ago
powless	add some comments	5 months ago
qln	First version of Discreet Log Contracts (#158)	10 days ago
sig64	Fix typos (#146)	2 months ago

digital currency initiative

Alin S. Dragos

MIT Media Lab

dci.mit.edu

github.com/mit-dci