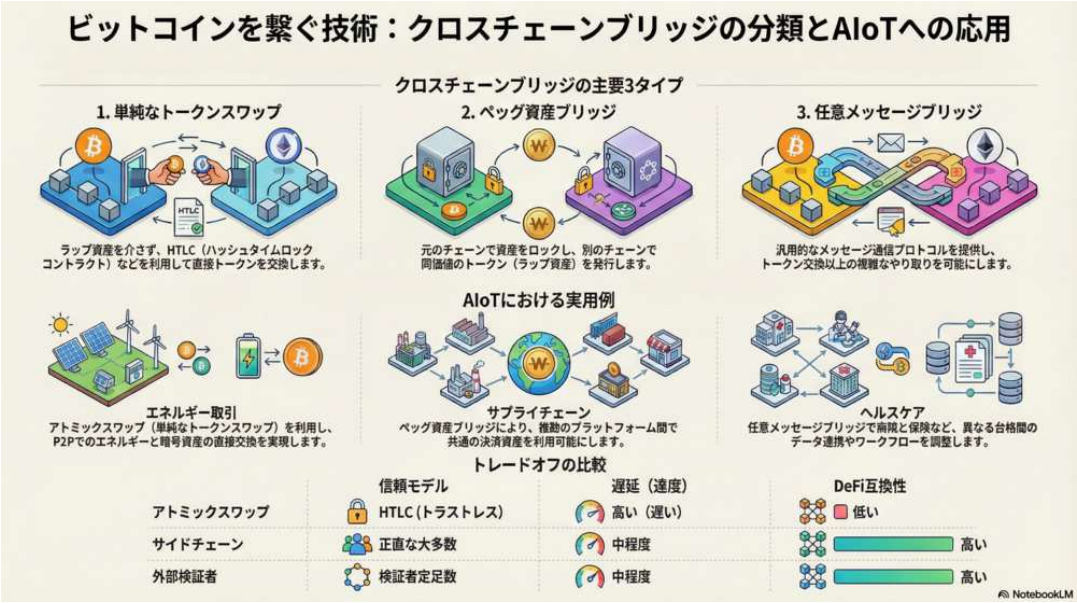
LNをDEXで使うことの考察

Bitcoinはスマートコントラクト機能が少なく他チェーンとの交流が難しい。
DEXで使うにはブリッジを使って他のEVMなどで扱えるようにする必要がある。
しかしブリッジはBitcoinの承認期間が長いので atomic性はともかく即時性はない。
ではLNだとどうだ？というのが今回の話である。

Bitcoinブリッジ

Bitcoinのブリッジ

こちらは、Bitcoinブリッジの考察を行った論文を元にした資料だ。
https://notebooklm.google.com/notebook/51b28ae9-4293-4f03-aa1e-5e68164995f0



ブリッジなのか売却なのか

あまり考えても仕方ないが、運営側のBitcoinアドレスに送金してトークンを得るという行為はBitcoinを売却してトークンを購入したと見なすこともできる。
「ブリッジ」と言い張るなら、運営側のBitcoinアドレスへの送金は「相手の資金を担保のためロック」ということになる。そう主張するために Peg-In / Peg-Out という用語を使い、Peg-Inで送金された UTXO は Peg-Out するまで維持しないといけないかもしれない。Bitlayerはそういう運用になっている。

Bitcoinブリッジは即時性がない

上の3方式のうち、おそらくよく使われるブリッジはサイドチェーン方式だろう。Peg-In で

Bitcoinアドレスに送金して reorg されないところまで待つことが多く、その時間がかかる。そうなると、DEX で注文してその時の金額で相手トークンと交換とするには時差があるので秒単位で交換レートが変わるような世界には向かない気がする。
あらかじめ WBTC などのトークンにしておいて、それを DEXで使うのであれば大丈夫かもしれないが、それがどこまで「我々はユーザの資金を預かっていない」と主張できるのか分からない。
ともかく完全に Decentralized なブリッジも現状では存在しないので、諦める範囲と法律との落とし所になるだろう。

LNはどうだろうか

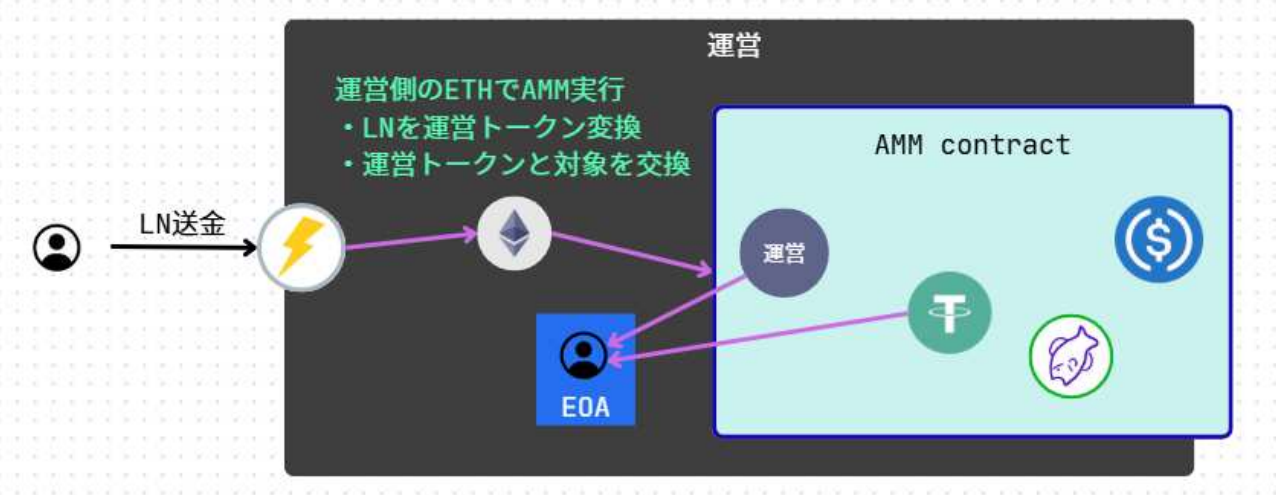
Bitcoin で即時性があるといえば Lightning Network である。
なので LNを使った DEXを考えるところが今まであってもよさそうだが、なさそうだ。
何か問題があるのだろう。

AMMとのやりとり

まず、AMMのやり方と違うので直接のやりとりが難しいのだと思う。
AMMを実際に動かしたことはないのだが、スマコンの流動性プールがあってマッチングさせて条件があえば交換、という感じだと思われる。流動性プールに直接アクセスできないので誰かが間に入ることでできるか？

ユーザーは交換が成功したら自分の EOA に交換後のトークンが入っているだろう。しかし初回は何もないかもしれない。ETHも持っていないのでスマートコントラクトの呼び出しもできないかもしれない。そうなるとユーザー自身はスマコンを動かすことができないので、AMMの交換元として運営が内部で運用するトークンを使い、スマコンを動かす手数料をユーザから差し引けばよいだろう。

ユーザーには運営ノードにLN送金してもらい、それを受け取ったら運営トークンとユーザーが交換したいトークンを交換し、ユーザーのEVMアカウントなどに転送する。
下で説明する「クロスチェーンスワップ(LNをDEXで使うことの考察#74b302)」と似たような流れになる。”共通して使用できるトークン" として運営トークンのように同じVMで使用できるトークンを用意して、あとはAMMに任せると他と同じ流れになる。



LN送金だと送金元が分からない

LN送金された場合、受け取った方は誰が送ってきたのか分からない。

これは preimage -- payment_hash の管理をすれば紐付けることはできるので、それで区別することはできるか。

LN invoice は金額ありにした方がチェックもできて安心だろう。その際にユーザのEOAと紐付ける。

直接のチャネルに限定してもよいかもしれないが、受け取った方は何ホップして届いたかがわからないので止めた方がよいか。

チャネル管理が大変

運営がLNノードを運用することになるが、チャネル管理の負担はかなり大きい。

LSP になる必要はないのだが、ユーザーのノードと直接チャネルを作った方が中継ノードによって不安定さを減らせるだろう。そうなるとユーザーの数だけチャネルを持つことになる。1ノードで1000チャネルくらい作ることができるのか？ それを何ノード用意すれば良いのか？

チャネル作成にお金がかかる

そのチャネル運用資金をどこから出すか。ユーザに作ってもらう方式にすれば初期投資は不要になる。それだとユーザーが増えないので運営側から作りたいとなると、ユーザーから BTC や fiat をもらってチャネルを作るしくみもいる。

流動性プールとは関係ないのでその分を運営資金から出さねばなるまい。せっかく AMM でユーザー同士で交換することで少ない元手で DEX を作ろうとしているのに準備金がかなり必要となるだろう。

リバランスがとても大変

INとOUTのどちらが多いか分からないが、いずれは片方に偏るだろう。そのときどうするか。

ユーザの手持ちLNがなくなったらユーザが自分で残高を調整するのを期待するのは難しいだろ

う。何らかのリバランス処理が必要になるが、それが非常に大変だ。
それは自分側のキャパシティも同様である。相手チャネルと資金移動するのも大変そうだが、それでも足りなかったら新しくチャネルを作ることになる。その費用も時間も管理も大変だ。

独自チャネル方式でなにかできるかも？

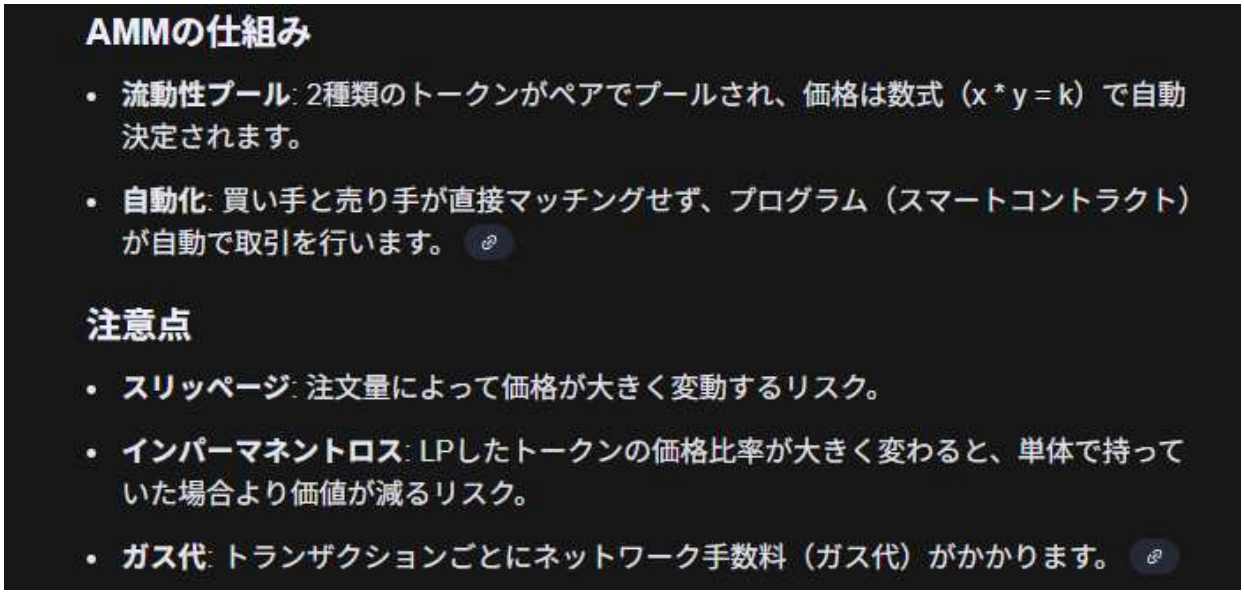
直接チャネルを作るのであれば、Taproot Assets や RGB のように独自の仕様を持ち込むことはできるだろう。ある意味では Muun Walletもそうか。ウォレットアプリを供給すれば独自方式にすることは難しくない。それを使って
ただ、純粋なLNから遠ざかると分散していると見なされなくなったりしそうな気もする。

資金のロックではなく支払いでは？

LNは決済手段になるので「支払い」になってしまうのではなかろうか。そうするとDEX と言えなくなる？ しかしクロスチェーンスワップで運営の持つトークンと交換を何度かやっても DEX になるなら、このくらいならよいのか？
そんなことを言い出すと普通に流動性プールを使うのだって別のトークンにしているんだから今さらなのか？ だんだんわからなくなってきた。

DEXの世界





流動性プールコントラクト

流動性プール＝AMMのスマコンある。スマコンのアドレスがそれぞれのトークンを保有

Uniswap V4

Uniswap V3

例えば Uniswap V4のPoolManagerには 36,407 ETH もの残高がある。
そのUSDT保有量は 102,695,839,704 USDT、Wrapped BTCは 124,963 WBTC、などを見ることができる。

ERC-20の仕組みに、特定の相手に指定した金額以内の自分のウォレット資金を動かす権限を与える(approval)というものがある。スワップするときはユーザーは `approve()` でAMMコントラクトに自分のウォレットを操作する権限を与えて AMMのコントラクトに任せることになる(API)。金額上限を付けないようにもできる。
推測だが、それを使って単にユーザの交換元トークンをAMMコントラクトに送金し、AMMコントラクトの交換先トークンをユーザに送金するだけだったのかもしれない。

以前の Uniswap はトークンのペアごとにスマコンをデプロイしていたようだが、最近は1つのコントラクトにまとめたそうだ。1つのコントラクトに全部のトークンが集まるのは怖いが効率は良い。

DEXをDEXのままにしたい場合(法的)

ユーザーの資金を預かると、それはもうCEXである。運用側の中央管理になる。
DEXをDEXのままにしたいなら、言い訳でも良いのでそれを回避する必要がある。

よくあるペッグ型のブリッジは、Bitcoinを運営のマルチシグアドレスに送金し、それをブリッジ先のコインにしてもらう。
ここで気になるのが、マルチシグとはいえ運営が管理するBitcoinアドレスに送金するならCEXと同じじゃないの？という点だ。AIに聞いてみると、どうもそこは業界としてはまだ「ユーザーの資金を預かる」とは見なされないらしい。秘密鍵の所有うんぬんではないという。本当かしら？

そしてその言い分が通るなら、ブリッジなど作らずにマルチシグアドレスを作ってユーザーにBitcoinを入れておいてもらい、あとは運営側が持っているコインを内部で使って「AMMで交換してます」という体裁にすれば済んでしまう。
しかしそういうDEXを見かけないというところからすると、マルチシグアドレスを使う以外にも「預かっていない」と見なす要素があると考えられる。

ChatGPTにその辺りを聞いてみると「多くの定義でDEXは『中央サーバで約定しない』ことを指す」そうだ。「運営主体が顧客資産を保管している」については引っかかっているがそれ以外が大丈夫だったからCEXじゃないよね、ということか。
実際の形態がどうあれ、法的にCEXの定義を回避することでDEXとして扱われている、それがHyperliquid。
つまり法律的にDEXをDEXのままにしたいなら、法律的にCEXの定義を回避せよ、ということになる。

DEXをDEXのままにしたい場合(技術的)

かといって法律の隅をつつくだけなのは技術屋さんとしてはあまりよろしくない。
どこまでできて、どこからは難しいというようなところを攻めていきたい。

まず、Bitcoinだけで完結させたいならネイティブな Bitcoin L2でないと無理だろう。しかしBitcoinスクリプトでできるのはアトミックスワップくらいで L2トークンを発行できるほどではない。
ブリッジを使って独自のトークンを作り、それが他のトークンとAMMで交換できるようであればできるかもしれない。つまり WBTCを一度挟む形だ。
Base のようなL2は Ethereumネイティブな L2に分類され、こういう感じで運用しているはず。

- Ethereum L1→L2：ネイティブなEVMスマコンで実現できる
- 同じVMの L2→L2：これもスマコンで実現できるだろう
- 違うVMの交換：いくつかある
  - クロスチェーンスワップ(多くのDEXアグリゲーターが採用している方式)
    - どちらのVMでも共通して使用できるトークン(USDCなど)を決める

変換元でそのトークンをロック

ブリッジでメッセージ送信

変換先でトークン(wrapped USDCなど)をmint

そのトークンで希望するトークンと交換

クロスチェーンAMM

複数のチェーンにまたがる共有の流動性プールを持っている

またがるといってもそれぞれのチェーンに流動性プールがあり、それをメッセージングで見せかけているだけ。

これでも "DEX" を名乗ることはできるようだ。