At some point I over generalized atomic swaps for Crosschain communication. So just skip to the bottom. ctrl+f “#latest

”

I’m doing some research into scaling and I want to be sure I am understanding this 100% clear.

I’ve asked around but I still don’t believe it.

So I can atomic swap an asset to a sidechain in a fully decentralized manner. Is that really true? Are there any attacks that can be performed to interrupt the atomic swap?

What does the receiving chain look like? Is the code different than a typical blockchain? Should I just copy a p.o.s. chain to start?

Other than $51% attacks, are there any other weaknesses to p.o.s.?

----------from reddit (u/646463)----------

Other than $51% attacks, are there any other weaknesses to p.o.s.?

No trustless light clients. Which, you know, might be useful for a dex.

You can DoS atomic swaps in some cases. Solved with timeouts / locktime (so they remain atomic). Not a great soln. You can DoS if you can prevent tx confirmation (for a specific tx).

The atomic swap basically just gives someone a pegged token. Right?

No, tho you could build a pegged token service on atomic swaps. They work for arbitrary tokens. (eg BTC <-> LTC)

---------- my response ----------

Is a trustless light client impossible?

So if I’m understanding you correctly, I can create a token on the mainchain/parentchain, and have that asset transferred to a sidechain. This is possible. Wow. It would seem that the sidechain would have to have a peg though. You say no, can you help me better understand? If someone atomic swaps an asset to another chain, what are they getting? or is that the situation in which you get a peg token?

I just realized I must have confused atomic swaps with another technology. I was caught up in the whole idea of “transfer” between different chains. Maybe it’s still relevant. But what I’m trying to do is take a token from mainchain and transfer it to a sidechain. Which I believe mainchain would have to “lock” the asset, just as the sidechain created a peg version.

I just realized something.

I don’t need atomic swaps at all. All I need is a contract dedicated to pegging on each chain and the ability for each chain to read each other.

Ethereum lacks the capabilities to read from a sidechain at the moment, but I can customize the sidechain to read from Ethereum.

For this to work mainnet is going to have to implement a protocol that can communicate with a sidechain.

Here is a proposal for crosschain communication.

arXiv.org

Atomic Crosschain Transactions for Ethereum Private Sidechains

Public blockchains such as Ethereum and Bitcoin do not give enterprises the privacy they need for many of their business processes. Consequently consortiums are exploring private blockchains to keep their membership and transactions private. Ethereum...

It also seems like plasma can help integrate this solution.Which someone brought up earlier but I wasn’t very knowledgeable about it. It would require back and forth communication between nested plasma chains. Which I believe is possible, but I think this was brought up as a UI issue. (Not if each transaction at each layer was automated if ascending and descending the layers was necessary)

https://blockchainatberkeley.blog/plasma-isnt-dead-7d0b8c16ad2e

Ultimately, all I need is for one blockchain to be able to read another.

Testnet is up for the smart contract that creates & maintains the distributed token.

Okay so basically. The only thing left for me to do is clone a plasma chain and make its proof of stake backed on a token created from parent chain.

This sounds much more feasible than what I first invisioned

[

Screenshot_20190603-162630

720×1440 81.1 KB

](https://ethresear.ch/uploads/default/original/2X/f/f7b6a62c75e4c8014967d8a553e7aa22a07a895c.png)

This seems odd though. Why would a plasma chain not have dApp capabilities? Something must be wrong.

Are the only complications moving up and down chains?

Well. this is what if found out most recently. So apparently this guy wasn't lying. apparently it's hard to do smart contracts on plasma

Well, it's as I thought… Security degredation at each layer… Yeah, that's what I've solved [

Screenshot_20190604-215337

720×1440 289 KB

](https://ethresear.ch/uploads/default/original/2X/b/b14ff98a42c974b89529d8b7dc4800e5ec0dbbca.jpeg)

[

Screenshot_20190604-220747

720×1440 210 KB

](https://ethresear.ch/uploads/default/original/2X/9/967526cf2745d988e9f14a473c246dfc8e4f7e25.png)

Dear Diary,

alright, I think I finally found what I need

docs.skale.network

SKALE Developers: SKALE Developer Documentation

Documentation for Developers, Validators, and Open Source contributors to the SKALE Network

I don't need plasma

Nevermind

I am looking for a sidechain repo to fork. I searched on GitHub but I don't think I'm looking at what I need. These things seem to be super rare

latest

so validators. that's the chain to chain communication. a bit of a manual process.

ok. that detail I missed.

I wonder if chain identity can be achieved in a similar way to node identity in a network. If so, there's potential for Interoperability at the protocol level