NEXUS
Developers Update JAN-25-25

This update outlines the following key areas of development for Nexus:

Current Progress:

GitHub Projects Organization:

- Creation of three projects: desktop wallet, mobile wallet, and LLL-TAO.
- Improved tracking of issues, enhancements, bugs, and project milestones.

Indexing System Revamp

- Breaking database instances into a sessions database and a global index database.
- Bug fixes completed, with critical issues resolved for exchanges.
- Trade functionality should be back online after one more update.

Assistance with XeggeX

- Supporting Geraldo in fixing implementation issues and initial logic.

Hard Fork Development

- Implementing version checks and testing on test and private networks.
- Solidifying reorganization code through local tests.
- Active work on the following branches:

    1. merging-indexing: Indexing system work.
    2. merging-6.0: Hard fork development.

Ledger Level Virtual Machine

- Key feature for enhanced security and access control patterns.
- Allows creation of multiple credentials with restricted access to specific actions (e.g., staking, debits, credits).
- Supports programmable access control, AND/OR logic, time limits, and multi-signature authentication.
- Enables functionalities like:

    1. Automatically executing wills with time-based access control.

2. Granular authentication for signature chains.

3. 2-factor authentication via mobile wallet or app integration.

Progress on Hard Fork Features

- Chain state parameters: In progress.

- Asset management: Not done.

- Difficulty adjustments: Nearly complete.

- Aggregate sig chains: Not done.

- Truncating the legacy chain: Not done.

- Next Hash authentication scripts: In progress.

Index System Revamp Progress

- Aiming for completion by the end of the weekend.

- Approximately 2,000-3,000 lines of code, 50-60% completed.

Ledger Level Virtual Machine Timeline

- Targeting completion within a week.

- Hard fork expected within 2-4 weeks, followed by a 2-week activation period.

Legacy Coin Migration

- Reminder to move coins from the legacy chain.

- Approximately 15,300,000 coins burned/lost on the legacy chain.

Unburned Coin Distribution

- Finalizing allocations for unburned coins.

- Planned on-chain vote for approval.

- Proposed distribution:

    1. 6,000,000 coins to the team for bounties.

    2. 10,000,000 coins to the satellite war chest.

Future Plans:

- Updates on progress in the coming weeks.

- On-chain vote to ratify unburned coin allocations.

GitHub Projects

Hey, guys. This update this week is gonna be short. What I've been working on primarily is working on an indexing system revamping. So I've been essentially breaking the database instances into a sessions database and then a regular global's index database. I've been doing some bug fixes.

I got pretty much all of the the critical bugs resolved for the exchanges. Trade over should be back online. We're having, I think, one more update, and then everything should be good. A lot of it's been also helping XeggeX with Geraldo. They're still fixing some of their implementation issues as far as some of their initial logic.

And then I've also been starting on the hard fork. So some of that is essentially putting in different version checks, doing some tests on the test net, private net. I've been getting some of the reorganization code really solid, so doing a lot of local tests with that. And really deciding how everything's gonna be broken up. If you wanna monitor the branches, merging indexing is the branch in which I'm doing all of the, work on the indexing system.

Merging-6.0 is the one that I'm doing the hard fork work. And then I also started on the ledger level virtual machine. So I pushed this feature up into present time for this next hard fork because this one's gonna be a really important security measure. So what you're gonna be able to do is create access control patterns for your signature chain. So I've mentioned this before, but just to give you a quick rundown of how it works.

You'll have your master credentials, and that'll be able to execute anything in your sig chain. Right? Debits, credits, transfers, claims, all of that. But then you'll be able to create any other set of credentials. So the set of credentials, think of that as just a different password/pin combination.

And for instance, one of them you could say, I want this access credentials to only be able to stake and only be able to add stake to my trust, but not take away stake. And only be able to credit to accounts, but never be able to debit. So the result of that would be if any of those credentials get compromised. Let's say, you get a virus on your computer or malware, any of the sorts, it won't matter. Because the attacker will not actually have full access to your section.

They'll have a limited access. So when you're staking and you're running your wallet and you're leaving it open, nobody will be able to withdraw funds or even unstake any of your coins. So that'll be a really powerful feature. It adds a lot of additional security. And this virtual machine basically will support AND and OR logic.

So you could say that this set of credentials can do this, or this set of credentials can do that. Or you can combine them together, and you can put a time limit on it. So you can say, this set of credentials, plus this set of credentials, plus this set of credentials have full access on my sig chain if the sig chain has not produced a transaction for the period of 1 year. So what that would be is an automatically activating will. So you'll be able to even put credentials that have access to one account.

So if you do have 3 children, you could say, okay. Well, this account will be able to be accessed by this child after my sick change inactive for a year. Or this account, this other account will be able to access by that child if my sick change inactive for a year. Or this deed, this asset will be accessible by this other account, this other person after a period of 1 year. So what that means is that those credentials will not be able to access a sig chain as long as your sig chain is producing transactions.

And you'll be able to set that time limit, so that creates kind of an automatically executing last will and testimony. And like I said, it'll be a programmable access control pattern. So it's gonna be, essentially, smart contracts for your led ledger level authentication system, and it's gonna follow some of the conditional contract logic. So I've started coding that. That's a really important one, and I want it to be really powerful so that you can have access to all of these different parts of the state of your sig chain.

This will also allow you to do multi signature credentials as well. So you'll have your master, and then you could create another set of credentials for debits that requires 2 sets of credentials to sign off on the transaction in order for that to be authenticated. So like I said, it's gonna add a lot of really powerful functionality. It'll also allow us to prevent your account from being hacked in many, many different ways. It'll allow you to create multi signature authentication.

It'll also allow us to add 2 factor authentication, where you can have a separate 2 factor authentication app and Nexus app per se, or we can make a 2FA code built into our mobile wallet so that you'll have to sign off on both devices. And that would be like a multi sig in order to do a debit, for instance, but maybe a credit could sign off with each individual one. So we'd be able to control these granular aspects of your signature

authentication system. So that's one of the the main features for this hard fork. As I said, we're basically doing chain state parameters and an asset That's not done.

Difficulty adjustments, that's just about done. The asset, that's not done. Aggregate the dial sig chains, that's not done. Truncate the legacy chain, that's not done. And then the Next Hash authentication scripts, that's in progress right now.

These things are being built. Now the the index system revamp, I'm gonna have that done by the end of the weekend. That's a huge milestone for the indexing system. I haven't as I've said earlier, been totally satisfied with the indexing system, so it's good to be getting that done. Getting that sorted.

And that's a lot of code. It's about 2 or 3,000 lines of code. So I'd say that's probably about 50, 60 percent there. Just gotta clean up some of the additional logic. And then the ledger level of virtual machine, ideally, I would like to have that done within a week.

And then we're wanting to get the hard fork out within the next 2 weeks. Potentially a little potentially later than that. It might be 2 weeks to a month. That would be ideal, and then it'll be a 2 week activation. If you still have legacy coins on the legacy chain, make sure you move them.

We did have somebody found to move their coins out of the legacy chain. So now there's about 15,300,000 coins that have been burnt and lost. So that's currently what our unburned is being set at. We're also working on the list of people, for the that unburned of where they're gonna be distributed to. I have most everybody's numbers just waiting on one more to get that finalized.

And then I'm gonna publish that in the main channel, and we're going to do an on-chain vote. So we're gonna do it like we did with the embassy on-chain vote. We're gonna create an account with a name, and I'm gonna put in that asset all the allocations to each individual. And then you'll send the smallest amount of NXS .0001 to that account, and you'll vote with your trust. And so we're gonna ratify that specifically on-chain.

But it's looking like about 6,000,000 will be distributed to the team for bounties and everything, and about 10,000,000 will remain in the satellite war chest. So I will keep you guys in the loop next week. I look forward to the next development update, and, till next time, guys.