Libertaria: progetto Mercury

costruiamo l'economia peer-to-peer

MERCURY

Versione:171101

Autore:
Markus Maiwald

Co-Autori:
Matias Furszyfer, Sarah Klostermair

Introduzione

Se vogliamo costruire sistemi complessi che siano veramente decentralizzati, abbiamo bisogno prima di un sistema per collegare le persone in modo decentralizzato. Le sfide in questo caso sono numerose. Come possiamo mantenere la privacy degli utenti? Come si collegano gli utenti senza un database centralizzato in cui si possa cercare? Come possiamo fornire agli utenti funzionalità che richiedono e trovano nelle configurazioni centralizzate tradizionali?

Mercury risolve questi problemi fornendo una serie di protocolli connessi che consentono la comunicazione sicura e fornisce servizi su una rete decentralizzata.

A differenza delle piattaforme parzialmente centralizzate come Ethereum, Mercury fornisce una rete di comunicazione e condivisione P2P veramente decentralizzata con un livello di servizio che consente a qualsiasi applicazione di funzionare in modo decentralizzato. I nodi possono offrire servizi incentivati agli utenti, il che garantisce che la rete sarà ramificata e sicura.

Mercury inverte il modello di piattaforma centralizzata dove le aziende e le autorità hanno dall'alto il controllo delle imprese che operano. Gli utenti, invece, mantengono il controllo completo dei propri dati e consentono ai provider dei servizi di connettersi a essi in base ai profili condivisi pubblicamente.

Basandosi sul duro lavoro e la ricerca del progetto Internet of People (IoP), libertaria è stato in grado di unire le loro conoscenze con nuove tecnologie e ha creato il punto di partenza per una vera economia P2P.

panoramica

La rete libertaria è formata da diversi tipi di nodi. Grazie a TitaniaOS di Libertaria quasi tutti i dispositivi possono funzionare come un nodo utente standard. Tuttavia, il sistema incentiva gli utenti a far funzionare anche nodi più potenti, i quali forniscono prestazioni di immagazzinaggio decentralizzato o di indicizzazione decentralizzata per alimentare i motori di ricerca decentralizzati.

La rete libertaria sarà:

- **aperta,** in modo che chiunque possa aggiungere o arrestare un nodo che possiede
- **affidabile,** quindi tollererà guasti dei nodi o problemi di rete
- **attendibile,** in modo che il sistema sia auto-convalidante
- **robusta,** quindi sia preparato per i nodi maligni
- **libera, in modo che chiunque possa unirsi o lasciare**

Con la rete stabilita, Mercury consente agli utenti di connettersi e interagire tra loro, così come di utilizzare i servizi forniti dalle dApps. Questa funzionalità è ottenuta attraverso tre livelli operativi:

- **Lo strato di connessione.** Gli utenti possono trovarsi e stabilire una connessione diretta basata sui profili che condividono. Essi possono anche connettersi a reti decentralizzate, ad esempio una rete di archiviazione di file (IPFS, StorJ), ai server di profilo, alla rete basata sulla localizzazione, alla rete di prossimità e/o qualsiasi blockchain.

- **Il livello di servizio.** Un livello astratto, agnostico, estendibile e plug & play consente di implementare i protocolli di comunicazione tra i servizi.

- **Il livello dell'app.** Gli sviluppatori possono creare dApps per gli utenti senza dover conoscere la complessità degli strati più profondi.

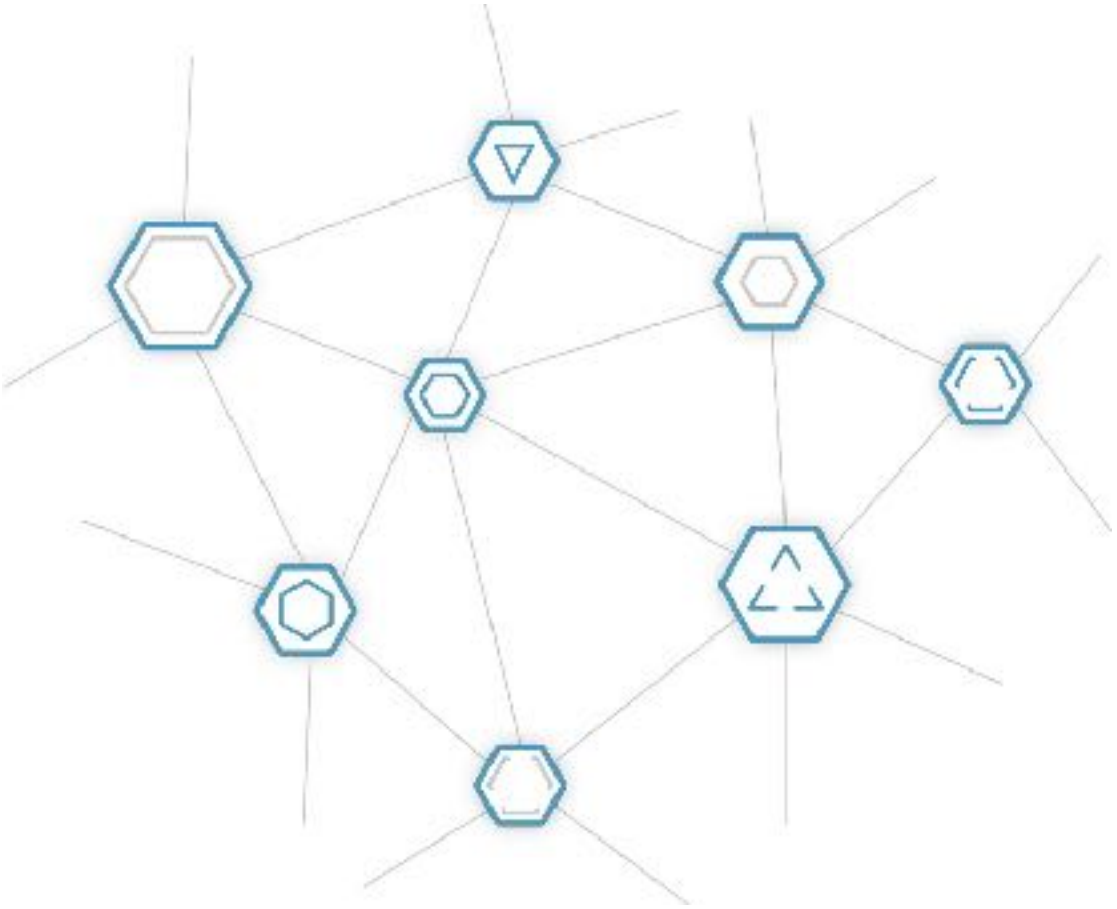
Nelle sezioni seguenti vengono illustrati i tre livelli in dettaglio, seguiti da una sezione sui diversi tipi di nodi che la rete supporterà.

Concludiamo con una spiegazione di come queste tecnologie si uniscono per fornire agli utenti una rete sociale aperta e una tabella di marcia di sviluppo che mostra lo stato attuale del progetto e quando le varie fasi avanzate del progetto saranno completate.

Il livello di connessione

L'infrastruttura che supporta la rete libertaria e connette i vari nodi è chiamata “libreria di connessione”. Tutti i nodi sono collegati dal protocollo Connect, che è a prova di manomissione e permesso.

Le reti peer-to-peer devono essere molto resilienti. La rete libertaria sarà molto implementata per garantire che i nodi possano rimanere sempre connessi. Se una connessione verrà persa, la rete tenterà di ripristinare una connessione tramite qualsiasi mezzo disponibile (ad esempio, tramite reti mobili private 5GHz).



Tutti i nodi sono collegati in una rete basata sul P2P con network autorizzati e affidabili che utilizzano la libreria connessa .

Libreria di connessione

La libreria di connessione è la porta d’accesso per la rete libertaria ed è nota anche come livello di rete.

La libreria di connessione si occupa di trovare e costruire profili e di collegarli a servizi e l’uno con l’altro.

La libreria di connessione può stabilire due diversi tipi di connessione: una connessione P2P tra gli utenti finali o una connessione a una rete decentralizzata, ad esempio ad una rete di archiviazione dei file (IPFS, StorJ), ad un server di profili, ad una rete basata sulla localizzazione, ad una rete di prossimità o ad una qualsiasi blockchain.

Esempio

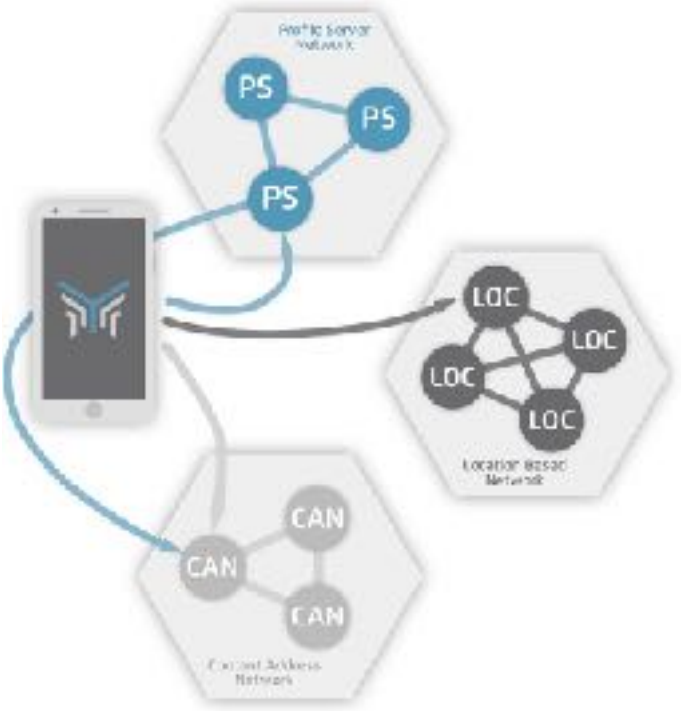
Un utente finale vuole caricare un video per condividerlo con le parti interessate (come caricare un video delle vacanza su Facebook).

Questo sistema P2P non funziona allo stesso modo delle piattaforme di servizio centralizzate (Facebook, Twitter, YouTube).

Tutti i dati, così come tutte le connessioni, sono accessibili solo in modo decentralizzato.

I file sono "memorizzati" su file System decentralizzati, i profili sono accessibili in reti di profili specifici. Anche i dati di posizione hanno una propria rete.

Per accedere a tutti questi dati con il tuo profilo, esso deve essere registrato su un nodo Home (dove è stata verificata la tua chiave), per poter accedere alla rete Profile server vicino a te (posizione e rete di prossimità).



Successivamente, è possibile caricare tutti i file nella rete CAN (file storage) e condividerli in un ambiente decentralizzato.

Stabilendo gli standard di protocollo tra le reti P2P, la libreria connessa riduce drasticamente il lavoro di sviluppo e il tempo per la creazione dApp

livello di servizio

Il livello di servizio è un livello astratto, agnostico, estendibile e plug & play che implementa i protocolli di comunicazione tra i servizi. Questi termini sono spiegati più dettagliatamente sotto:

- **Astratto e agnostico:** l'architettura è un' API di alto livello che è stata costruita in modo da non essere legata a qualsiasi servizio o piattaforma. La rete libertaria non è collegata ad alcuna tecnologia di servizio particolare (blockchain, sistema di Lima decentralizzato, rete di profili, ecc.) e ogni sviluppatore può generare il proprio servizio ed usarlo alla base della biblioteca di connessione del livello di servizio, seguendo questi standard.

- **Estendibile:** chiunque può aggiungere qualsiasi servizio disponibile al proprio profilo, costruire il proprio servizio/protocollo e collegarlo alla rete decentralizzata in qualsiasi momento.

- **Plug & Play:** qualsiasi dispositivo finale può aggiungere un servizio in qualsiasi momento e collegarlo alla rete senza dover reinstallare o configurare nulla. [1]

Il livello di servizio si trova immediatamente sopra la libreria di connessione e sotto il portale di connessione. Si tratta di un processo in background Android/Desktop con una Common Object Request Broker architecture(CORBA). Una porta per iOS è prevista e sarà consegnata entro la fine del 2017.

1 un buon confronto è un IDE come IntelliJ, Eclipse o NetBeans. In questo tipo di software, sostenere un'altra lingua è semplicemente questione di scaricare il collegamento giusto. In altre parole: gli utenti e gli sviluppatori devono solo collegare i servizi e essi sono pronti per essere utilizzati in una rete decentralizzata. Un buon esempio è l'installazione di un'applicazione esterna come un'app di chat o un wallet sul telefono. Quelle applicazioni saranno collegate con i loro servizi al loro profilo

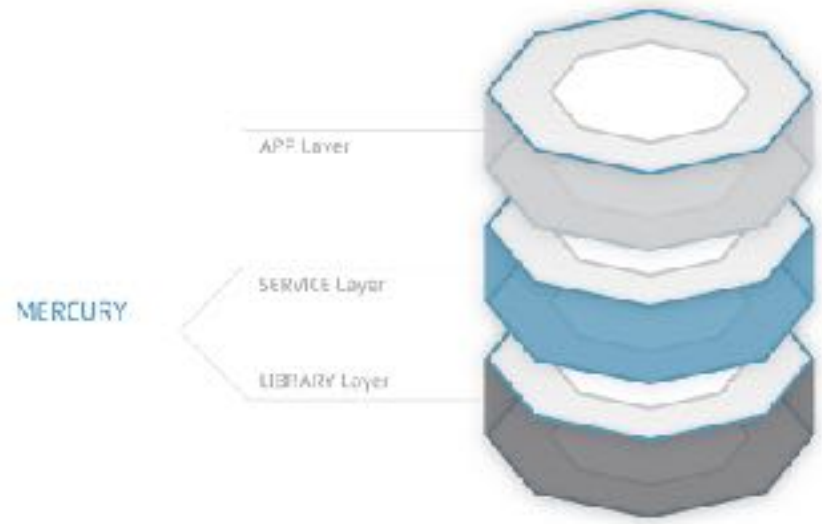
Questo livello non è “consapevole” di come le connessioni sono costruite o dove altri dispositivi si trovino. Chiunque può aggiungere qualsiasi servizio disponibile al proprio profilo, costruire il proprio servizio/protocollo e collegarlo alla rete decentralizzata in qualsiasi momento.[2]

Per migliorare la sicurezza, i servizi comunicano tra loro. I nodi non sanno come i servizi sono stati costruiti, come funzionano o quali dati vengono inviati attraverso di loro. Essi instradano solo i messaggi criptati tra i dispositivi. La rete è addormentata e viene utilizzata solo end-to-end. Il protocollo di crittografia fa parte del livello di rete (libreria di connessione). Il livello di servizio può scegliere tra diversi algoritmi di crittografia tra i diversi parametri di impostazione della connessione (TTL, Max Message queue limit, Relay message attraverso il profilo server, Tor, WebRTC) con una connessione personalizzabile pronta per un uso P2P

livello dell'app

Assieme ai livelli di connessione e servizio, Mercury supporterà applicazioni decentralizzate P2P-Enabled (dApps).

In realtà, qualsiasi applicazione può essere convertita in una applicazione decentralizzata e abilitata P2P con l'infrastruttura di Mercury.



Le dApps Libertaria saranno apps P2P decentralizzate che fermeranno la diffusione di app su piattaforma centralizzata di Governi e corporazioni (Airbnb, Uber, denaro digitale governativo, ecc.) e attiveranno una vera economia P2P.

In Libertaria, tutti le DApps sono basate sulla struttura di Mercury.

Questo semplifica il lavoro per gli sviluppatori rendendo le lunghe curve di apprendimento obsolete.

Invece di dover comprendere ogni singola parte dei diversi protocolli, dei server e degli agenti all'interno della rete libertaria, gli sviluppatori possono concentrarsi sulla qualità del loro prodotto o servizio.

2 esempio: Bob e Alice utilizzano un servizio di chat criptato per comunicare, utilizzando un servizio di localizzazione (come una app per taxi), per condividere la loro posizione in tempo reale, e/o utilizzando un servizio di acquisto/vendita per consentire a Bob l'acquisto da Alice senza pagare commissioni a terze parti che non aggiungono valore al prodotto finale.

Nodi

La rete libertaria sarà popolata da una vasta gamma di utenti che impiegano una vasta gamma di dispositivi per impegnarsi in una vasta gamma di attività di comunicazione e transazioni.

Sarebbe chiaramente inefficiente cercare di soddisfare tutte queste diverse esigenze con un solo tipo di nodo; di conseguenza, la rete incoraggerà i proprietari dei nodi a utilizzare diversi nodi personalizzati in base alla funzione che il proprietario del nodo desidera ed è più adatto allo scopo.

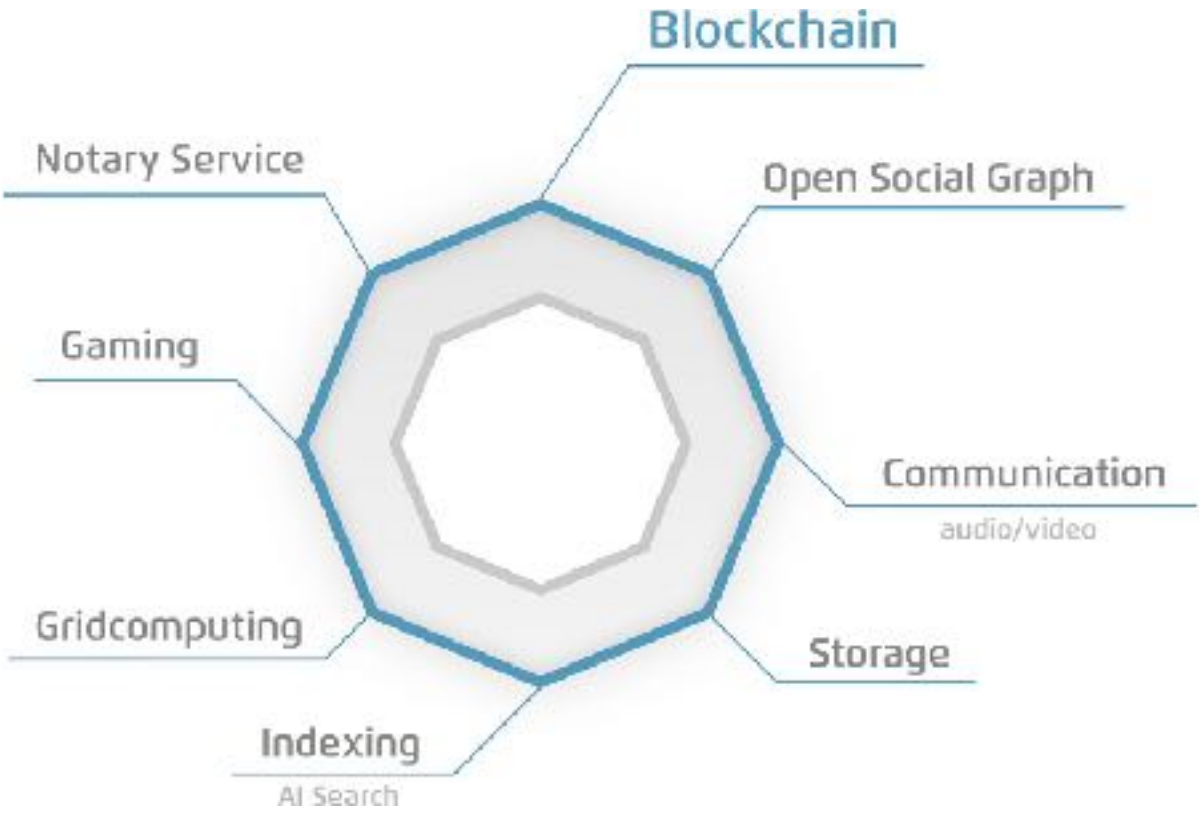
I nodi possono essere personalizzati, e quindi le possibili variazioni sono quasi infinite. Tuttavia, esistono due tipi principali di nodo: nodi completi e nodi di servizio. I nodi completi vengono fatti lavorare sui server e fungono da spina dorsale della rete, mentre i nodi di servizio vengono girati su dispositivi meno potenti o mobili e offrono (micro-)servizi

I nodi sono interconnessi tra loro tramite lo strato di connessione.

La rete che formano è senza autorizzazioni, per cui ogni nodo è collegato ai suoi vicini senza discriminazione. Gli smartphone e i service provider aiutano la funzione di rete in modo corretto ed efficiente offrendo servizi (Storage, blockchain, testimonianze, condivisione, ecc.) per sostenere l'infrastruttura di Mercury.

I nodi possono offrire servizi multipli. Questi servizi saranno offerti gratuitamente o tramite un modello incentivante di scelta del proprietario del nodo. Ogni nodo dispone di un certo numero di slot per i distinti servizi che il nodo può offrire.

Ad esempio, slot A potrebbe essere un host per la blockchain IoP e i micropagamenti, slot B potere essere la connessione sociale grafica aperta (profilo server per le reti sociali), slot C potrebbe ospitare la scelta del proprietario del nodo di Messenger, servizio chiamate e comunicazione come email, ecc.

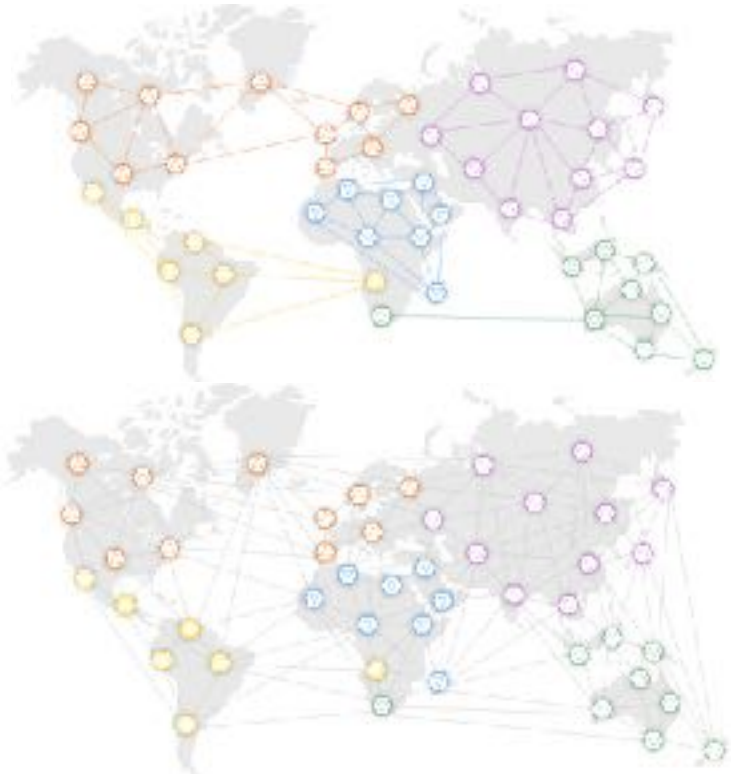


Selezione di possibili slot per nodi da agganciare ai servizi

È fondamentale che gli utenti siano liberi di scegliere la tecnologia e la valuta che meglio si adatti a se stessi e alla loro comunità. Ad esempio, un proprietario di nodo potrebbe offrirsi di fornire alla Comunità l'archiviazione decentralizzata del cloud tramite il relativo nodo attivando il livello di archiviazione nello slot D con il protocollo StorJ. In questo caso, il nodo del servizio verrebbe alimentato dai token StorJ ricevuti dal multi-Wallet del nodo.

Rete sociale aperta

Gli strati Connect e Service, di Libertaria in combinazione con i nodi e le dApps sviluppate dalla Comunità, aziende o sviluppatori indipendenti, formano un social network aperto che tutti possono utilizzare per condividere le informazioni.



Interconnettibilità

Come descritto sopra, le dApps sono collegate alla rete Libertaria tramite la libreria di connessione.
Qualsiasi dApp con attributi di servizio simili può quindi connettersi con altre dApp e condividere informazioni. Questo fornisce nuove dApps ad una comunità preesistente, il che significa che gli utenti non hanno bisogno di installare diverse applicazioni con funzioni simili o identiche solo per connettersi a tutti i loro coetanei (com'è attualmente nel caso di applicazioni di messaggistica).

facilità di utilizzo per i dispositivi mobilii

Applicazioni P2P mobili spesso soffrono di carenze di risorse su dispositivi mobili, come il consumo della batteria e requisiti di memoria elevati. Libertaria risolve questo problema dando la possibilità di separare il dispositivo e il nodo. I dispositivi mobili non hanno bisogno di agire come nodi completi, ma possono invece connettersi via Bluetooth a un dispositivo più robusto come un nodo Titania che svolge questa attività. Questo rende più efficace per i dispositivi mobili connettersi alla rete, così come aiuta a stabilire una rete P2P stabile e riduce i tempi di inattività inutili.

Utilizzo continuo

Il Mercury Open Social Network è costruito per fornire agli utenti la stessa facilità d'uso che sono abituati con le loro applicazioni regolari. L'obiettivo è che non ci siano barriere all'uso di dApps nella rete libertaria. Questo è particolarmente importante, come libertaria stia cercando di portare decentramento per le persone con poca conoscenza tecnica delle reti e dei nodi P2P.

Modi di uso infiniti

Mentre libertaria sta definendo e sviluppando ulteriormente il protocollo di Mercury, questa parte importante dell'insieme della rete di libertaria permette di sviluppare le applicazioni decentralizzate per quasi tutti i casi di uso. partner del progetto di libertaria è Internet of People, che ha contribuito in parti significative dell'infrastruttura ed è attualmente pronta a fare diverse implementazioni di riferimento per semplificare i diversi modi di utilizzo, come la messaggistica, il carpooling, il dating e lo scambio di attività.

Tabella di marcia

fase 1(2018Q1)

- Rendere più facile per gli sviluppatori della comunità il contribuire alle API della libreria di connessione API e scrivere applicazioni su di essa.

- Terminare le prime poche applicazioni mobili basate sulla libreria di connessione, per ispirare gli sviluppatori della Comunità a contribuire. La qualità del codice dovrebbe essere abbastanza alta da far si che gli sviluppatori possano facilmente capire come fare le proprie dApps in base ai nostri esempi.

    - Messaggeria
    - Multi-Wallet di alta qualità
    - Condivisione della posizione (simile a Google Maps)
    - Semplice condivisione di file
    - Multi-Wallet nel browser Web
    - Messaggeria sicura
    - Inizializzazione di un wallet HD, memorizzata o generata da password complessa
    - Un pulsante di suggerimento con tutto il codice proveniente da server federati: server HTTPS in esecuzione su ogni nodo completo

- Consentire alle applicazioni Web del vecchio mondo di integrare alcune funzionalità da componenti della libreria di connessione, senza compromettere la protezione e la privacy dei dati memorizzati nella libreria stessa.

- Aiutare le persone che desiderano impostare nuovi nodi o componenti completi di libertaria con documentazione, script e hardware preinstallati e creare una rete distribuita di nodi completi e di nodi di servizio.

- Definire gli standard per il protocollo Mercury

- inserire diversi protocolli e standard nel nodo

- Abilitare comunicazioni e messaggistica sicure

- Autenticazione basata su blockchain e server di profilo

- Un Vault per certificati, contratti, profili, identità

- Social media integrato, che unisca sia le reti centralizzate come Facebook, sia quelle decentralizzate come libertaria.

- Libreria di connessione sul Web con hosting dai nodi *. IOP. Network federati.

Fase 2 (2018Q2)

Dopo aver unito i progetti più promettenti (che siano sufficientemente maturi) della fase 1 nel nostro nodo, nella fase 2 inizieremo a sviluppare le nostre soluzioni per ogni slot nel nodo.

I compiti prioritari sono:

- Nodi di servizio abilitati per micropagamenti
- Protocollo Mercury
- Protocollo del social network aperto
- Web decentralizzato