LISK

Build and deploy blockchain applications in JavaScript.

Presented By:

Ashutosh Chandra (IRM2015001)

Pallavjeet Singh Nirwan (IIT2015131)

Aditya Powale (IRM2015003)

Muthyala Nagnath (ITM2015006)

Abhishek Sharma (IHM2015005)

Overview

- Lisk was the first **modular** cryptocurrency that allows developers to write decentralised application using Javascript.
- Lisk was the first decentralised application written entirely in **node.js**.
- The Platform allows developers to craft their own **side-chains** that are linked to the main network.
- The objective of developing **Lisk** was to address the problem of **scalability** in bitcoin and ethereum.
- Rather than using proof-of-work and proof-of-stake, it uses **Delegated Proof of Stake** concept.
- It became the 2nd most traded and popular cryptocurrency after **bitcoin** in mid 2016.

Modularity

Modularity :

- Scalability has been a problem with crypto-currencies since Bitcoin’s introduction.
- Scalability is the capability of a system, network, or process to handle a growing amount of work, or its potential to be enlarged in order to accommodate that growth.
- The core objective of Lisk is to address the problem of scalability in other top blockchain networks especially Bitcoin and Ethereum.
- Lisk will become the first truly modular crypto-currency by utilizing sidechains as a solution to scalability. Lisk sidechains allow us to implement various features into the Lisk main network simply as Blockchain Applications.

Modularity :

- Lisk is able to support thousands of applications as each application will run on its own sidechain.
- Future developments to these modules are far easier to implement.
- LISK mainchain in this way will remain lean as it will not get polluted with all the dapp data.
- Lisk also provides a store/directory of apps available on the Lisk platform. You can access these right from the Lisk Client. So Lisk provides a decentralized store for blockchain apps to exist and distribute.

Delegated Proof of Stake

Delegated Proof Of Stake (DPoS)

- Bitcoin mining was too energy-intensive and eventually centralization of mining would occur, leading to an imbalance of network control
- There is also the issue of speed which, due to the proof of work method of bitcoin mining, can be very slow
- Delegated proof of stake uses real-time voting combined with a social system of reputation to achieve consensus
- Active delegates are voted into their roles by token holders
- The voting power that the token holder has, otherwise known as voting weight, is determined by how many of the base token the account is holding

Roles Of Delegates

- Ensuring their node is always up and running.
- Collecting the transactions across the network into blocks.
- Signing and broadcasting those blocks, validating the transactions.
- If there are issues in regard to consensus, DPoS allows these to be resolved in a fair and democratic way.

Advantages Of Delegated Proof Of Work

Actually Decentralized: Mining of transaction in a block is not only possible by giants who have acres of concentrated computing powers. Earlier, mining was possible via a personal computer, but such is not the case anymore.

Fast and Efficient: Transactions are confirmed in an average of 1 second by having a deterministic selection of block producers. This is way faster than Bitcoin’s confirmation time that ranges from 10 minutes to hours.

Democratized: The delegates in a DPoS implementation are elected by the stakeholders. Also, if a delegate seems to act in a nefarious manner, the stakeholders can remove him.

Sidechain

Sidechain

- Sidechains are an independent cryptographic ledger which attach to the main blockchain,but does not impact the speed or security of the main chain.
- Sidechains are important because they reduce the 'bloat' on the main chain allowing the main chain to continue being fast and efficient and only those who are interested in the Dapp are responsible for maintaining it and not everyone. Thus keeping the entire platform lean.
- Since applications are being developed on sidechains if something goes wrong on another applications blockchain it won’t force Lisk to have a hardfork because it won’t affect the Lisk blockchain.

Sidechain(contd.)

- Each sidechain(dapp) has its own consensus.Sidechain consensus is maintained among the 101 master nodes using the same Delegated Proof-of-Stake (DPOS) method used to secure the Lisk blockchain.

- The motivations behind this form of consensus are to prevent unnecessary enlargement of the Lisk blockchain and to retain individual sidechain autonomy, while at the same time, ensuring the integrity of each side chain is constantly upheld.

Core Features

Usernames

- Lisk allows users to register usernames. Which **act as an alias** to your account
- This **eliminates the need to remember** long account addresses
- The network fee for username registration is **100 LISK**
- Each username is unique. The length is currently limited to **16 characters**.
- Currently, it is **not possible to remove a username** from your account.

Contacts

- Allows users to maintain a contact list to **store frequently contacted accounts.**
- If an account has many confirmed contacts, **it may be considered more reputable**.
- When a user is added to the contact list, it will show as a **pending contact request** in the user's wallet. Once the other user accepts the request, the **requester will be added to his contact list**
- Network fee for adding a new contact or accepting an request is **1 LISK**.

Multi-signatures

- Lisk allows users to create a **multi-signature group** which can be configured to require **some or all signatories for approval.**
- To achieve this a M of N multi-signature architecture is implemented.
- **Members of a multi-signature group (N)** are added, up to a **maximum of 16 signatories.**
- **M must be greater than 1** and **less than or equal than N**.

Multi-signatures

- Once you **initiate a transaction** from the multi-signature group, **all members will see** this pending transaction and **decide whether to approve or ignore it**.
- The **owners of a multi-signature group may change the rules** of the group at any time **with the approval of at least M of the signatories**.

A Block in Lisk

- Block generation occurs **every 10 seconds** within the Lisk network using **DPoS consensus**
- When a delegate is assigned a slot and has a node running, that delegate **generates the next block** and **confirms up to 25 transactions from the transaction pool**
- These c**onfirmed transactions will be added to the payload of the block** and subsequently signed into that block.

Block Header

- A 32 bit integer **identifying** the version of the block
- A 32 bit epoch **timestamp** of when the block was created
- The 64 bit **Id of the previous block**
- A 32 bit integer corresponding to the **number of transactions processed in the block**
- A 64 bit integer corresponding to the **total amount of Lisk transferred**
- A 64 bit integer corresponding to the **total amount of fees associated** with the block
- A 64 bit integer corresponding to the **Lisk reward** for the delegate
- A 32 bit integer corresponding to **payload length**
- The 256 bit hash of the **payload**
- The 256 bit **public key of the delegate** who generated the block

Security

- The system uses **EdDSA (Edwards-curve Digital Signature Algorithm)** as it provides a much faster mechanism for hashing and providing security; rather than ECDSA.
- When a user creates an account, a **passphrase** is generated for the user. This passphrase is hashed using the **SHA-256** hash function into a 256 bits string. This hash is subsequently used to generate the **private key ks** and derives its **public key kp.**

Second pass phrase

- Lisk offers an **additional layer of security** for the user.
- Using a **specific class of transaction (Type-1)** , the user can register **a second pass phrase** that is associated with the Public Key.
- This relationship requires that **all subsequent transactions to be signed** using the second pass phrase in order to be considered valid.

Thank You!