Legion Network

A collection of distributed blockchain networks for secure messaging and data storage.

Introduction

There are many problems with the current state of internet based messaging and data storage. We trust a large portion of our digital lives (in actuality, our real lives) to large corporate entities, giving them access to our private conversations and sensitive personal records. We trust these large corporate entities to handle our information responsibly. We trust them to keep it secure from hackers. We trust them not to tamper with or alter our information. We trust them not to lose our information. We trust them not to use our own information against us by selling it to third parties. We trust them not to turn our data over to legal authorities without a warrant, in blatant violation of the fourth amendment of the United States constitution.

As we have seen repeatedly, these corporations are incapable of properly securing our personal information. Large-scale hacks where millions of passwords are harvested and identities are stolen occur frequently. As revealed in documents leaked by Edward Snowden, the US government is actively engaging in bulk data collection, harvesting our movements, phone calls, emails and text messages without the approval of a judge. Large email providers sell our personal information to advertisers. Social media giants now act as the judge, jury and executioner, removing content that it finds offensive or politically misaligned. Large, centralized data warehouses hold the backend data for countless websites and computer applications (full of our personal information and data) just hoping that clever hackers won't get their hands on it.

Clearly, our trust has been misplaced.

Blockchain networks such as Bitcoin have changed the world in that they give us a new way to trust trustless parties, without the need of a trusted third party. Peer-to-peer transactions over the internet are now a reality. But of more importance is the fact that we now have a way to share *data of any kind* in a secure, distributed, immutable form. We no longer have to send private correspondence to a third party such as an email provider, trusting them not to intrude into our private lives. No longer must websites and applications store data in centralized data warehouses, hoping administrators don't pry and large corporate entities don't sell our data. This is all due to the power of blockchain networks.

Goals

The goal of the Legion Network is to provide an immutable messaging layer for private correspondence, secure data storage, public data storage and the transfer of value using cryptocurrencies. While there are likely existing blockchain networks that can meet these goals, the Legion Network is also:

- **Lightweight -** The Legion Network is actually a collection of an infinite number of small blockchain networks, each fully contained and isolated.

- **Extendable -** All Legion Network functionality is exposed via RESTful APIs, allowing messages to be securely sent from any application or command line.
- **Modern -** Written in NodeJS, the Legion Network is easy to setup on any operating system, on any server or workstation.with just a few commands.

Terms

Throughout this paper the following terms will be used.

- **Sidechain -** This represents a collection of computers (nodes) all communicating to each other using the Legion Network software. Sidechains can be public or private.
- **Mainchain -** This represents the first sidechain ever created on the Legion Network. Sidechains that wish to be public can list themselves on the mainchain, allowing nodes around the world to join their sidechain network.
- **Node -** This represents a computer that is connected to one more more Legion Network sidechains.
- **Master Node -** This represents a special type of node on each sidechain network that help determine “truth”. There can be one or more master nodes on each sidechain. These are typically under the control of the sidechain administrator.
- **Miner -** This represents a specific type of node that does the work of that sidechain. Miners compete to solve cryptographic puzzles in exchange for cryptocurrency (such as Bitcoin.)
- **Token -** This represents one unit of cryptocurrency. Each sidechain uses its own native token.
- **Message -** There are multiple types of messages allowed on the network, such as *Private Messages, Public Messages, Token Transfer Messages, Administrative Configuration Messages,* and *Content Tag Messages.* In order to send any message, some amount of tokens must be permanently burned by the sender. The amount depends on the length of the message.
- **Sidechain Administrator -** This represents an account with special privileges on a sidechain network. Sidechain Administrators can send *Administrative Configuration Messages* to update network rules, as well as create and sell tokens.
- **Block Reward -** This represents the amount of cryptocurrency (such as Bitcoin) a miner is paid for solving a block. The amount is set by the sidechain administrator and paid by the sidechain administrator.
- **Expected Block Time -** This represents the amount of time it should take to mine a block. All sidechains will have an expected block time of 60 seconds. Difficulty will be adjusted to meet this expected block time depending on available hash power.

Each of these terms is further explained in this document.

Use Cases

Below are multiple use cases which will help illustrate some of the intended uses of the Legion Network

Use Case #1: Alice and Bob have a professional business relationship. Due to the insecure nature of email, and the sensitive details they are often required to discuss, they seek a more secure method of communication that uses asymmetric encryption. Alice creates a private sidechain on the Legion Network, which Bob then joins from his computer. Their messages now flow completely encrypted across their two-node peer-to-peer network, ensuring they can never be read, deleted or altered by any third party.

Use Case #2: Jan works for a large corporation. She has uncovered evidence of insider trading and wants to make the information public, but wishes to do so in a completely anonymous and untraceable way. As opposed to sending the evidence via email, or some other way in which her IP address might be traced, she insteads submits it via the Legion Network on the sidechain of a major news organization. This contains no record of her identity or IP address.

Use Case #3: Jake is a farmer who sells bushels of wheat to various buyers. Jake tracks all sales using a third party application that writes data to a sidechain on the Legion Network. Weeks after a sale, a buyer insists he only received 100 bushels, not the 120 bushels Jake actually sold. Because of the immutability of blockchain technology, Jake is able to report to the buyer exactly which bushels were sold on the date in question.

Use Case #4: Jane is a protestor in a country where internet access is heavily restricted and censored. She has evidence and pictures of police brutality, however she does not have access to standard email or file transfer services because they are blocked. Because the peer-to-peer nature of the Legion Network makes it virtually uncensorable, she is able to send pictures abroad.

Use Case #5: Nick is a software developer working on a large and custom application. Because he does not trust Microsoft, he is unwilling to store his source code on github or any other centralized service. Instead he uploads his code to the Legion Network, encrypted by both symmetric and asymmetric encryption. In addition to keeping his source code protected, the immutability of the public Legion Network ledger demonstrates ownership of his own intellectual property, in case the source code is otherwise stolen and litigation is required.

Use Case #6: Julie is a blogger who regularly writes on controversial political topics. She is hesitant to trust any blogging platform with her content, because they may have reason to alter or delete her posts. Instead she uses a popular blogging chain on the Legion Network. Her content is meant for public consumption, as such it is not encrypted. But because it is stored on the Legion Network, it cannot be changed, censored or deleted.

Use Case #7: Tim is a CTO of a medium-sized fabrics company. He wants to move the company database server offsite, for better security, redundancy and reliability. However the cost of centralized data storage services is too much for his budget. Instead, he decides to create a private sidechain on the Legion Network. He then joins that sidechain from a home PC, a hosted virtual machine, and one machine at the office. These computers all do the work

of storing, encrypting and sharing data relevant to the business and ensure it can be accessed at all times, without the cost of a centralized hosted database.

These are just a few cases in which an anonymous, peer-to-peer, encrypted messaging and data storage platform can be used as a better alternative to current technologies.

Sidechains

As previously stated, the Legion Network consists of an infinite number of smaller blockchain networks, known as *sidechains*. Sidechains can contain any and all types of data. Any message sent to a node is immediately sent to all other nodes on that sidechain's network. Each node adds the message to their memory pool and eventually the message is added to a block via proof-of-work consensus, where it will remain forever as long as at least one node remains connected to the sidechain network.

Sidechains can be either public or private. Public sidechains can be joined by any computer on the internet. Those computers form a distributed peer-to-peer network, where each computer performs the work of that network (sharing content, listening for messages, and solving blocks). Private sidechains can only be joined by authorized nodes. Nodes are authorized by signed messages with public keys specified in the genesis block or an Administrative Configuration Message, as managed by the sidechain administrator.

The first sidechain ever to be created on the Legion Network is referred to as the *mainchain*. The mainchain serves one purpose: To allow the listing of sidechains. All public sidechains have the option of listing their chain by writing a message to the mainchain. This allows other Legion Network users to see and potentially join the sidechain network (committing their processing power to solving blocks and earning cryptocurrency) which further distributes the content around the world.

This creates an extremely distributed ledger for any type of data, private or public. A small sidechain network of just two computers can be created to exchange secure messages in a completely peer-to-peer way without worry of these messages being viewed, removed or altered by a third party. A sidechain network may grow over time to include dozens or hundreds of computers all around the world, ensuring that the data stored on that network is available, immutable and uncensorable at all times. Applications can be developed on top of these ledgers using simple HTTP methods to store and retrieve data, connecting to any node in the sidechain network, ensuring that there is no central point of failure or authority of the data. The possibilities are endless.

Cryptocurrency

Each sidechain utilizes a cryptocurrency (often referred to as "token") that is completely private to that sidechain. The purpose of these tokens is not to be listed on an exchange, or necessarily to increase in value, although the value of these tokens can certainly vary. Their purpose is to act as an anti-spam measure for the chain, ensuring that there is a small cost for

storing data or sending messages on the network. Otherwise each sidechain would end up being just as cluttered as your average spam folder.

In order to write data to any chain on the Legion Network, some amount of cryptocurrency must be permanently burned. If the sending account does not contain enough of the cryptocurrency to pay for the message data, the message will be rejected by the network.

Tokens can be purchased at master nodes, using a web browser or API call. The price of the token is set by the sidechain administrator, depending on the needs and purpose of the network.

One token is worth one kilobyte of data. One million tokens will be created during chain creation, in the genesis block. Sidechain administrators can mint additional tokens as the network grows.

Message Types

Technically any type of data can be serialized and stored on the blockchain of any sidechain. We will categorize messages into 5 basic types:

- **Private Message -** This represents a message from one user to another. The content of the message will be asymmetrically encrypted using the public key of the recipient, so only the recipient can read the message.
- **Public Message -** This represents data that is intended for public consumption, so it is not encrypted.
- **Data Storage -** While the Legion Network is not intended to be a file storage system it can be effectively used to store basic application data.
- **Administrative Configuration Change -** Sidechains can be managed by sidechain administrators, who will sometimes issue configuration changes. Nodes will read these configurations from the blockchain, and put the new rules into effect starting at the next block.
- **Transfer -** This represents the sending of cryptocurrency from one user to another.

All messages will be persisted on the blockchain forever, as long as at least one node remains on the sidechain and connected to the internet. Sending any message requires the permanent burning of some amount of the sidechain token. The amount of token burned depends on the length of the message.

Administrative Configuration

When creating a sidechain, the user will be required to supply information about the new chain. This information will be stored in the *genesis block* (the first block created on the new chain.) All other nodes will read this information from the genesis block when they join the chain. This information will include:

- **Chain Name** - This does not necessarily need to be unique, but should clearly identify the purpose of the chain or organization that owns the chain.

- **Token Name** - This is a three to ten character alphanumeric string that identifies the underlying chain token (similar to BTC for Bitcoin, or ETH for Ethereum)
- **Max Message Size** - This is the max allowed size of each message in kilobytes and will vary depending on the purpose of the chain. For example, a chain intended to hold pictures should allow a much larger message size than one intended to send basic plain-text messages.
- **Token Price** - This is the price of a single token in US dollars. Each token represents 1 kilobyte of network storage. Network users can purchase tokens with cryptocurrency, such as Bitcoin.
- **Block Reward** - This is the price in US dollars that the sidechain administrator will pay for each block solved.
- **Public or Private** - The Legion Network allows for either public or private chains. Public chains can be joined by any computer on the internet, while private chains can only be joined by authorized nodes.

These are just a few examples, other information will be required and will be covered in detail in separate documentation. Some options may be modified by an administrator as the network grows.

Private sidechains will have a much simpler configuration, as it can be assumed that all nodes on the chain are part of an organization and can be trusted. For example: the Max Message Size can be set very high, the Block Reward and the Token Price can be be set to zero.

Mining

Mining is the process of doing computational work in hopes of being rewarded. The Legion Network uses proof-of-work consensus, similar to most other blockchains in the world today. Mining is a fairly technical concept that will not be discussed further in this document, but the steps required to turn a computer into a *mining node* are very easy and straightforward. No technical expertise is required.

Mining is not required. If desired, a user can setup a *listening node* which will only listen and distribute messages and blocks to other nodes on the network. Listening nodes will not be rewarded with cryptocurrency, but their energy usage will be far less than required by mining nodes. Some users may decide to setup a listening node because they support a cause or group and want to assist in storing and distributing content, but do not want their CPU to be continuously pegged by the mining software.

Public vs. Private Sidechains

A sidechain can be set to either public or private:

- Public sidechains can be joined by any computer on the internet. The sidechain will be listed on the mainchain making it easy to find by potential mining or listening nodes. Each node will receive a full copy of the blockchain when they first join, and will then become an active node on that sidechain.

- Private sidechains can only be joined by authorized nodes. Private sidechains do not need to be registered with the mainchain, thus they will not be displayed as a joinable sidechain to the public. If an unauthorized node somehow finds a private sidechain and attempts to join, all other nodes on the sidechain will ignore the unauthorized node. The unauthorized node will not receive any messages. Any messages sent by the unauthorized node will be ignored by all other nodes on the network. Nodes are authorized using signed messages by public keys defined in the genesis block or by an administrative configuration change message sent in a later block.

Public sidechains make sense when the data to be stored is for public consumption. Public sidechains allow any computer on the internet to mine blocks and to be rewarded financially with cryptocurrency.

Private sidechains make sense when the data to be stored is for private consumption, such as for private business data. Nodes on private sidechains will still use mining to solve blocks. In some cases, it will likely make sense to have one machine setup as a mining node and all others as simple listening nodes, although for redundancy two mining nodes may be desired. Although developers may be tempted to not encrypt data on private sidechains, encrypting data should still be encouraged as best practice.

Master Nodes

Each sidechain must contain one or more master nodes. The first node on a sidechain will be a master node by default, others can be added as necessary (with an administrative configuration change message) to ensure master node availability.

The main purpose of master nodes is to prevent 51% attacks. While most blockchain systems determine truth by adopting the longest chain, it would be far too easy for an attacker to take over a sidechain with a 51% attack, especially on smaller sidechains. As such, master nodes will be used to establish truth, and will only allow new blocks to be appended to the end of the chain. Once a block is added to the chain of a master node, it is considered “truth” and cannot be overwritten.

In the event that no master node is available on a sidechain for any amount of time, the network should continue to operate as normal. Nodes will continue to share messages and blocks as normal. Once the master node(s) are back online, they will sync with the network as normal. Master nodes will be prioritized, in case they find themselves in opposing chains, the higher priority node will win. When syncing with a sidechain network, nodes will first attempt to sync with the highest priority nodes, which will be the master nodes. If unavailable, they will sync with lower nodes until the master nodes are available.

Content Tags and File Types

Public sidechains are a powerful way to store content in an uncensorable, immutable way. While this can be used for good, there will arise occasions where *node operators* can object to

some content on the sidechain. While no single person can decide that some piece of content must be removed from the network as a whole, each individual node operator must be given the opportunity to remove objectionable content from their own node.

If a node operator objects to the type of content on a sidechain, they should leave that sidechain and commit their computing resources to a sidechain that is more in line with their personal views.

The Legion Network allows individual node operators to remove content by the use of:

- **Content Tags -** Users are given the option of providing content tags when uploading data. Node operators could, for example, ignore any content tagged “nsfw”. Content can also be tagged by a sidechain administrator.
- **File Type -** All uploads will be scanned by each node to determine the type of content in the stream. A node operator could, for example, ignore any files of type “executable” because they do not wish to assist in the spread of viruses. Certain file types can also be rejected by the entire sidechain as configured by an administrator. Obviously, encrypted content cannot be parsed in this way. But a node operator could choose to reject any content that is encrypted.

If content is removed from a node, users will have to visit other nodes on the sidechain to download the desired content.

By default, any new sidechain will be configured to reject certain types of file content, such as executables and pictures. But the sidechain administrator will always have the ability to change these settings.

File Download Security

Any file download utility used to retrieve content from the Legion Network must hash the data received and compare the resulting hash to the hash they requested. If it is not a match, the content must be deleted and never provided to the user. Otherwise it is far too easy for rogue nodes to inject viruses and malware into the stream. The Legion Network uses the SHA-256 Cryptographic Hash Algorithm.

Block Time

The block time is 60 seconds. This means the goal of the network is to generate one block every 60 seconds. Network difficulty will be adjusted to meet this goal, depending on available hash power. If no messages are available, no blocks will be created.

Sidechain Economics

Private sidechain economics are quite simple. In a private chain, only authorized nodes are allowed to join the network, all under the control of a group or organization, working towards a common goal. There are no bad actors, and there is no reason to incentivize nodes to perform the work of the network. The block reward and the token cost should both be set to zero in these cases. We do not need to incentivize nodes to solve blocks with a reward, and the token will never be bought or sold - it will be freely given to each node to use as needed. Private sidechains are quite simple in their configuration.

Public sidechains economics require some thought and planning. Specifically, two values must be considered:

- **Token Price -** A token represents one kilobyte of network data storage, no matter the type of message being stored on the network (file content, private messages, public messages, etc.) Tokens are priced in US dollars, because at this time the price of Bitcoin is simply too volatile. Tokens are sold by master nodes via an API request or in a web browser. Sidechain administrators may set the token price however they choose, depending on the purpose of the network.

  For example, a token price of $1.00 will allow users to submit one kilobyte of data for $1.00. One kilobyte of data is equal to 1,024 characters. So if the purpose of the sidechain is to send short messages, this might be a fair price. However, this would strongly discourage users from storing pictures on the sidechain, as that would be an incredibly expensive storage rate.

  As another example, a token price of $0.01 will allow users to submit one kilobyte of data for just $0.01. This may still be adequate to discourage users from storing large high-definition pictures, but still be an acceptable price for storing smaller images.

  Token price should be set according to the intended use of the sidechain network. Token price can be changed by a sidechain administrator at any time.
- **Block Reward -** This is the price in US dollars to be paid to each miner as they solve blocks. The block reward will be paid in cryptocurrency, using the current rate conversions. Because each sidechain network is configured to complete one block per minute, the sidechain administrator(s) must consider how much they are willing to pay to keep the network online.

  For example, a block reward of $0.01 will cost the sidechain administrators approximately $0.60/hour, or $14.40/day, or $432/month. Depending on the purpose of the sidechain, that may be an appropriate amount, especially considering the sidechain administrators will also be selling tokens required to write data to the network.

  The block reward can be changed by administrators at any time. Administrators should take special care when calculating the block reward. A high block reward will encourage

miners from around the world to join the sidechain. Lowering the block reward could result in miners leaving the sidechain, committing their computing resources towards more profitable chains. A low block reward may deter miners from joining the network in the first place.

Another consideration is the rate of flow of data. If only one message is sent over the network on average per hour, then only one block will be created per hour. Empty blocks are not allowed. Sidechains with a low data flow will require fewer blocks, and will likely need a higher block reward to keep miners in the sidechain.