

```
import { MarketDataProvider } from '@providers/market-data/market-data';
import { SettingsDataProvider } from '@providers/settings-data/settings-data';

import lodash from 'lodash';

import { Network, Fees, TransactionDelegate, PrivateKey, TransactionType } from 'panacea-ts';

import { TranslateService } from '@ngx-translate/core';

import * as constants from '@app/app.constants';
import { PinCodeComponent } from '@components/pin-code/pin-code';
import { ConfirmTransactionComponent } from '@components/confirm-transaction/confirm-transaction';
import { Clipboard } from '@ionic-native/clipboard';
import { ToastProvider } from '@providers/toast/toast';
```

```
@IonicPage()
@Component({
  selector: 'page-wallet-dashboard',
  templateUrl: 'wallet-dashboard.html',
  providers: [Clipboard],
})
export class WalletDashboardPage implements OnInit, OnDestroy {

  @ViewChild(Content) content: Content;
  @ViewChild('pinCode') pinCode: PinCodeComponent;
  @ViewChild('confirmTransaction') confirmTransaction: ConfirmTransactionComponent;
```

```
public profile: Profile;
public network: Network;
public fees: Fees;
public wallet: Wallet;

public address: string;

public ticker: MarketTicker;
public marketHistory: MarketHistory;
public marketCurrency: MarketCurrency;

public onEnterPinCode;
private newDelegateName: string;
private newSecondPassphrase: string;
```

```
public emptyTransactions = false;
public minConfirmations = constants.WALLET_MIN_NUMBER_CONFIRMATIONS;
```

panacea



whitepaper

ver 2.0



ENG

Introduction

Blockchain has emerged as a potentially disruptive technology over the past ten years since the rise of Bitcoin.

The core concept of blockchain technology is that it creates a distributed ledger across a network of peers. This is called “Distributed Ledger Technology” (DLT).

Although DLT is still a fairly new technology, it has caught the attention of large corporations, banks, SMEs, and developers alike.

The Panacea Ecosystem will revolutionize DLT by providing a high throughput, low-cost solution for both enterprises and the general public. The Panacea Ecosystem will also have multiple real world applications, such as mobile and desktop wallets, a decentralized exchange, and a messaging system. We believe in building real world applications alongside a cutting-edge DLT solution.

Why is it a revolutionary idea?

Before Bitcoin and DLT, there was a traditional transaction structure - data was recorded, registered, and kept in a private database, usually owned and maintained by one entity. While this has worked in the past, it opens up potential security flaws, as well as the fact that one corporation can control potentially millions of records of sensitive data.

Blockchain fixes this issue by distributing the data across all nodes in the network.

This reduces the risk of data loss to essentially zero - since every node keeps a record of the chain, even if a node goes offline or its database is wiped, it can resync to its peers and get the latest version of the chain.

Blockchain is the “Next Internet”

Many people believe that blockchain technology will be as important as the rise of the Internet in the early 90's. This is because there are numerous applications for DLT across a wide range of sectors, including trade finance, healthcare, and real estate.

The immutability of the blockchain means that banks and other financial institutions can reduce fraud by having a paper trail for every transaction on their network.

Hospitals that are connected to a blockchain network can receive patient information in real time from peers all across the world, and real estate companies can verify ownership of deeds by verifying signatures using a blockchain ecosystem.

Another reason why blockchain technology is so powerful is that it is a true democratization of a network - anyone that participates in the network has a voice in how that network operates.

What is blockchain exactly?

A blockchain is a distributed ledger that is shared across all nodes on a network. This ledger is maintained by these nodes, and is immutable - this means that the data can never be altered once it is committed to the chain.

There are many of blockchains in existence as of this writing, with many being tailored to specific use cases. For example, one may be for music streaming, where users can commit music files to a blockchain, and users can read this data across the world.

Another is file storage, where users are paid tokens for letting users use their extra hard drive space on their computers.

Panacea

Panacea is a high throughput blockchain platform that uses DLT to create and support real world applications.

Written mostly in Javascript, Panacea will provide low blocktimes, high throughput of transactions, and an easy to use API that will allow developers to build on top of our chain. Panacea aims to utilize its blockchain technology in the real world.

What will Panacea do for the world of Blockchain?

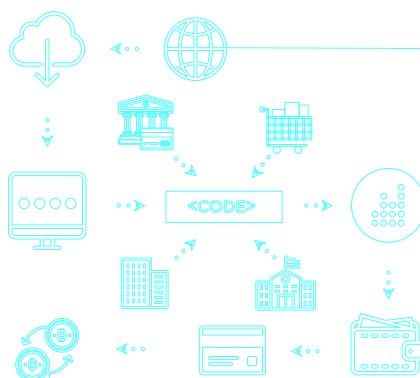
There are hundreds of new blockchains emerging all of the time, but these chains do not have any real-world applications built on top of them. Our aim is to provide real-world applications to everyday people, so that they can easily benefit from the power of Blockchain.

All-In-One Platform

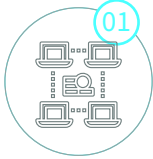
Panacea is building an entire blockchain platform - not just a chain, and not just for developers. Our main focus is to build applications powered by the distributed ledger for the public. Another focus is to make creating blockchains and applications extremely easy. The current barrier to entry for blockchain development is very high - there are not that many people that now how to write blockchain code. We will provide a way for the average developer who wants to use blockchain technology in their

application to use our platform with a few simple clicks of a mouse.

While we build this platform, we will continue to support local initiatives through partnerships with universities, meetups, and conferences. We want to educate and help foster adoption of blockchain technology to developers, hobbyists, or really anyone who will listen.



How it works



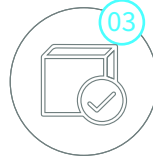
Transactions

Transaction is requested by users.



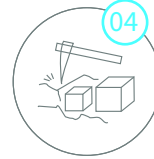
Broadcasting

Transactions are broadcast to all nodes in network.



Validation

All nodes verifies whether the transactions are valid. Once the majority of nodes confirms it is valid, transactions are now sent to forging delegate.



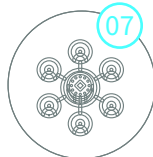
Forging

Forging delegate now turns the transactions into a new Block. Panacea process 1200 transactions per block.



Monitoring

All transactions, Block information, User IDs, delegates information are recorded and monitored in individual's wallet and also online explorer.



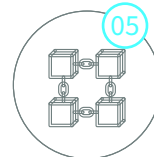
Share

Delegates propose to share their rewards & transaction fee with people who vote for them. In Panacea, this is built-in function in Panacea Wallet by smart contract algorithm.



Reward

Forging delegates are rewarded with "Reward-coin" for the service they provide to maintain the network.



Chaining

New block is added into the chain of blocks. It is now permanent and unalterable. Panacea adds new block in every 8 seconds.

Basic Terms



Node

Any devices (mostly PCs) that connect to the blockchain network is called a node.



Delegated POS

Not all nodes have authority to generate (forge) blocks. Only delegates who have "delegated authority" can generate the blocks.



Blockchain network

Nodes are all connected each other and create P2P blockchain network.



Voting

Delegates are elected by digital voting system. The top 81 delegates become forging nodes in the network.

B

Blockchain

The next question to ask is “why is blockchain even needed?”, and this can be explained with a few scenarios.

First, blockchain is needed because data siloing is generally a bad thing.

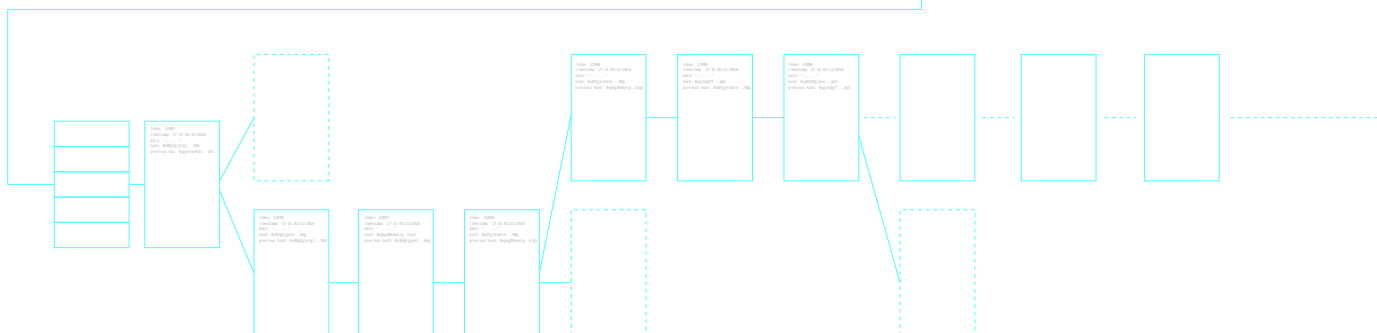
If there is ever a catastrophic failure, then all of this data is lost. If we use blockchain technology, then all of this data is replicated across each node in the network - even if a majority of the nodes were reset, they can resync to their peers and get the latest copy of the database.

Another reason why blockchain is needed is because blockchain allows trustless operations. What this means is that, even if you do not know who the other peer is, due to consensus algorithms, you can trust the data without necessarily trusting the peer. Think of a bank - why do you trust them? We are biased to think that the bank is the safest place to keep monetary assets and that there is no other replacement to hold our assets. People commonly believe that the money stored in a bank is safe and guaranteed. In most situations, this is true, but not 100%. In the United States, only \$250,000 is insured by federal government. For some countries, it is much less, while some countries do not even have this.

Now we have a general understanding of how a blockchain works, but why do blockchains exist?

Let's first understand how you interact with the non-blockchain world.

Blockchain provides massive advantages in dealing with four main aspects: Permission, Trust, Privacy, and Security.



Permission

Let's look at a bank, for example. In the non-blockchain world, you have some money - this money is yours, and you can do with it what you please. However, once you give your money to a bank, the dynamic changes. When you want to get your money out, the bank gives you permission to do this. If the bank did not want to give you your money, there isn't much you can do about it. This problem will likely never occur in the real world, but the threat remains: the bank has control of your funds and allows you access to it. When you ask the bank how much money you have with them and they tell you "\$100," you are also trusting the bank's word. You are assuming that when you go to withdraw the money, it is there in the first place. You are also trusting that the bank is not doing something irresponsible with your money.

One of the most important and fundamental aspects of blockchain is that only the party with the correct private key owns the asset - in other words, you actually control your funds because you have the private key to those funds. This is exactly the opposite of how the "real world" transacts today - in a blockchain driven world, you and only you can move funds or assets.

Trust

Keeping with the banking example, you trust the bank to keep your money safe and allow you access. This works well until the bank becomes a target of malicious parties - what if your money is lost, or your password is leaked? Blockchain technology allows for trustless consensus. This means that you don't need to know the party that you are transacting with - as long as consensus is reached, then the party can be trusted. Using this technology, two parties (e.g. you and your bank) can effectively transact without sharing any sensitive

data. This mitigates potential data loss by not even putting said data on the network.

Privacy

You are also expecting the bank to respect the privacy of your sensitive information. You are assuming the bank is not disclosing your sensitive information to third parties unless your contract with the bank states otherwise. Some corporations and institutions might take any opportunity to profit off of your data and information, provided it is within the law and the agreement between you and the organization. Many people legally agree to things without fully realizing what they are agreeing to. Using blockchain technology, you can see all of the transactions that happen on the ledger, due to the fact that it is public. Therefore, you can see if the bank is sharing your data with other parties, as they can only do so through the blockchain. This allows for greater transparency across all users of the network.

Security

Lastly, you are entrusting the bank to protect your money from criminals, hackers, and bad actors through various security measures. It is the bank's responsibility to make sure your money is safe, not yours. Although banks are sitting on decades of security technology advancements, massive hacks of major institutions do happen - namely, the Equifax hack of 2017 and others.

A blockchain's cryptographic nature provides the highest security available, provided the network is properly decentralized. Blockchains exist to "cut out the middle man", as some people view the middle man to be a possible point of vulnerability in these four key areas.

Blockchains are essentially distributed databases - every node on the network has a copy of the database. Due to the fact that this database is copied across multiple nodes, there is a need for consensus.

Therefore, consensus is a process where all of the nodes on the network agree to specific values on the blockchain.

Panacea Consensus Algorithm

Panacea uses Distributed Proof-Of-Stake (DPOS) as its underlying consensus algorithm. We chose this over others for a few reasons:

- Traditionally faster than Proof-of-Work (POW)
- Allows for a more “democratic” consensus (i.e. each node has one vote)
- More decentralized than others
- Proven consensus mechanism with many well-known chains using it in production

Panacea’s consensus algorithm is a decentralised governance, utilising 81 main nodes to run the network and validate all transactions. Every 8 seconds, all transactions are placed into a block and added to the blockchain if verified by these nodes. Each node verifies a block every 8 seconds. Each node’s position changes randomly each round, around every 7 minutes - this keeps the voting fair and not centralized like

we’ve seen on other PoW blockchains. There is a “2 Reward Token” block reward for the node that creates the block. This incentivizes users to run their own nodes to power the network. Using this consensus algorithm allows us to achieve faster confirmation times and lower transaction fees than almost every other chain on the market today.

Further about DPOS

DPOS is a consensus model that further enhances the benefits of POS. In this model, instead of individuals using wallet balances to determine whether their nodes forge blocks, a distributed collective of nodes called “delegates” control the ledger and validate the blocks. This opens doors to sizeable performance improvements, like transaction times, blockchain upgrade lead times, and block size modifications.

There is no limit to the number of delegates that can exist in a DPOS environment.

Each provides a valuable service by validating transactions, maintaining a copy of the ledger, and protecting the integrity of the data and the network. However, not all delegates are authorized to validate new blocks and add transactions to the ledger. In DPOS, only a select few have this authorization - they are called “forging delegates”. These delegates have the authorization to process transactions and add them to the ledger. However, to have a network used by so many to be controlled by so few goes against the decentralized nature of the blockchain concept itself. Because of this, all users of the network have a say in who is authorized to be a forging delegate, and who is not. This is done through a continuous voting process, which restores decentralization to the network.

Users of the blockchain who have wallets cast a vote for any delegate they choose, and the value of the users wallet is assigned as “weight” to the delegate. Due to the constant voting and unvoting of wallets, and transactions constantly moving between various wallets assigned to different delegates, the forging delegates are in a constant state of flux. It should be noted, though, that voting for a delegate does not send the wallet balance to the delegate nor does it lock up funds in some sort of escrow. The wallet holder is free to do as they wish with the funds while voting takes place. Moreover, votes remain active even when the user closes their wallet or shuts off their computer, as these votes are transactions on the chain.

Consensus & Voting Algorithm

As stated earlier, the Panacea blockchain uses Delegated Proof-Of-Stake (DPOS) as its consensus algorithm. We chose DPOS over other consensus algorithms due to its democratic nature and scalability.

DPOS works by using the concept of “delegates” to verify transactions, create new blocks, and achieve consensus. These delegates are “voted” in by members of the community. This means that any and every token holder has the same weight in terms of deciding who will become an active delegate - we believe that this system is the most decentralized possible, as there is no possibility of the system eventually becoming more centralized in the future.

```
var quorum = 0
noquorum = 0;

// For every node on the network, we will check and make sure that they are up to date
// Because we have a set block time, we do not need to wait for a block to be mined - rather it is "forged"
// Conditions for a vote of "Yes":
//
// 1. The peer must have the latest version of the blockchain
// 2. The peer must have the same "slot" (timestamp) for the chain
// 3. The peer must be allowed to create blocks
//
// Once a peer satisfies these conditions, they will vote "Yes" on creating the block
for (var i in network.peers) {
  var peer = network.peers[i];
  if (peer.height == lastBlock.height) {
    if (peer.blockheader.id == lastBlock.id && peer.currentSlot == currentSlot && peer.forgingAllowed) {
      quorum++
    } else {
      noquorum++
    }
  } else if (peer.height > lastBlock.height) {
    maxheight = peer.height;
    noquorum++
  } else if (lastBlock.height - peer.height < 3) {
    noquorum++
  }
}

if (quorum / (quorum + noquorum) > 0.66) {
  // We have reached consensus - let's create a new block
}
```

(panacea consensus)

Panacea is using DPOS as its consensus mechanism. In order for the network to reach consensus, there are some conditions that must be met:

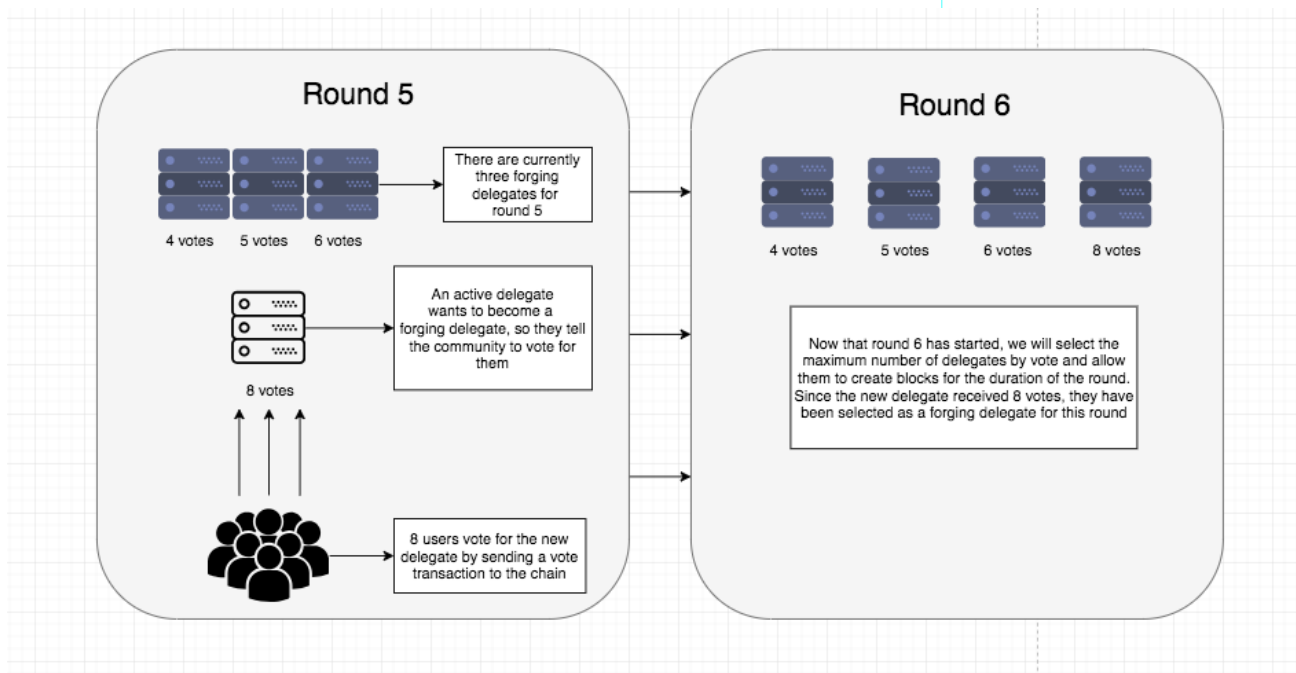
For every node on the network

1. The node must have the latest version of the blockchain
2. The node must have the same "slot" (timestamp) of the chain.

These two points are to make sure that the node is synced to the latest version of the chain

3. The node must be allowed to create blocks

New forging delegates are added by their peers voting for them. Members of the community can vote for delegates to become forging delegates at any time during rounds. Once a new round begins, we check which delegates have the most votes (up to the active delegate limit) and make them forging delegates. These delegates can now create blocks.



Above is an example of a voting round. There are currently three forging nodes that are in round 5. However, there is a new delegate that wishes to become a forging delegate.

Think of these new delegates as "campaigning" for their spot in the forging delegate section - delegates can talk to community members, post server specifications, and let them know how they will be supporting the chain. If enough community members vote for this delegate, then when the next round starts, that delegate will now become a forging delegate.

N Node

Node is one of the key concepts and drivers for entire blockchain platform, not only for Panacea but also others.

In this section we are going to talk about what types of nodes are on the Panacea Network.

Forging Node

Forging delegates are nodes on the network that have the ability to commit new blocks to the chain. These 81 nodes are chosen by a decentralised voting system where every PAN token holder has a voice to elect which nodes should validate transactions and run the network. The nodes that actively run the chain are called forging delegates. These nodes are voted on by the Panacea community - this means that any user has the ability to become a delegate node, which allows them to commit to the chain and earn PAN tokens.

Delegate Node

Delegate nodes are much like forging delegates, in that they have the ability to create new blocks. However, not all delegates are forging delegates. This is where rounds come into play. Voting rounds randomly select new delegates and make them forging delegates for a set number of blocks in the chain. To become a delegate, a user has to register a unique username on the Panacea chain and pay a fee in PAN. Once they are registered, the public community can vote on whether or not they want them to be a forging delegate.

Voting

Delegate Nodes ask for public votes quite similar to a political campaign. The node operator makes a proposal and the public holds them accountable to secure the network. Proposals can offer a wide variety of contributions, from creating a project to grow the ecosystem to sharing part of their earned block creation rewards.

By changing the forging delegates every set number of blocks, as well as allowing users to “vote” for the delegates that they wish to become forgers, the Panacea network is truly democratic and decentralized.

Roadmap

The Panacea team has a lot in store for the next 18 - 24 months. Below we are going to talk about some of the projects we are working on.

Panacea Explorer

Release : Version 2.1 November 2018

Every transactions, Block info, Delegates info, network status and every information about panacea's blockchain is broadcast online and users can access to this data whenever they want.

Desktop & Mobile Wallet

Release : Version 2.0 November 2018

We are currently in active development of the Panacea mobile and desktop wallets. This will allow users to send and receive PAN tokens, vote for delegates, and monitor basic information about the Panacea Chain, such as current block height, average number of transactions, and top delegates.

Panacea Desktop Portal

Release : Version 3.0, January 2019

Panacea Desktop Portal comes with every fundamental functions you need to enjoy panacea platform such as Manage ID and security passphrase, Access your assets (coin, token, digital assets, etc), Vote delegates, Profit share management, Deploy Smart Contract, Monitoring transactions and network.

Multi-tasking & Sub Delegates

Release : January 2019

The Panacea Chain will have a "subdelegate" system. This system rewards users that are delegates, but who have not been a forging delegate in some time. They are still maintaining the network - they just have not been selected to be a forger. Since we want as

many people to verify and run the chain as possible, we will reward a percentage of tokens distributed to forgers to these “sub-delegates” as well. Sub-delegates will be operating as safeguard for maintaining the network and also will be used to strengthen node securities.

Panacea will also operate with the concept “Multi-tasking Forging Delegates”. Forging delegates generate block every 8 seconds but each generates only 1 block in every 10min. To get the best efficiency, Panacea allows nodes (only for whom are approved by its working history) to participate multi-sidechains so that reduce unnecessary idle-time.

Reward & Profit Sharing

Release : January 2019

Not like other blockchain platforms, Panacea compensate the Nodes and Delegates with “Reward Coin”, not Platform coin itself.

This is to prevent coin volume inflation and also the coin price decrease. Currently, most of crypto-currency business companies distribute enormous amounts of coins for free or without taking the impact into the consideration which will cause devaluating the Investors and Stakeholder’s coin value.

Instead, the Panacea will compensate the “Reward coin” based on each participants’ contribution and the coin value will be determined according to the profit gained from this entire eco-system.

Crypto-Currency Lending Exchange

Release : Version 1.0, March 2019

Panacea is also on a way to develop the Crypto-Currency Exchange that provides a secure and user-friendly trading platform to trade not only the major coins such as BTC, ETH but also the altcoins. On top of this exchange platform, panacea provides Lending trade market which bridges lenders and borrowers with low commissions and transaction fees.

Digital Payment Gateway

Release : Version 1.0, June 2019

Panacea Digital Payment Gateway provides a blockchain-based payment solution (Mobile App, Digital card, Online payment solution) to Business, Merchants and Consumers. Panacea coin will be used as default digital token for payments. Panacea Payment Gateway will be the secure, fast and inexpensive payment solution all around the world.

Crypto-Currency Lending Exchange

We are currently in active development of a decentralized crypto-currency exchange powered by the Panacea chain. This exchange will allow users to exchange Panacea tokens for other forms of cryptocurrency. Not only will users be able to exchange cryptocurrency such as ETH and BTC, but our sidechain tokens as well.

On top of Decentralised Crypto-Currency exchange, Revolutionizing credit markets globally by facilitating safe, secure and regulated peer-to-peer [P2P] and institutional lending, that eliminates barriers to entry for household loan recipients such as limited collateral or lack of credit history while extending the capacity for lending institutions to transact higher volume, digital currency loans in a highly secure, regulated environment.

Panacea coin exchange lending is cryptocurrency lending service where a user can lend cryptocurrency for a certain period to Pananex by agreeing on the loan contract agreement. Upon expiration or termination of the agreement, Pananex will return cryptocurrency with annual % rate on top of it.

- ✓ Transaction Fee income from developing [Lending Smart Contract]
- ✓ Commissions from lenders and borrowers each month
(Charging certain portion of interest earned)
- ✓ Increases in Transaction volume and Deposit balance by injecting demand of lending into Pananex exchange.
- ✓ Promoting for the Trading volume increase and Transaction activation with Leverage Service.

Pananex is the crypto-currency lending exchange where customers enjoy leverage effect freely within his/her own collateral limit.

Pananex **Bridges** lenders and borrowers using smart contract and make profits from its interest, management and trading.

Pananex provides healthy leverage to all of our **Community.**

Pananex workflow

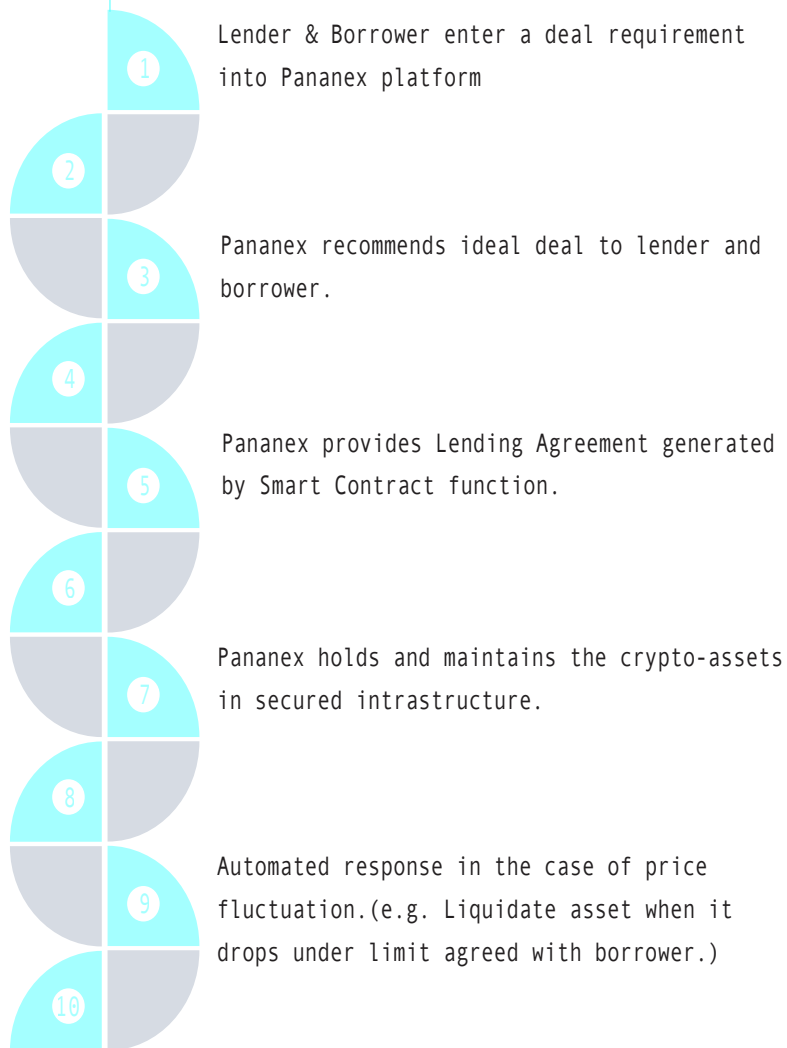
Pananex creates collateral auto-liquidating guideline based on Crypto-asset value and market forecast.

Clients select the most suitable deal for their own.

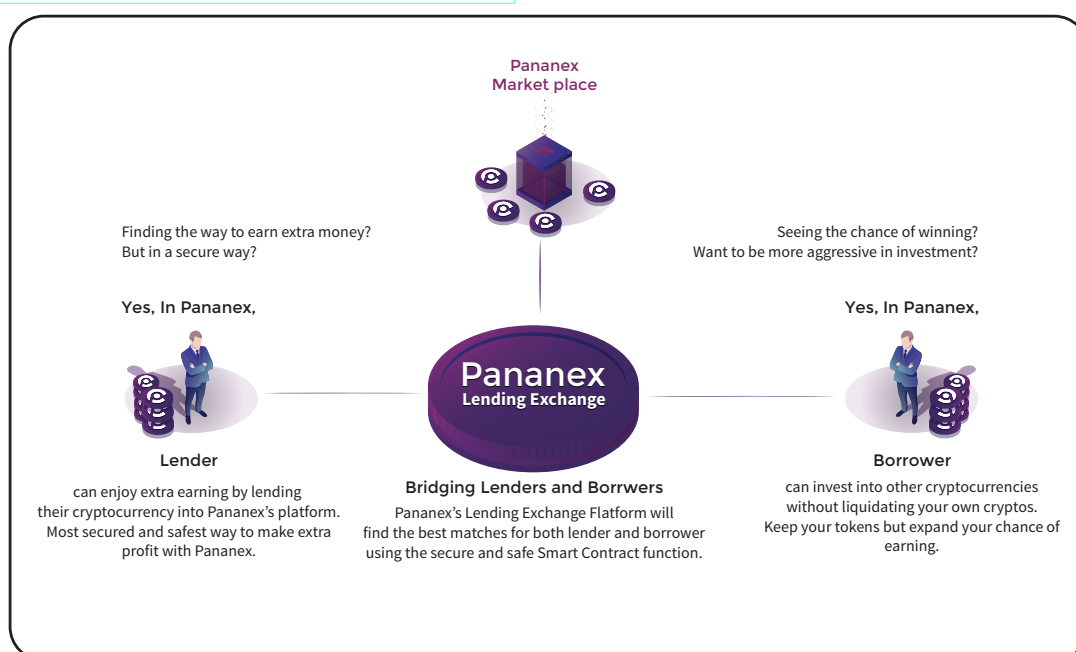
Lender and Borrower transfer its crypto-asset to Pananex account.

Charging related fees to each party and distributing to Stakeholders according to POT and POS algorithm.

Termination of Contract Pananex verifies contract condition and announces its termination. Crypto-assets are released to its origination.



Benefits of Lending Exchange



All of our products are secured using best encryption practices. We never store a users private keys, and all of our internet traffic is encrypted with AES-256 grade SSL.

Wallet Generation

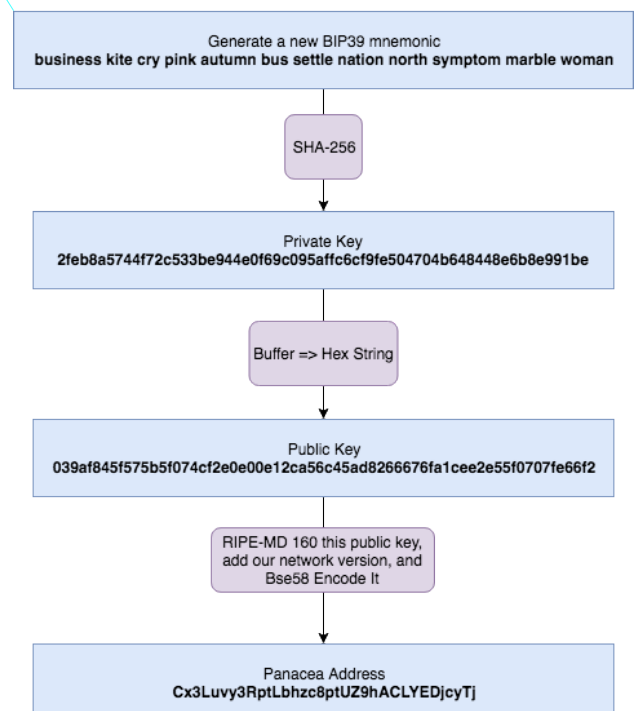
All Panacea wallets are derived from the BIP32 standard for Hierarchical Deterministic Wallets, as well as the BIP39 protocol for generating unique seed phrases. These seed phrases are used to derive a new wallet's keys. Panacea wallets follow standard elliptic curve cryptography (ECDSA) to generate these keys, as well as secp256k1 for defining the parameters on the elliptic curve.

First, we generate a 12 word seed phrase using the BIP39 protocol. Once we have this seed phrase, we take a SHA-256 hash of it. This hash is now the private key of the wallet.

In order for us to derive the public key, we need to take the base point of the elliptic curve G and tweak it using the newly generated private key in its integer representation. Once we have this tweaked value, we encode it and convert it into a hex string. This is the new wallet public key.

Finally, we need to derive the address by taking a RIPEMD-160 hash of the public key as a buffer. After adding our network version to this buffer, we run a standard Base58Check encoding to it. This will generate the Panacea Address.

Wallet Generation Process



Transaction Creation

Panacea transactions are simple to make and confirm very quickly. The following will detail how to create a transaction for the Panacea network and push it to the blockchain. First, we take the transaction data in bytes and SHA-256 hash it. Then we use the sender's keys to sign this hash, which is now the transaction ID. We store this signature in the new transaction and send it to one of the nodes on the Panacea network, where they validate signatures, timestamps, and amounts. Once all of the fields have been verified, the transaction is added to the memory pool and will be added to a block shortly.

A basic transaction structure is listed below:

```
{ type: 0,
  amount: 1000000000,
  fee: 5000000,
  recipientId: 'CvKdVCVLD6GGcursWLjTN1e15M7TprQid4',
  timestamp: 622594,
  asset: {},
  senderPublicKey: '02761a1c196dc9870c9802bea6b657bb85efcb2b9755f0e7a0f207622902c1c6eb',
  signature: '304402202668ec561e20ab41386b5dee7fa6891ed22310457d7a2cfa5be2-
feebd021bd8d022053e3e16054c073d2a0c8e3d2237cc7cef1ae08d186201b45e2470e567b0c90a6',
  id: '1b49e1e671ab0315d4086962e5a40cd90946c3179afb56d50c675a555f8b7ee1'
}
```

Explanation of the fields:

Type: This is an integer representation of what type of transaction is being pushed to the chain (payment, delegate registration, etc)

Amount: Integer representation of the amount of Panacea to send in its smallest denomination

Fee: The fee in Panacea for the transaction

Recipient ID: The recipient of the transaction

Timestamp: A timestamp for the transaction

Asset: Object with asset data of what asset is being transferred - defaults to an empty object if Panacea is being sent

Sender Public Key: The public key of the sender of the transaction

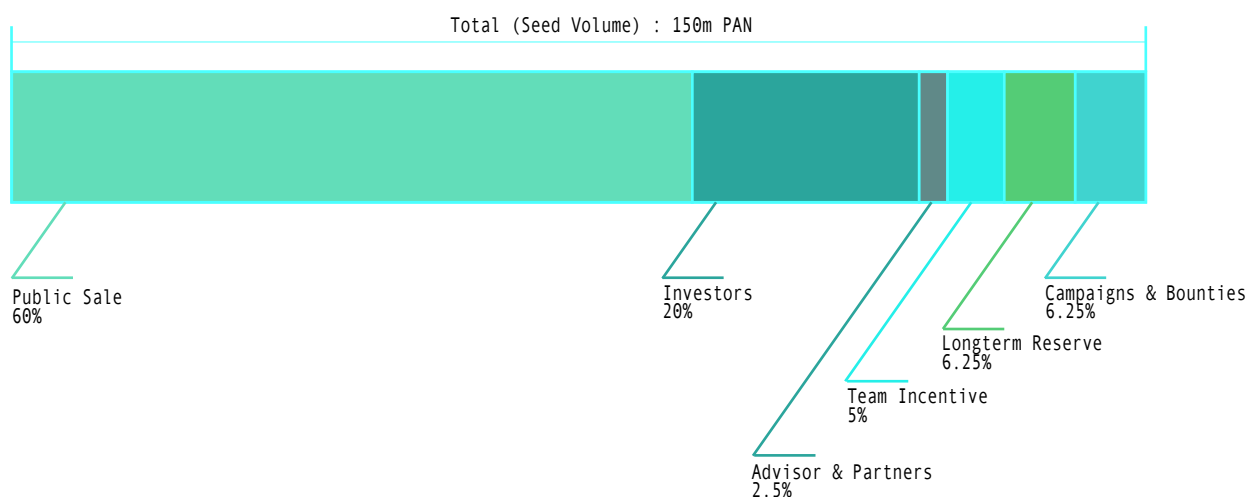
Signature: The ECDSA signature hash from the sender signing the transaction with their private key

ID: SHA-256 hash of the transaction

Distribution

Key factors of Coin sales and distribution plan are as below and all initial funds raised from public sale will be used mainly for Crypto-currency exchange, Payment gateway solution and further dapps & supporting program.

Token Distribution



Fund Distribution

