



# GoldStone

去中心化多链数字货币钱包

白皮书V1.0.0

## 摘要

区块链是一项新技术, 虽然已经在金融领域取得了令人赞许的成绩, 可把它推向更多的领域, 目前却还处于探索中. 对于广大普通用户来说, 理解和使用区块链相关的产品需要掌握的知识有很多, 这其中的操作对普通人群来说更是晦涩难懂. 我们期望能够利用我们的专业知识以及对大众人群的理解, 来打造一款简单易用又安全强大的区块链钱包产品帮助大家安全的保管资产, 便捷的交易资产。我们也会在严格的审核下为用户带来安全有用的第三方 DAPP。

GoldStone是在这一前提下产生的支持多链的去中心化钱包。GoldStone的使命是让更多的人可以便捷、安全的获取、保管和使用自己的数字货币。

GoldStone 目前支持比特币、以太坊、以太坊经典、EOS、莱特币, 及比特币现金链上的货币及Token管理。

# 目录

<b>摘要</b>	<b>2</b>
<b>目录</b>	<b>3</b>
<b>GoldStone钱包</b>	<b>4</b>
概述	4
GoldStone钱包的特点	5
同一身份管理跨链资产	5
完全BIP44钱包	6
使用私钥或Keystore管理	7
安全资产管理	9
开发者友好	9
GoldStone 说明	11
多链钱包结构	11
资产管理	13
市场相关功能	14
GoldStone 时间线	16
<b>GoldStone Token (GST) 通证</b>	<b>17</b>
<b>团队</b>	<b>18</b>
团队	18

# GoldStone钱包

## 概述

区块链是一项新技术, 虽然已经在金融领域取得了令人赞许的成绩, 可把它推向更多的领域, 目前却还处于探索中. 对于广大普通用户来说, 理解和使用区块链相关的产品需要掌握的知识有很多, 这其中的操作对普通人群来说更是晦涩难懂. 我们期望能够利用我们的专业知识以及对大众人群的理解, 来打造一款简单易用又安全强大的区块链钱包产品帮助大家安全的保管资产, 便捷的交易资产。

GoldStone 钱包是支持多链的去中心化钱包。GoldStone 支持比特币、以太坊、以太坊经典、EOS、莱特币, 及比特币现金链上的货币及Token管理。



图1 GoldStone钱包支持的链类型

## GoldStone钱包的特点

1. 使用同一个身份管理跨链资产
2. 链上资产去中心化管理
3. 开发者友好，支持测试链

### 同一身份管理跨链资产

每一条链都有自己的独有的使命, 他们是不兼容的, 如果你的资产分布在不同的区块链上, 那么GoldStone可以帮助你使用一个身份来进行管理。

- 只记忆一份私钥（或助记词）
- 所有币种一目了然

## 完全BIP44钱包



图2 GoldStone钱包使用1个助记词管理多链资产，及派生同一个链的多个账号的示意图

对于使用GoldStone钱包创建账户的用户，GoldStone默认使用助记词(BIP39) + BIP44 Path 的方式为用户生成每个链的公私钥。用户仅需记忆一份助记词，就可以直接管理各种链上的资产。

使用助记词钱包的用户，可以随时使用新的Path添加各链的子地址。

对于使用助记词导入其他钱包账户的用户，GoldStone支持使用自定义Path导入其以往钱包账户，并对导入后的钱包同样支持创建子地址的功能。

链	默认Path	默认新增子地址Path
比特币 Bitcoin	m' / 44' / 0 / 0 / 0	m' / 44' / 0 / 0 / n
莱特币 Litecoin	m' / 44' / 2 / 0 / 0	m' / 44' / 2 / 0 / n
以太坊 Ethereum	m' / 44' / 60 / 0 / 0	m' / 44' / 60 / 0 / n
以太坊经典 Ethereum Classic	m' / 44' / 61 / 0 / 0	m' / 44' / 61 / 0 / n
比特币现金 Bitcoin Cash	m' / 44' / 145 / 0 / 0	m' / 44' / 145 / 0 / n
EOS EOS	m' / 44' / 194 / 0 / 0	m' / 44' / 194 / 0 / n

表格1 GoldStone默认Path及默认的子地址Path

## 使用私钥或Keystore管理



图3 GoldStone钱包使用1私钥管理多链资产

对于使用单链的私钥或是Keystore文件导入账户的钱包，GoldStone采用将私钥转为WIF，再按各链规则生成各链公私钥对的方式来完成一个私钥（或keystore）管理多个链资产的功能。

对于这种私钥派生方式生成的多链钱包，用户记录其中任一链的私钥（或keystore），都可以恢复这一账户下的其他链资产。

这一类型的钱包不支持新增子地址的操作。



## 安全资产管理

### 用户资产处理完全去中心化

- 不存储明文私钥
- 编码与签名过程完全在本地完成，私钥不离开客户端
- 保证客户端在脱离自有节点后仍能正常运转
- 业务服务器与节点分离

### 赋予用户主动选择权

- 用户有主动选择节点与服务提供者的特权

### 多种加密加固手段

## 开发者友好

GoldStone对全部已经接入的脸均提供测试节点的全功能支持。并且在产品内嵌一键切换到测试网络的功能。

链	类别	名称
BTC[0]	主网	BTC主网
	测试网	测试网(Testnet3)
LTC[2]	主网	LTC主网

	测试网	测试网
ETH[60]	主网	ETH主网
	测试网	Ropsten测试网
		Rinkeby测试网
		Kovan测试网
ETC[61]	主网	ETC主网
	测试网	Morden测试网
BCH[145]	主网	BCH主网
	测试网	测试网
EOS[194]	主网	EOS主网
	测试网	Kylin测试网
		Jungle 2.0测试网

表格2 GoldStone钱包支持的各链网络

# GoldStone 说明

## 多链钱包结构

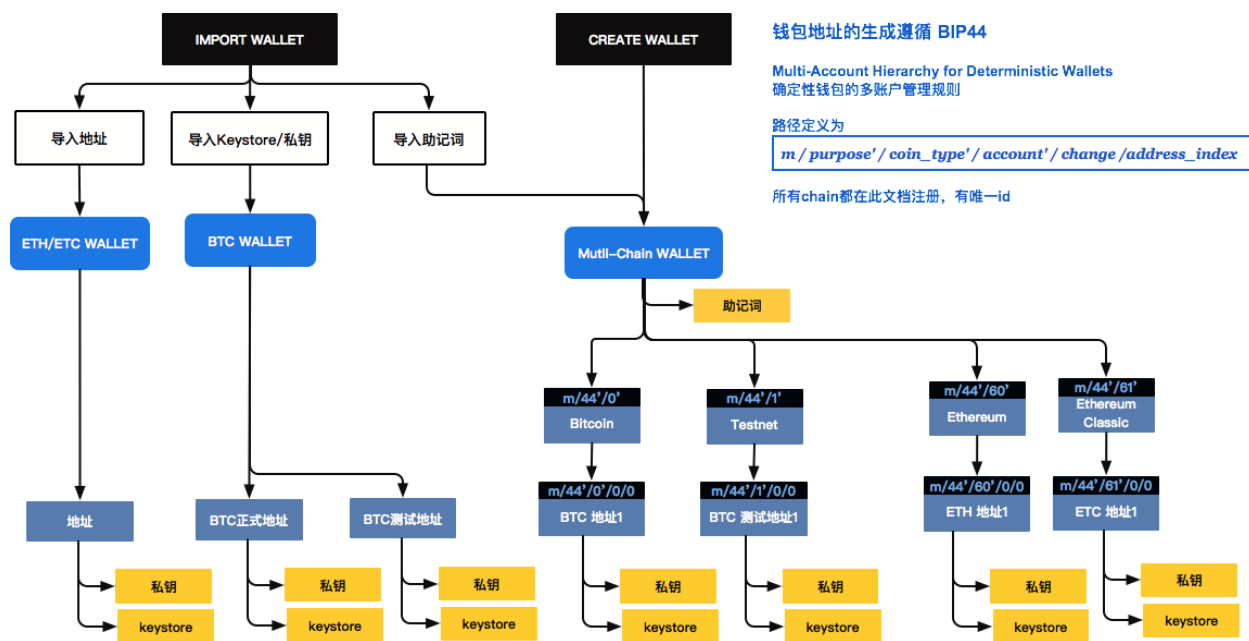


图4 GoldStone的多链钱包结构

GoldStone支持使用助记词、私钥或Keystore备份和导入账户。用户一旦导入GoldStone，每次需要调用私钥签名或转账时，用户使用密码或指纹（指纹授权功能针对可以获取指纹cipher的机型支持）即可进行授权。

私钥/助记词/Keystore不会以任何形式上传至网路，他们只在用户的客户端中使用，且客户端本地永远不会存储明文私钥与助忆口令。

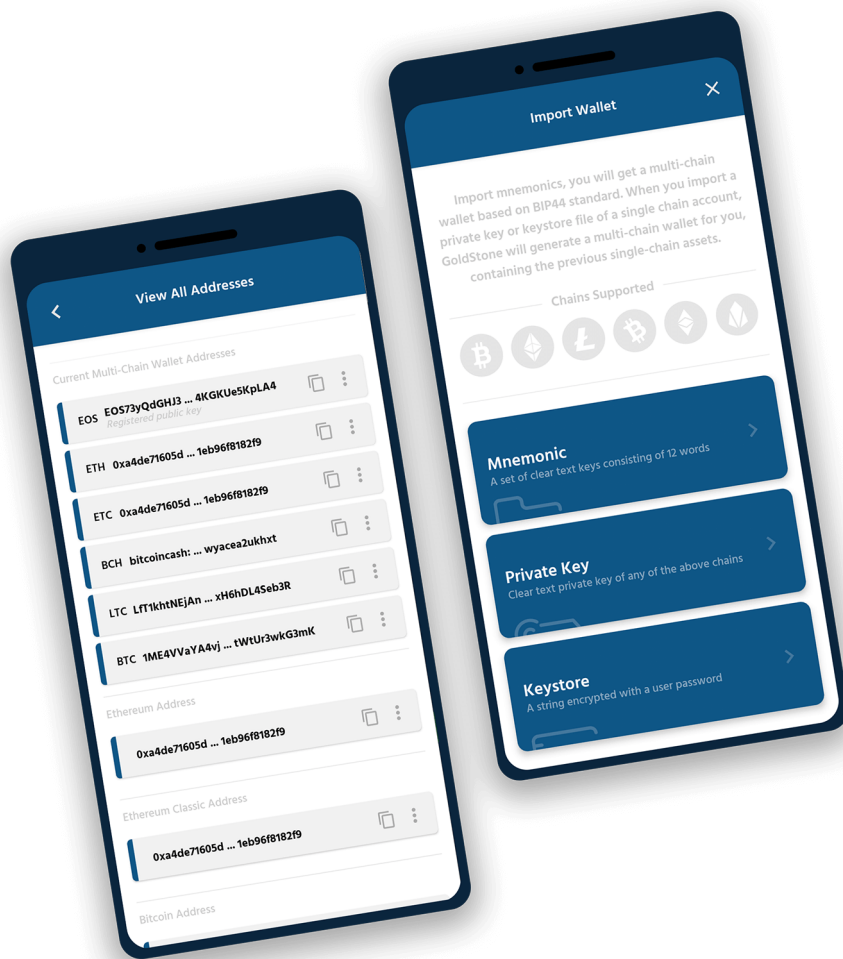


图5 GoldStone多链资产在一个账户中管理

用户使用GoldStone钱包，无需在各个链中切换，各个链的货币及Token都可以在同一个界面中展示及管理。

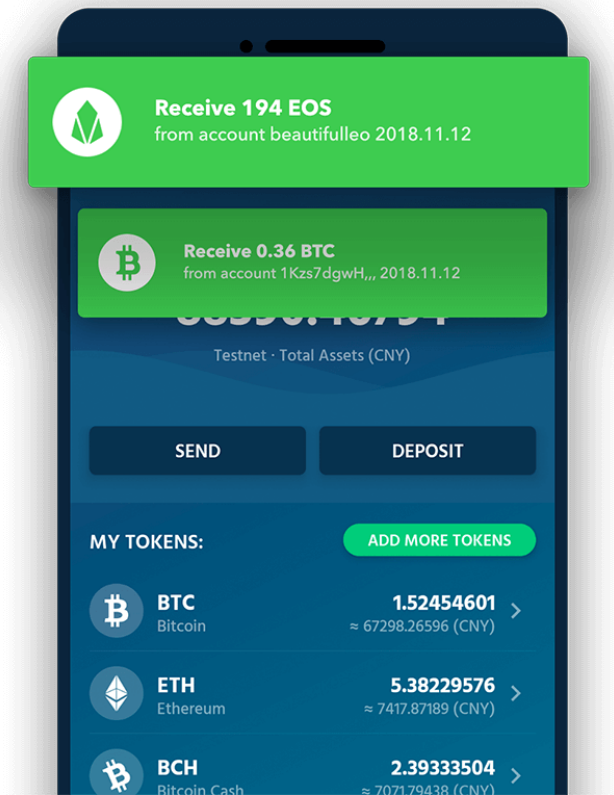


图6 GoldStone钱包各链资产在同一个界面管理与展示

## 资产管理

GoldStone提供如下资产管理功能

1. 创建全新的账户 (遵循BIP 44标准)

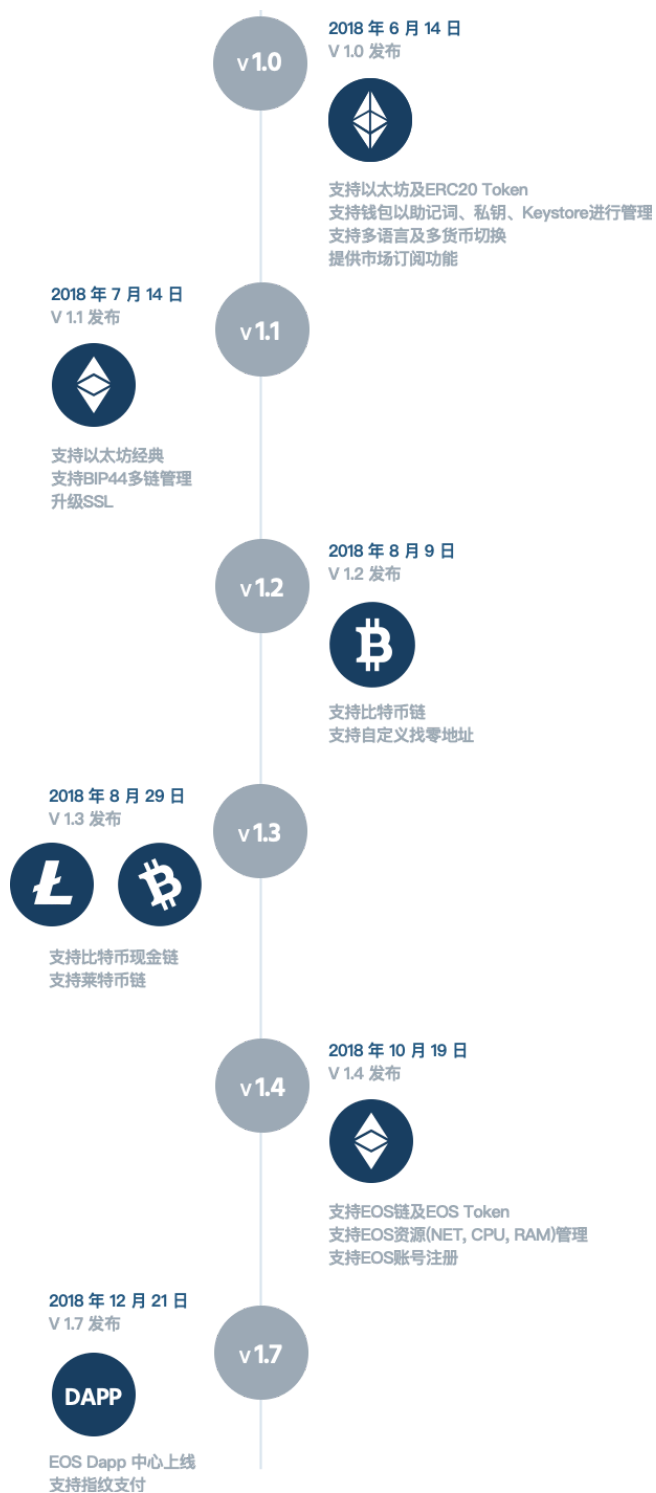
2. 通过明文私钥 / 助记词 / Keystore的方式导入已有账户
3. 仅通过地址或EOS账户名导入一个用于观察余额与实时转账消息的观察钱包
4. 查看钱包账户内的BTC、ETH、EOS、ETC、LTC、BCH 以及所有ERC20 Token币的余额、进行转账，并查看账单详情。
5. 管理EOS NET/CPU/RAM资源，进行租赁、赎回与买卖内存操作。支持资源租赁与撤回租赁的管理操作。
6. 提供转账燃气费的智能建议
7. 内置Dapp 中心，可以无缝使用EOS Dapp并便捷安全的进行钱包支付。（兼容Scatter，可使用Scatter支付的所有Dapp均可以用GoldStone访问）

## 市场相关功能

1. 为用户计算您钱包内所有资产的当下估值，支持数十种货币转换。
2. 支持添加并展示各大虚拟币交易市场中的价格走势，现已支持火币、币安、Okex、Bitfinex、FCoin等市场。
3. 提供市场币与token的实时市值排行榜。



# GoldStone 时间线



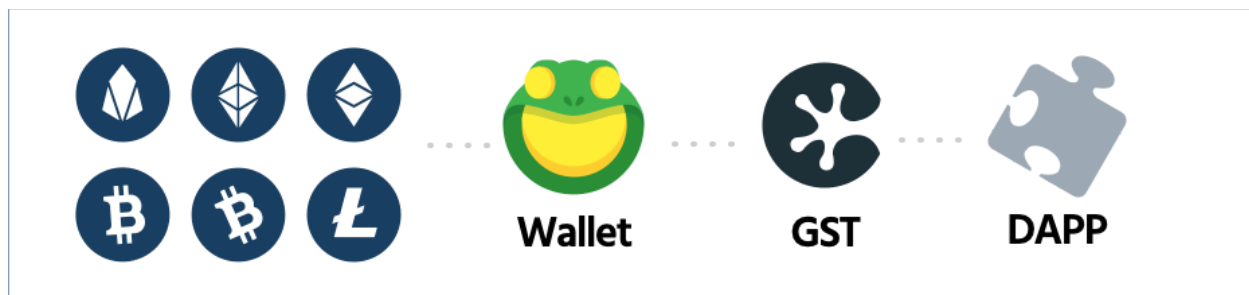




## GoldStone Token (GST) 通证

区块链是开放、包容、透明的共享体系。GoldStone钱包将助力

GoldStone钱包GoldStone Token (GST) 通证将用于GoldStone用户激励体系及优质Dapp开发者激励政策。



GST的总发行量：10000000000

GST的流通量：100000000

## 团队

### 团队

我们专注于区块链技术的研发, 在数字加密货币钱包, Ethereum 及 EOS 智能合约开发上有独到的见解和经验. 我们一直在孜孜不倦的追求生产出完全的去中心化的 DAPP。

我们相信区块链这项技术可以被广泛的应用在各个领域, 它所独有的可溯源以及信任机制会大大的提高机构乃至全世界的生产协作效率. 同时我们也坚信作为一款便捷安全的数字加密货币钱包所承载的不仅仅是安全的保管用户的财产, 同时也是链接个体与区块链的纽带. 为此我们将孜孜不倦的完善和打磨我们的产品。