ColoredChain Whitepaper

Version 0.3.0

Sep, 2015

Authors

Adam Miller, Andrew Hamlin, Samiran Ferrin

Table of content

i. Introduction

1. What is Coloredchain

ColoreChain is a fully new blockchain applications framework including many creative features and functions with powered proof of stake consensus algorithm.

With coloredchain, developers and users can create decentralized applications on their own sidechains easily through 3 level dapps deployment framework,such as colored tokens platform,custom smart contracts,name system, voting, decentralized storage,and many other dapps.

No ming,no inflation,lightweight,and it's well suitable to run nodes on most devices with trim feature,including VPS,PC,even smartphone and raspberry pi.

2. What are the core creative innovations

Powered Proof of Stake Coloredchain uses virtual powered proof of stake mining to secure the p2p network,no special mining equipment required,no mining cost,no inflation,environment friendly;

Masterchain and Sidechains The masterchain and sidechains architecture provides more flexible,scalable,clear framework to develop and deploy applications easily.

Decentralized Application Framework Coloredchain will build in 3 level framework for developing,deploying and using decentralized applications.

- Modularized toolkit for developing DApps.

- Colored Vitual Machine(CVM) to provide a runtime environment for DApps.

- Plugin kit for installing DApps.

Trim The Masterchain and Sidechains architecture allows to trim transactions of sidechains,and dramatically decreases the size of blockchain database, solves the float problem,makes it possible to run nodes on most mobile devices,like smartphone,raspberry pi and internet of thing(IOT) hardware.

3. Vision

Coloredchain aims to be a public blockchain applications platform with many creative features and scalability.

And with more decentralized applications built on coloredchain ,such as colored token platform ,the first dapp built in coloredchain,which expects to be used by financial area for issuing and trading digital assets, shares, forex,precious metals,oils,and so on.

And with decentralized application framework,many other dapps can be easily created and deployed,like smart contracts,name system,voting system, decentralized storage system,message,lottery,and so on, all of these will make blockchain ecosystem more colorful!

And with flexibility, scalability and lightweight,coloredchain will also be one of the best solutions for internet of thing(IOT) economy area.

ii. Consensus Algorithm and Tech Specification

1. Powered Proof of Stake

ColoredChain adopts a virtual Proof of Power(PoW) consensus named Powered Proof of Stake(PPoS),aims to be a efficient,light,environment friendly system.

1) Virtual Proof of Power

Every token in coloredchain(masterchain) will have power to secure the p2p network like mining in bitcoin,but no need special equipments for this virtual mining.The power is proportional to amount of tokens.

No inflation,'miners' can only mint for transaction fees.

2) Power Transfer

Every token has power of securing network,and the power can also be leased to other nodes to secure the network during a period of time without sending tokens to others.

So this will let those who can not run nodes lend their power to other online nodes to secure network without sending their tokens to others, trustless and no security risk.

The more tokens participates for 'ming', the more secure p2p network will be.

3) Anti-Nothing at Stake

There will be some counterparty economic disincentivizes to prevent potential attacks,such as'Nothing at Stake',even though N@S is not really a threat to system due to many different forks existed at some time but no one can really compete with masterchain.

If the nodes tries to fork masterchain,it will lose power of tokens temporarily ,or be punished for some money(tokens) to miners as fees.

2. Total Supply Amount

Total amount of coloredchain tokens is 100 million,fixed,no inflation.

All tokens are distributed in genesis block one time.

3. Mint

There will be no inflation in coloredchain system.The total amount of tokens is fixed,so nodes can only collect transaction fees during process of securing network.The process of protecting network and collecting fees is named mint.

4. Block Time

Block time will be around 30 seconds both for masterchain and sidechains.

5. Fee

Transactions will have a dynamic transaction fee structure,and the system will automatically recommend the transaction fees according to transaction type and speed.Users can also set them manually.

The fee on masterchain will be denominated by masterchain tokens. Fee on sidechains will be denominated by meta tokens of each sidechain respectively.

Masterchain tokens and sidechains tokens can be converted with internal exchange at a market driven price at any time.

iii. Core Features

1. Powered Proof of Stake

Coloredchain uses Powered Proof of Stake(PPoS) consensus mechanism as virtual proof of power to secure network.

Every token in coloredchain masterchain will have power to secure the p2p network like mining in bitcoin,but no need special equipments for this virtual mining process. And the power is proportional to amount of tokens.

No inflation,’miners’ can only mint for transaction fees.

Efficient,lightweight,secure,environment friendly.

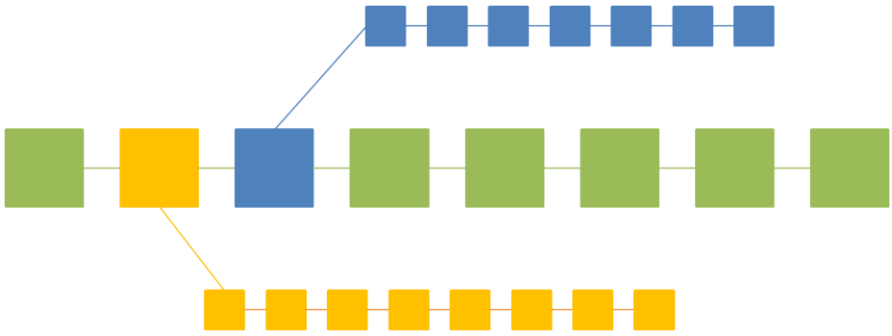
2. Sidechains

Coloredchain uses masterchain and sidechains architecture to provide a more flexible,scalable platform to users and developers.

The masterchain will only manage one type transaction,coloredchain token transfer.And the tokens on masterchain will only have one function,secure the network.

All other transactions and applications will be existed on sidechains. Anyone can easily launch their own sidechains at any time.

All sidechains will have their own meta tokens.The transaction fees on sidechains will be denominated by their own meta tokens.Tokens of sidechains will not have the power/responsibility to secure network.



The transactions on sidechains can be submitted to masterchain on demand based,that is,when there are transactions needed on sidechain, these transactions will be submitted to nodes of masterchain to get confirmed.If there are no transactions,there will be no blocks created on sidechains.This can also decrease the blockchain database size, improve efficiency.

Blocks of masterchain will be generated around 30 seconds all the time.

Sidechains blocks time is also 30 seconds if continuously generated.

3. Decentralized Applications Framework

Coloredchain will provide a 3 level decentralized application deployment framework for users to develop and deploy their decentralized application on sidechains easily.

1) Colored Virtual Machine(CVM)

Coloredchain system will build in a virtual machine(CVM) to provide a runtime environment for decentralized applications,such as custom smart contracts, name system, voting system, decentralized storage system,message,lottery,and so on.

All these applications will run in CVM.

2) DApps Development Toolkit

Coloredchain will build in a decentralized applications development toolkit for developers to create application as easily as possible.

The tool kit will be modularized, can be called easily,and will also provide implementation references for most functions.

3) DApps Install Plugin Kit

Users can easily install these decentralized applications developed by third

parties through Plugin Kit ,and use these wonderful apps to launch their business.

4) DApps Case:Colored Token Platform

As a use case,coloredchain will deploy the first decentralized application,Colored Token Platform.Users,companies and banks can build gateways to form a global trading with any assets,such as Bitcoin,Ethereum,other crypto currencies, precious metals, shares,forex,oil,and so on.

No single point failure,totally transparent,almost real-time,fully decentralized,solid secure.

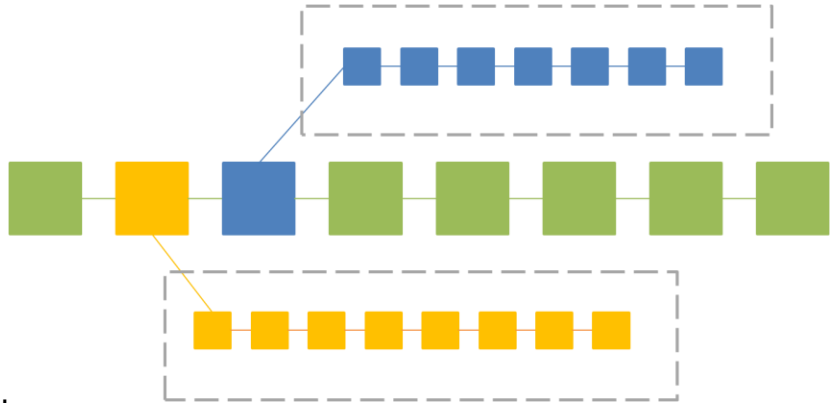
4. Trim

The Masterchain and sidechains architecture allows to trim transactions on sidechains without any potential risk.

All transactions on sidechains will be trimed periodically,and only save the hash of snapshot on blockchain.

Trim of masterchain will not happen frequently,and because of

masterchain only including one type transaction as mentioned above,this will not float blockchain much.And if there is need to trim masterchain, hardfork will be a option.



.

Trim will decrease size of blockchain database dramatically,make it possible to run coloredchain nodes on most devices,like smartphone,raspberry pi,let alone VPS,PC.And this lightweight feature will make coloredchain suitable well for internet of things(IOT) economy space.

Another,lightweight will let run nodes on mobile device more suitably and easily,make coloredchain nodes more decentralized and network more secure.

5. Other planned features

- **Multisignature** - m of n signature for special transaction with custom m and n.
- **Mixer** - a mixed pool run all time with fixed input and output for privacy.
- **Archived nodes bounty** - incentive for nodes to back up pruned data.
- **Voting** - Decentralized transparent voting and voting lease.
- **Name** - Decentralized domain name system and account name.
- **Data stream** - Date communication.
- **Colored tokens direct trading pair** - Direct exchange between colored

tokens without involving meta token.

• **Online Wallet** – Web online wallet

iv. References

[1]. Proof of Stake wiki https://en.bitcoin.it/wiki/Proof_of_Stake

[2]. Bitcoin Whitepaper https://www.bitcoin.org/bitcoin.pdf

[3]. Blockstream Sidechain https://www.blockstream.com/sidechains.pdf

[4]. Factom Whitepaper https://github.com/FactomProject/FactomDocs/blob/master/Factom_Whitepaper.pdf

[5]. David Johnston. Decentralized Applications

https://github.com/DavidJohnstonCEO/DecentralizedApplications/blob/master/README.md

[6]. NXT Whitepaper https://nxtwiki.org/wiki/Whitepaper:NxtBitcoin

[7]. Proof of Stake: How I Learned to Love Weak Subjectivity

https://blog.ethereum.org/2014/11/25/proof-stake-learned-love-weak-subjectivity/

[8]. Slasher: A Punitive Proof-of-Stake Algorithm

https://blog.ethereum.org/2014/01/15/slasher-a-punitive-proof-of-stake-algorithm/

[9]. Formalizing distributed consensus

https://docs.google.com/document/d/13_FSQ1Koq8uLvqTaSvZdb6OT2SpUZZq53vFiiDQj4qM/edit#

[10]. How to Vote Privately Using Bitcoin http://eprint.iacr.org/2015/1007.pdf

[11].Two-Factor Authentication for the Bitcoin Protocol

http://link.springer.com/chapter/10.1007/978-3-319-24858-5_10

[12].Open Asset Protocol

https://github.com/OpenAssets/open-assets-protocol