YUC

WHITEPAPER

A DECENTRALIZED DATA EXCHANGE CHAIN PROVIDED BY YUC

TABLE OF CONTENTS

0、Abstract

Nothing in this white paper constitutes legal, financial, busy or tax advice, and you should refer to your own legal, financial or tax advice. Tax or other professional consultants should know the relevant information before engaging in any activities related to this.

This white paper is intended for general reference only and does not include a prospectus, offer document, securities offer, ipo or any offer to sell any product, project or asset (whether digital or otherwise). The following information may not be exhaustive and does not imply anything about the contractual relationship. There is no warranty or warranty as to the accuracy or completeness of such information, and no warranty or promise is given or appears to be given as to the accuracy or completeness of such information. This white paper includes information obtained from third party sources, and the foundation and/or certification teams do not independently verify the accuracy or completion of such information. This blank paper may be time deducted and outdated, and the foundation is not obligated to update or correct this document.

The white paper can be translated into languages other than English if there is a conflict or ambiguity between the English version and the translated version. English shall prevail. You acknowledge that you have read and understood the English version of the blank sheet of paper.

No part of this white paper shall be reproduced, reproduced, distributed or disseminated in any manner without the foundation's prior written consent.

1、INTRODUCTION

Bitcoin was developed and released in 2009 in response to inherent flaws in the way Internet transactions are handled. Businesses on the Internet rely almost entirely on financial institutions acting as trusted third parties to handle electronic payments, Mr Nakamoto explained in his white paper. While the system works well in most transactions, its model still has inherent flaws in the trust-based model. Since its birth in 2009, bitcoin has been

rapidly adopted by today's modern markets. What are the main problems with bitcoin right now? Its rapid adoption is an increase in the need for the original blockchain to handle large transactions of varying degrees. As demand increases, the transaction waiting period increases, leading to an increase in transaction costs that try to accelerate the transaction validation time.

The core innovation behind bitcoin is its decentralized structure. Unlike traditional fiat currencies, bitcoin has no central control, no central information warehouse, no central management, and no center of failure. One of the challenges for bitcoin, however, is that most of the actual electronic services and e-commerce built around the bitcoin ecosystem are centralized. Because of the current system's centrality, e-commerce is run by individuals in specific locations that leverage vulnerable computer systems and are vulnerable to legal disputes. Because of its consistent commitment, YUC is one of today's truly decentralized currencies built on the core of bitcoin while bringing a new layer of anonymity to fruition.

2、PROLOGUE

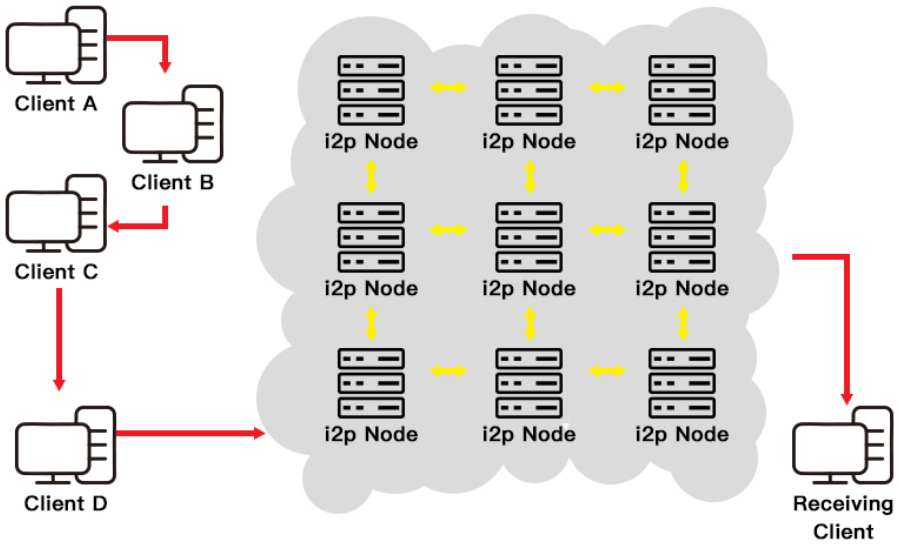
YUC uses a decentralized network design that is an IP obfuscation service that can communicate anonymously over a layered circuit-based network. Direct Internet traffic through a free global volunteer network of more than 7,000 relays to hide a user's location and usage without letting anyone conduct network surveillance or traffic analysis. And enable these continuators to complete calculations quickly (using shorter block times, requiring only a small number of blocks as "confirmations"), provide predictable performance (by keeping the time between confirmations about the same), and increase computing and storage capacity without limit as demand for their services increases. These protocols must be secure to control a critical percentage of their nodes, must generate cryptographic randomness, and must remain decentralized in nature, as its size increases to millions of nodes. YUC is achieved by encrypting the application layer of the communication protocol stack, and the nested layer is similar to the onion layer. The data, including the next node destination IP, is encrypted multiple times and sent via

virtual circuits that include continuous random selection of relays. Each relay only decrypts the packet wrapper enough to know which relay is coming from, and which relay sends the data to the next one. The relay then repackages the package in a new wrapper and sends it. The final relay decrypts the innermost encryption layer and sends the raw data to its destination without revealing or even knowing the source IP address. Since each hop of communication routing in the YUC decentralized network is partially hidden, this method eliminates any single point in communication nodes that depends on knowing the communication source and destination.

3、I2P Integration

I2P was originally designed to provide hidden services that allow people to host servers in unknown locations. I2P offers many of the same benefits as YUC. Both allow anonymous access to online content, use peer-to-peer style routing structures, and both use hierarchical encryption. However, I2P is designed as a network within the Internet, with traffic contained within its boundaries. I2P performs grouping based routing, not circuit based routing. This provides the benefits of allowing I2P to dynamically route around congestion and service interrupts in a manner similar to Internet IP routing. This provides higher reliability and redundancy for the network itself.

Figure 2.1
How an i2p Transaction Occurs

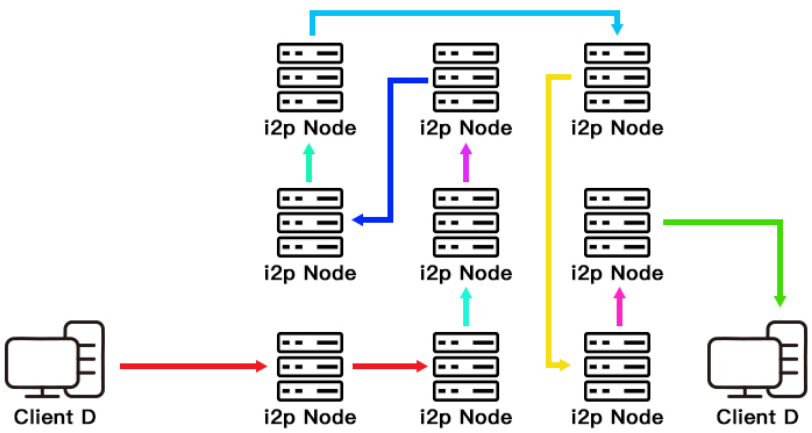


When a user first wants to contact another user, they query the fully distributed "network database" - a custom structured distributed hash table (DHT) based on the Kademlia algorithm. This is done in order to efficiently find inbound tunnels for other users, but the subsequent data between them usually contains this information, so no further network database lookup is required.

I2P is a highly confusing tunnel service that USES IPv 6 to anonymously all YUC data sent over the network. Each client application has their I2P "router" built several inbound and outbound "tunnels" - a sequence of peers that pass data in one direction. In turn, when the client wants to send YUC data to another client, the application sends a message through one of the outbound tunnels of one of the inbound tunnels to the other client, eventually reaching the destination.

I2P USES two distributed hash tables to coordinate network state, rather than relying on a centralized set of directory servers. A distributed hash table or DHT is a distributed, often decentralized mechanism for associating hash values with content. The main advantage of DHT is their scalability. A successful decentralized P2P network requires good scalability of its services to ensure that the scale of content or transaction sharing continues to grow as needed. In addition, I2P does not rely on trusted directory services to obtain routing information. Instead, network routing is dynamically formed and constantly updated, with each router constantly evaluating other routers. Finally, I2P establishes two separate simplex tunnels to communicate with each host network to form a single duplex decentralized network map.

Figure 1.1
How an YUC Transaction Occurs



4、YUC Wallet

The advantages of YUC wallet are fast, simple and low resource utilization. It USES secure remote servers to handle the most complex parts of the YUC network, and allows users to recover their wallets with a secret seed phrase. YUC also provides an easy-to-use cold storage solution. This allows users to store all or part of a distributed digital currency offline.

YUC supports multiple signatures, which require multiple keys to authorize YUC transactions. A standard transaction on an edge network can be called a single-signature transaction, because the transfer requires only one signature -- from the owner of the private key associated with the YUC address. In YUC transactions that support multiple signatures, multiple signatures are required before transfers are made. YUC then needs to provide multiple different square addresses for any processing.

Here's an example:

One electronic wallet is on your home computer, the other is on your smartphone - the digital currency cannot be used without the signatures of both devices. Therefore, attackers must access both devices to steal your digital currency.

5、Multi-Algorithm Support

YUC is a multi-algorithmic cryptocurrency designed to give equal access to digital currencies to people with different types of mining equipment. It is the only cryptocurrency that supports five hash functions on a blockchain. This increases safety, and a wider range of people and equipment can be mined to ensure that everyone is equally allocated to the digital currency. The total supply of YUC is 27,400,0000. What makes YUC stand out from other cryptocurrencies is the five validation algorithms running on its blockchain: Scrypt, X17, Lyra2rev2, myr-groestl and blake2s. All five algorithms have a block target block time of 30 seconds. The difficulty is only affected by the hash rate of the algorithm. Improved security and protection against 51% attacks.

6、YUC ISSUANCE PLAN

YUC is based on Ethernet fang ERC20 standard digital currency, a circulation of 27400000 pieces, of which 50% is produced by mining, mining the initial amount, 2000000, the initial offering price of 2.35 $, development teams hold YUC digital currency 30%, hold some will lock in 1 year, then will be lifted within 24 months monthly geometric, held by a team of digital currency is mainly used for technology research and development of distributed data exchange chain/network security/money a few pieces of content.

ASSIGNED PROJECT	PROPORTION	NUMBER OF COINS
development team	30%	8220，0000
contributors	10%	2740，0000
private	10%	2740，0000
Mining	50%	13700，0000

7、Android YUC+I2P

YUC is at the forefront of innovation in mobile cryptocurrencies. We pioneered two very unique android wallets, one for the Onion Router and one for the Internet project (i2P). Both wallets are built on anonymity. The wallet has no built-in functionality and cannot connect or broadcast user information through Clearnet. The transaction was made through simple payment verification (SPV), a technique described by Satoshi Nakamoto. A ticket that allows a wallet to verify a transaction by including a proof to verify that a particular transaction is contained in one block, rather than downloading the whole block.

The SPV allows near-instant payment confirmation because it ACTS as a shortened version of the wallet, requiring only the download bulk, which is much smaller than the full block. The wallet also has built-in security features, such as 4-bit passwords and biometric lock options, to add a physical security layer.

In addition, wallet can also process P2P qr code scanning transactions through instant verification.

8、P2P Platform-Integrated Portals

P2P is an online technology that allows users to transfer money via the Internet or mobile devices. To do this, the user USES an online application or, in this case, bot to specify the number of digital currencies to be transferred. The receiver is specified by its user name only, and once the sender initiates the transmission, the receiver will be notified of the use of the online robot. He received a sum at a newly established deposit address. The user can then send a message to the robot via a simple command. They are then given a set of instructions on how to receive the newly acquired address. This service does not require any additional information beyond the amount you want to send and to whom. In this process, IP address, location, name and other private information are not retained. The initial transaction beyond your personal identity is still completely anonymous.

YUC is one of the only cryptocurrencies to offer P2P solutions currently available, which apply to disagree, Twitter and Internet relay chat (IRC), and Reddit, Slack and Steam will offer support in the future. These P2P products allow users to transfer YUC to anyone who is on the same social platform as them.

9、Wraith Protocol

The Wraith protocol makes it possible for the first time in cryptocurrency history to choose between public or private ledger accounts while remaining anonymous in both cases. With this innovative new system, users who value transparency and accountability, such as merchants, can choose to view transactions on the blockchain. On the other hand, it also offers an option for those who want the deal to disappear entirely. The Wraith protocol allows full anonymity for maintenance while providing a safe and reliable way to send and receive digital currencies, and transactions are untraceable on public ledger accounts. The updates include stealth addressing and the latest SSL integration, which will take our core QT users out of clearnet and migrate them to the latest YUC network.

It also includes the ability to specify that a user wishes to make transactions through a public or private ledger. With convenient simplicity, the Wraith protocol update will allow the user to switch a switch in the core QT wallet, which allows the

user to trade through an additional IP confusion layer secret addressing over the YUC network.

What are the key protocols?

A key negotiation scheme is a process in which two or more users negotiate a value from which two or more users can then get one or more keys for symmetric encryption. Neither party can fully determine the key values. Instead, they all contribute to the ultimate critical value, and most importantly, no one watching the exchange can tell the final outcome. Note that the basic form of key protocol schemes is anonymous, and they do not tell either party the identity of the other.

The original Diffie-Hellman key protocol scheme was based on multiplying integers with a large prime number, especially Numbers larger than 1 and smaller than p, where p is a large prime number. ECDH is a similar scheme based on point addition on elliptic curves.

What is the difie-hellman algorithm?

In both scenarios, the basic operations are combined to create an original function called a keyed function. The way the function works. A keyed one-way function is a function that takes two inputs and produces one output. Considering the two inputs, the calculated output must be straightforward. However, you can only use other inputs and outputs to compute keys, which is not computationally feasible. In this way, both parties can use their private keys without leaking them to anyone, either the other or the eavesdroppers.

What is the Elliptic-curve Diffie-Hellman?

ECDH is a variant of the difie-hellman algorithm for elliptic curves. This is a key protocol protocol, meaning the ECDH defines how keys are generated and exchanged between parties. How these keys are used to encrypt data is up to us. EDCH is implemented to solve the following problems:

Both sides want to exchange information securely so that third parties can intercept them, but may not be able to decode them.

Here's how they work:

1. Anthony and Billy generate their own private and public keys. We have private key *dA* and public key *HA=dAG* to Anthony, key *dB* and *HB=dBG* to

Billy. Note that Anthony and Billy use the same *G* basis points on the same elliptic curve in the same finite domain.

2, Anthony and Billy exchange their public keys *HA* and *HB* through an unsafe channel. The middle man intercepts *HA* and *HB*, but can't find *dA* and *dB* without solving the discrete logarithm problem.

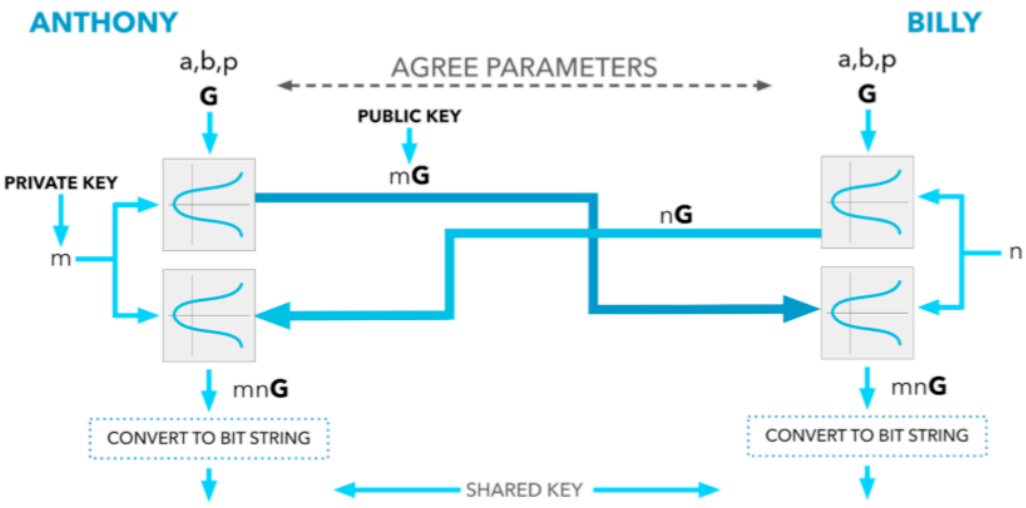
3. Anthony calculates *S=dAHB*(with his own private key), and Billy calculates *S=dBHA* (with his own private key and Anthony's public key). Note that actually Anthony and Billy's *S* are the same:

S = dAHB = dA(dBG)= dB(dAG)= dBHA

However, the middle person knows only *HA* and *HB*(and other domain parameters) and cannot find the Shared secret.

In our particular example, both Anthony and Billy must agree to the transaction parameters a, b, p, and g before the agreement begins or the transaction begins in this case. For Anthony, this is m, and Billy, this is n, and then each of them multiplies their private key by base point G to form a new point that represents their public key. On the elliptic curve remember that every point is made up of x coordinates and y coordinates.

Then Anthony and Billy exchange their public key and multiply it by another public key generated by their own private key. This creates a new point, which is the same for each side. It's just going to convert this point into a bit string that's suitable for use as a key.



What is invisible addressing?

Implicit addressing allows the sender to create an unlimited number of one-time target addresses on behalf of the receiver, without requiring any interaction between the parties. These addresses can only be restored and used by the receiving party and cannot be publicly linked to the sender or receiver address distributed from it. This is achieved through a cryptographic system called an elliptic curve, or more specifically, an elliptic curve difie - hellman(ECDH for short) in this case. The ECDH works by allowing any two individuals who know each other to work on the public key so that it can calculate a Shared public key that no one else can copy or link to either party. Because of the unique cryptographic nature of the ECDH algorithm, the Shared key cannot be reverse-engineered to reach the sender or receiver address.

Main mode of reception

1、The public address cannot be contacted with the original public address;

2、Do not link to any other one-time address;

3、Only the recipients can link their payments;

4、Only the recipient can issue the key associated with the one-time address;

Implicit addresses enhance the one-time public key of user privacy in each transaction by allowing user generation, automatically generating and recording who can use output in future transactions. By effectively allowing users to make transactions outside the publicly visible blockchain, the implicit address prevents the output from being associated with the wallet address. Outside observers can't tell whether money is being transferred from one user to another, nor can they link wallet addresses together just by looking for transactions on the blockchain.

YUC + SSL Integration

Previously, our CoreQT wallet let our users trade through clearnet. With the Wraith protocol, we migrate all QT users from clearnet to YUC. Still, our QT wallet will no longer be able to connect to any network outside the YUC network, which will help ensure that our users remain anonymous. YUC is a

decentralized system that allows users to connect through the relay network, which confuses user IP address information by randomly jumping from one node to another, effectively eliminating any information tracking. Our YUC integration also includes SSL encryption, which establishes a secure and encrypted link between wallets to ensure that all data passed between wallets remains private and complete. SSL encryption also ensures that data from one wallet to another is not intercepted or modified.

10、Wraith Protocol Use Case

See Jessica. As a nursing student about to graduate, money is often tight and access to mobility is vital. Recently, she used her credit card on shopping online. Unfortunately, her credit card number was stolen at her own fault to buy a luxury handbag in Perth. Although her credit card company agreed to reimburse her, her new card won't arrive for several days. After this experience, she knew that financial security was her own responsibility. She knew she could use the YUC and Wraith protocol to make payments to her favorite e-commerce store via Coinpayments, and guaranteed that her payments would not be stopped or tampered with in any way. She can do business without fear of theft and know her financial fate is in her own hands.

11、Atomic Swaps

Atomic cross-chain trading, also known as Atomic cross-chain trading, allows YUC and all other cryptocurrencies in circulation to interoperate with each other while supporting Atomic swap capabilities. The way the atomic exchange works is the same as the way the user trades different cryptocurrencies by allowing the user to cross-trade without relying on centralized parties. YUC will implement the BIP65 check lock time validation (CLTV), also known as the hash lock contract (HTLC). HTLC is a payment method that USES hash locks and time locks, which requires the payer to confirm receipt of the payment before the deadline by generating an encrypted payment certificate, or to return the payment to the payer by waiving the ability to claim payment. For example, both parties commit their respective transactions to

the appropriate blockchain. User A sends YUC on the border blockchain, and user B sends ETH on the blockchain. The receiver can declare the transaction only by revealing a secret hash (proof of payment). This leads to both transactions being connected to each other, although they occur on two different blockchains. If the payee does not disclose their secret hash - payment then confiscates and returns the payer.

Our users will be able to take advantage of the atomic exchange while transacting across the YUC network through the ghost protocol, thus maintaining IP aliasing and personal identity integrity while sending and receiving edges through cross-chain transactions. In addition, this implementation not only allows for cross-chain transactions, but also paves the way for future implementations, such as the Lightning network, which will allow for automatic execution of cross-chain transactions and transactions.

12、Bloom Filters: BIP37

BIP37 is the primary filter used by SPV clients to speed up transaction processing by requesting only matching transactions and merkle blocks from the full node. This BIP adds new support for peer-to-peer protocols that allow peer nodes to reduce the amount of transaction data they are sending. Peers can set filters for each connection after the release handshake is complete. A Bloom filter defined as transaction-derived data. Bloom filter is a probabilistic data structure that allows test set membership - they may have false positives, but they will not have false negatives.

13、Future Development: YUC Smart Contracts

Rootstock, or RSK as it's commonly known, is a bidirectional fixed side chain that grafts the smart contract function onto the edge network. It also introduced a non-chain protocol for near-instant payments. RSK is a separate blockchain that does not have its own token and relies instead on existing tokens (such as YUC). RSK can do this by binding (or matching) its smart token to YUC, so the value of the RSK token is exactly the same as the value of the YUC token. Users are free to move tokens back and forth between the two chains.

14、Contributors

As an open source project, we find it very important to thank our contributors for helping us get to where we are today.

Thanks to the following contributors:

@JtheLizzard @lucklight @Cryptonator92 @feyziozsahin @Slemicek @Trilla6six6 @Dabbie USA @Cyrus7at Buzztiaan @Thehunter9 @Crypth