



BITE

BitEthereum White Paper

Value Transfer + Asset Issuance and Management = BitEthereum

Table of Content

| | |
|---|-----------|
| Abstract | 3 |
| Chapter 1 Design Philosophy | 4 |
| 1. Development motivation | 4 |
| 2. Development direction | 4 |
| 3. BitEthereum Token Giveaway Campaign..... | 5 |
| Chapter 2 Technical Details..... | 6 |
| 1. Use of token..... | 6 |
| 2. Graphene toolkit | 6 |
| 3. Platform model..... | 7 |
| 4. Asset issuer and user authentication | 8 |
| 5. User roles and community governance | 9 |
| 6. Free Transactions | 11 |
| 7. Asset dividend payout..... | 12 |
| 8. Token asset alliance..... | 13 |
| 9. Improved token asset payment..... | 13 |
| 10. Business-friendly SDK and independent user interface..... | 16 |
| Chapter 3 Development Route | 17 |
| 1. Development blueprint..... | 17 |
| 2. Support for third-party developers..... | 17 |

Abstract

BitEthereum is created to address the inability of Bitcoin to provide advanced crypto token asset issuance, management and circulation and the slow transfer speed of Bitcoin and Ethereum blockchain. BitEthereum's mission is becoming the bridge between corporates, users and businesses. And its goal is to create a well-developed ecosystem of crypto token assets that addresses the current problems in Bitcoin and Ethereum. BitEthereum also enables user authentication, automated asset dividend payout and alliance formation. And also introduced zero transaction fee feature. Besides, BitEthereum is provided with an easy-to-use advanced payment system. Meanwhile, to enrich BitEthereum's ecosystem, we offer a more advanced and convenient third-party software development kit (SDK) so that third-party developers and corporate users can give full play to BitEthereum in application development.

Chapter 1 Design Philosophy

1. Development motivation

Currently, Bitcoin can only handle up to 7 transactions per second, Ethereum can only handle up to 30 transactions per second. Slow transfer speed and difficult-to-use user interfaces make it difficult for general public to accept blockchain-based applications, and also making it difficult for merchants to apply blockchain technology to their businesses.

BitEthereum can easily solve these problems. And more applications can be constructed to satisfy the market demands for token asset management and utilization.

2. Development direction

During preliminary development, it is expected to complete the basic structure so that BitEthereum can fulfill zero transaction fee, user authentication, token asset issuance and management, alliance formation and other fundamental functions and provide service for small and medium-sized merchants. Subsequently, the token asset payment and circulation functions will be optimized to strengthen its capabilities and attract larger merchants. In the coming future, automated asset dividend payout and advanced token asset management functions will be developed to serve other industries.

3. BitEthereum Token Giveaway Campaign

1. The total supply of BitEthereum Token(BITE) is 100 million, 99% of BITE tokens will be distributed to the BTC, ETH token holders. All BTC holders can claim a total of 66 million BITE tokens, and all ETH holders can claim 33 million BITE tokens.

The team will take a snapshot of the BTC and ETH blockchain at 00:00 on December 21, 2017 (GMT+8) . The snapshot will record the token balances of all BTC and ETH accounts at that time.

The snapshot requires that the address with balance $BTC \geq 0.1$ and $ETH \geq 1$.

2. Claim: The team will release BitEthereum wallet in mid-January 2018, and token holders of BTC and ETH can claim their BITE tokens by submitting the BTC / ETH address's signature to the BitEthereum blockchain after installing the BitEthereum wallet. When user submits signature on BitEthereum wallet, BITE token will be automatically distributed to his BitEthereum account.

3. Calculation: To get a sense of the token giveaway math, take John as an example: John owns 10 bitcoins, At time of snapshot, the total amount of bitcoin circulation supply is 16748650. Since all BTC holders can claim a total of 66 million BITE tokens, so John can claim $10/16748650 * 66000000 = 39.40616$ BITE tokens.

4. BitEthereum blockchain network set the giveaway campaign deadline for March 21, 2018.

Chapter 2 Technical Details

1. Use of token

BitEthereum Token (BITE) is the basic system token that can be used to:

1. Pay transaction fees arising from issuance of assets;
2. Pay deposits for issuance of assets;
3. Contribute to or maintain fee pools;
4. Generate bandwidth for the zero transaction fee feature.

2. Graphene toolkit

BitEthereum will build a blockchain bottom layer with the Graphene toolkit--which is a real-time blockchain development kit characterized in its high performance, high concurrency and low latency. The Graphene toolkit is originally an underlying development framework for use with the BitShares blockchain. Daniel Larimer created BitShares in 2013, aiming to set up an ideal free market financial system (IFMFS). Through continuous improvement, BitShares has maintained stable operation for years. It enables fast transaction confirmation at the average speed of 1.5s and efficient multi-transaction processing (3,300 transactions per second). There are several successful Graphene toolkit-based blockchain products in the market, such as STEEMIT, YOYOW and EOS.

Graphene toolkit is provided with development libraries of consensus algorithm, networking, user management, databases, block formats and blockchain file storage. Since the Graphene toolkit is developed for the blockchain-based distributed digital asset exchange BitShares 2.0, it

requires comprehensive restructuring of the Graphene toolkit in consensus algorithm, user authentication and other aspects before it apply to BitEthereum. With years of experience in Graphene toolkit and BitShares development, our development team is in a position to make highly customized modifications and improvements to the Graphene toolkit to underpin the construction of BitEthereum.

3. Platform model

| | |
|--------------------------|--------------------------|
| Software Development Kit | UNIVERSAL USER INTERFACE |
| BitEthereum Core | |
| Graphene Toolkits | |

BitEthereum is mainly composed of three layers:

The bottom layer consists of the Graphene toolkit to provide underlying blockchain service. The Graphene toolkit allows fast transaction confirmation at the average speed of 1.5s and efficient multi-transaction processing (3,300 transactions per second). It is a high- performance and low-lag underlying blockchain platform.

BitEthereum Core, as implied by its name, is the core layer, as well as the intermediate layer of BitEthereum. It is mainly designed for communication with the Graphene toolkit to implement the underlying service logic.

The service layer is on the top and encapsulates the software development kit and universal user interface.

4. Asset issuer and user authentication

Authentication is an important function of the system. Considering that there will be a large number of business users, universal criteria and compliance should be addressed when designing the function. Authentication is not compulsory but optional. High-value business users may unlock the function when forming a point alliance with business partners or seeking approaches to enhance their images and credit standing among users.

To ensure the system's authoritativeness and tamper-resistant property to the greatest extent, the development team takes the practical application into full consideration when designing the system. In terms of user authentication, the public key infrastructure (PKI) technology will be applied to BitEthereum and the PKI-based X.509 certificate standards will be integrated into the Graphene toolkit for development.

For instance, Verisign, as a certificate authority (CA) that has obtained the WebTrust international certification and receives recurring audit, also implements the X.509 certificate policy. There are dozens of CAs in the market using the same standard and policy. Hence, it can be directly applied to user authentication and digital certificate distribution. The detailed procedures are given as follows:

1. There is a credible CA Keystore under the Committee's management, which includes root certificate public keys of CAs. The Committee is in charge of regular inspection and review of the reliability of these CAs. Should the Committee find any questionable or incredible CAs in the Keystore, it shall be entitled to revoke the root certificates of such CAs.
2. Users are required to pass the verification (at least Class 2 verification) according to the standard verification procedure provided by relevant CAs.
3. CAs are responsible for distribution of user certificates and private keys.
4. Users to back up their private keys safe and secure.
5. As to key operations, except for verifying login credential, the system also require to verifying the certificate issued by CAs.
6. The system's consensus module verify the submitted data and signature data with system's internal Keystore.

5. User roles and community governance

Committee: The Committee is the core of BitEthereum's governing structure. The BitEthereum Committee has X members and each shall be elected by BITE holders. The voting weight of every BITE holder shall be determined by the proportion of its holdings to the total system capacity.

The Committee is mainly responsible for:

1. Adjusting system fee rates of processing registration, transfer and bandwidth generation ratio;
2. Reviewing proposals on developer remunerations and system improvement;
3. Managing the internal CA Keystore.

Witness: Witnesses are also elected by BITE holders according to the same voting weight calculation method as that of Committee member election. Witnesses are mainly responsible for processing transactions, packing them into blocks and transmitting them to other witnesses for confirmation. BITEs will be granted to the witnesses who have participated in transaction processing at regular intervals.

Ordinary user: Ordinary users refer to asset holders. Every ordinary user is provided with a unique identity and the right of holding different assets. Because the system offers zero transaction fee feature, generally, ordinary users will not be charged for transaction or other day-to-day operations.

Asset issuer and manager: Asset issuers and managers are allowed to issue customized assets. Upon registration, they are required to pay a specified registration fee. To increase credit standing, they may optionally submit a certain amount of deposit and pass verification. Issuance fee is required in case of issuing assets.

Asset issuers and managers are given the following authorities to:

1. Pay registration fees for users;
2. Lock deposits to obtain bandwidth;
3. Issue customized assets;
4. Specify the bandwidth available for users to respectively transfer issuers' assets per day

Third-party developer: BitEthereum will provide third-party developers with APIs so that they can develop more applications and further improve the BitEthereum ecosystem.

6. Free Transactions

Free Transactions is one of BitEthereum's core functions. In daily life, no transaction fees will be charged when users receive or pay for token assets. To our knowledge, blockchain is a value network that requires witnesses/block producers to process transactions. Considering the cost of running witness nodes, it is expected to generate profits from these witness nodes to maintain sustainable operation. Therefore, it is not deniable that financial incentives play an essential role in the construction of BitEthereum. However, from an ordinary user's perspective, for no reason would an ordinary user be attracted by a system charging transaction fees.

Hence, a set of free transaction functions have been introduced to BitEthereum: The "bandwidth" generated from the pledged tokens of an asset issuer and manager in the system is used to pay the transaction fees arising from transfers during issuance of assets. Example:

Assumed that there is a Merchant A who has issued point assets: Point A, with 100 BITEs having been pledged by Merchant A to the system when creating the assets and three users--User 1, 2 and 3, are holding the point assets,

100 bandwidth will be generated from the pledged BITEs on a daily basis. If BitEthereum charges 10 bandwidth for each transaction, the three users holding Point A can pay transaction fees with

the bandwidth generated from Merchant A's pledged BITEs when they enter into payment/transactions with Point A.

However, it is likely to bring about misuse of service. In the example above, if User 1 conducts 10 transactions during the day, it will cost all of the 100 bandwidth indirectly provided by Merchant

A, which compromises User 2 and 3's rights to enjoy the free transaction service in the same day.

To solve this problem, BitEthereum will enable Merchant A to set a limit on the number of daily free transactions per holder. For instance, Merchant A may require every Point A holder to use the free transaction function for no more than three times a day.

7. Asset dividend payout

In addition to the general bonus point assets, asset issuers and managers also demand for issuance of token assets featuring in dividend payout.

There is no decentralized blockchain system for asset management that enables automated dividend payout. To fulfill similar functions, the existing systems may require a centralized facility to carry out snapshot operations on a specific date and complete dividend payout manually. These operations are not desirable and will not be applied to BitEthereum.

Instead, BitEthereum will be equipped with a smart contract-driven automated asset dividend function. Details are given as follows:

1. Asset issuers and managers declare a dividend payout plan.
2. Asset issuers and managers specify the dates and time of ex-dividend and payout, enter the value of dividend per share into smart contract and lock the assets for dividend payout into the system.
3. When it reaches the block following the date of payout, the smart contract will automatically transfer the locked assets for dividend payout to the accounts who are holding the assets prior to the ex-dividend date.

8. Token asset alliance

Asset issuers and managers may form an asset alliance by entering into a smart contract, in which case, users can exchange assets issued by different asset issuers and managers of the alliance at a fixed exchange rate. Considering BitEthereum's transfer and asset circulation functions, it is necessary to establish a pegged asset exchange rate regime. Otherwise, the alliance is probably faced with violent asset exchange rate turbulence that goes against the original purpose of establishing the alliance. To overcome this problem, BitEthereum provides fee pools at pegged exchange rates for alliances.

9. Improved token asset payment

An advanced Graphene toolkit-based payment notification model and an optimized transaction identification function have been put forward:

A special functional field for identifying and tracking transaction sources has been added to the block format. The data structure of the field is as follows:

Advanced/primary mode + separator + additional data

In the primary mode, order information (e.g. branch identification number and order number) should be included in the additional data to realize simple payment confirmation, as shown in the following example:

1. A branch endpoint uses date and time, identification number, transaction amount and GUID algorithm-based order number to generate a QR code for transfer.
2. Users can enter into transfer transactions by scanning the QR code.
3. The branch can use an observation wallet to check the transaction records of the master account and the additional transaction data contained in the special functional field for identifying and tracking transaction sources. Absolute matching indicates a successful transaction.

In the advanced mode, each branch endpoint requires a key (the key is irrelevant to the account). An branch endpoint can use the key for encryption of all transaction information and add it to the additional data. The advanced mode provides superior order notification and order confirmation functions, as shown in the example below:

1. branch endpoints use their keys to connect to the master endpoint through reliable and secure off-chain P2P encrypted communication channels.
2. branch endpoints submit order data through encrypted channels.

3. The master endpoint generates order numbers and sends them to the corresponding branch endpoints.
4. branch endpoints use their keys for encryption of order numbers.
5. branch endpoints generate QR codes and payment links for transfer purpose from the master account addresses, transfer amount and encrypted order numbers.
6. Users implement transfer operations.
7. branch endpoints or master endpoint can observe the master account transaction records, decrypt the additional data (i.e., the encrypted order numbers) and check the consistency between the transaction records, additional data and the submitted order data. Absolute matching represents a successful transfer.

The primary mode is applicable to the merchants who only demand for simple transaction confirmation functions whereas the advanced mode is suitable for online payment (e.g. transactions in demand for instant payment notification) and those require master endpoints to process transactions or have stricter transaction confirmation requirements. Also, the advanced mode allows encrypted off-chained P2P communication between branch endpoints with their keys and the corresponding master endpoints for information transfer, superior order data confirmation and submission. Meanwhile, in order to maximize the fund security level, branch endpoints have no privilege to employ the funds in the master account.

10. Business-friendly SDK and independent user interface

Except for APIs, BitEthereum also provides third-party developers with a complete SDK so that they can efficiently develop BitEthereum-based asset issuance and management systems.

On the other hand, BitEthereum's universal user interface wallet is a fully functioning universal blockchain wallet and blockchain explorer. Since some business users may want to have a name-brand wallet, in the future, BitEthereum will release Wizard customized wallet generation programs so that merchants even without development capabilities can have their own asset issuance and management systems that facilitate brand building.

Chapter 3 Development Route

1. Development blueprint

Launched in December 2017, BitEthereum expects to release its first version prior to January 2018, on April 2018 the version with token asset issuance and management and verification will be released . The SDK, asset dividend payout, alliance formation, asset circulation and other functions are anticipated to go live in June 2018, with more applications coming soon.

2. Support for third-party developers

To pursue sustainable development, diverse applications and application contexts should be continuously introduced to BitEthereum. To this end, BitEthereum, upon release, will offer third-party developers a series of APIs for the purpose of development.