BFchain White Paper

An Encrypted Application Oriented Digital Currency Ecosystem

(Revised)

Background

Today's hype surrounding cryptocurrencies and blockchain technologies rivals the dot-com bubble in the 90s. After years of development, their decentralized design, fault tolerance, anti-attack, and anti-collusion encryption have been generally recognized by the public. Ethereum, a version 2.0 blockchain technology, is not just a digital currency but also a blockchain-based platform with many features. It features smart contracts, the Ethereum Virtual Machine (EVM), and its currency, Ether, for peer-to-peer contracts. Ethereum has developed a statically typed, contract-oriented programming language, Solidity, for writing and implementing smart contracts on various blockchain platforms. The smart contract by Ethereum extends blockchain applications because it is a decentralized system that exists among all permitted parties; There's no need to pay intermediaries, thereby saving time and conflict and demonstrating the ability to create a self-sustaining global node computing ecosystem. Bitcoin and Ethereum are both well designed cryptocurrencies. Bitcoin is computationally intensive and slow, while Ethereum is relatively fast. Based on the contractual mechanism of Ethereum, we created the BF platform (BFchain, BFcoin, BFtoken), an encrypted digital currency ecosystem as a version 3.0 blockchain. BF platforms are more user-friendly to most application scenarios.

Table of Contents

Design Philosophy

1. Decentralized Infrastructure and Neutralized Application layer. We inherit the advantages of Bitcoin and Ethereum by designing BFchain and BFcoin as a globally decentralized distributed application and ledger system. Moreover, we also designed an additional set of distributed LAN ID systems for BFtoken to better capture data and reinforce the use of cryptocurrencies for better real work application support and performance.
2. We hope BFcoin reflects its value not only in the virtual community but also in the real world through the public's acceptance and usage. We pledge to be fully open sourced and not be controlled by organizations, institutions or individuals.

3. In order to prove the value of BFcoin, we will design various application scenarios for the usage of BFcoin and BFtoken, combining the virtual world with reality.
4. We want to guarantee the privacy and security of the BFcoin but also the independence and scalability of each application.We developed BFcoin for the purpose of situational applications, but we do not prevent BFcoin owners from trading on any platform. We welcome the use of BFcoin on different platforms, whether in the application platform or the trading platform, and whether in the virtual community or in real world applications.

About BF Platform

BF platform is a decentralized application platform, providing a series of SDKs and APIs to help developers create both decentralized and centralized applications based on BFchain technology. By providing a whole set of industry standard solutions, including customized BFchain, smart contracts, application hosting, etc., BF platform intends to offer an easy-to-use, fully functional ecosystem with BFcoin and BFtoken. Our long term strategy is to leverage BFchain by focusing on copyrights, anti-counterfeiting, gaming, digital merchandising and other scenarios so that the value of BFcoin is reflected in not only virtual currency trading platform applications, but also practical applications. We utilize the abundant network resources to mine through our decentralized BlockNAS(Block with Network Attached Storage), rewarding original block participants with our encrypted digital currency, BFcoin. While BFtoken is designed as a distributed LAN ID System that BFchain co-produced parallelly with a public key and a private key. Only those IDs signed by the root certification authority are allowed to enter the network. This way, we improve security and flexibility for these applications in our platform.

Here are some application scenarios that can bring in reward:

1. Reward the original author through the cloud copyright block node with BFtoken, after verifying the original record and creating the encrypted private key.
2. Reward the original author through the cloud streaming media block node with BFtoken, after verifying the original product and creating the encrypted private key.
3. Reward the value creators through the GPS block game node with BFtoken, after verifying the movements or operations in the games.
4. Other Incentive Programs that can be applied to other platforms, such as Community Welfare Platforms, Social Platforms, and Copyright Platforms...

Technique Specification

1. BFcoin

1.1 Algorithms

a. compared to Bitcoin's C++ and stack scripts, Ethereum's Solidity and JavaScript are more popular and easily maintained. BF new language will follow Ethereum's simple user friendly principles.

b. BF EVM is the operating environment for BF Smart contract. It is completely isolated, meaning that code running inside the EVM does not have access to the network, file system, or other processes. Even smart contracts have limited contact with other smart contracts. In order to make BFcoin more popular, the BF web browser is already in development and testing. After the success of the R & D test, the browser will be open sourced.

c. Bitcoin has SPV (Simplified Payment Verification) concept that the implementation does not verify everything, but instead relies on either connecting to a trusted node, or puts its faith in high difficulty as a proxy for proof of validity. This is the traditional Merkle Tree which trie has only one node. While Ethereum is using Merkle Patricia Tree (MPT) that the root node

becomes a cryptographic fingerprint of the entire data structure and defines three different node types (branch, leaf, and extension). The BFchain also uses a Merkle Patricia Tree's cryptographic authentication data structure with a block header, a list of transactions, and a list of uncle blocks. The block header has the hash root of the transaction which is used to check the transactions list. The transactions that are transmitted on the p2p network are a list that is assembled into trie to compute the root hash. This data structure is not necessary except for the check blocks. It can be technically negligible once the block has been validated correctly. This means that the transaction list is stored locally as a trie and is serialized into a list when sending to the client. The client reconstructs the transaction list trie tree to verify the root hash after receiving the transaction list. We use RLP (Recursive length prefix encoding, recursive length prefix encoding) to encode all trie entries. Thus BFcoin becomes a globally decentralized distributed application and ledger system.

1.2 BFcoin's Mining Design

```
{
   "difficulty": "0×400",
}
```

"difficulty": "0×400", binary system，we can setup the difficulty for the block. If it is too hard, the CPU mining will be difficult. We setup an easy one on purpose.

1.3 BFcoin's Unit of Measurement

BFcoin's smallest unit is Feng, then Jiang, then Lei ：

1 Jiang = 10^{12} Feng

1 Lei = 10^{15} Feng

1 BFcoin = 10^{18} Feng

1.4 BFcoin’s Distribution

For the purpose of focusing on practical application of BFchain, BFcoin has a revised total circulation of 30 billion, of which 40% are for BFchain users for applications, 30% are for original development teams, 10% are for mining activities, and 20% are reserved for incentives, future participation and collaborators who contribute to the program.

2. BFtoken

2.1 What’s Different?

Unlike Bitcoin and Ethereum, BFchain has different systems for BFcoin and BFtoken. BFtoken is designed as a distributed LAN ID system generated by public key and private key. Only those authenticated BFtoken IDs signed by the Root Certification Authority are allowed to enter the network.

The ID generated in BFchain is a globally unique identifier. It ultimately comes from the top of the DNS hierarchy. The payBF network allows users to define

their usernames as they like, because usernames do not need to be unique. But the IDs generated by public and private keys are unique globally.

As long as BFtoken owner's signature matches his private key, the BFtoken owner is authorized for service. Once we apply a valid IP obfuscation system, the BFtoken network can be completely anonymous, leading to improvement of the security of the system.

BFtoken ID uses Public Key Infrastructure (PKI) and X.509 (commonly known as PKIX). An X.509 certificate contains a public key and BFtoken ID, and is signed by BFchain Root Certificate Authority. When a certificate is signed and validated, user who holds that certificate can rely on the public key it contains to establish secure communications and validate documents digitally signed by the corresponding BFtoken private key. The encryption solution is a public-key cryptosystem. For BFtoken ID authentication process, the X.509 standard public key encryption system provides a digital signature. The user can then generate information fingerprinting. The user encrypts the digest with the private key to form a signature. The recipient decrypts the signature with the sender's public key and compares it with the received message.

2.2 BFtoken for Applications

BFchain comes with the unique distributed LAN ID System for BFtoken. BFtoken, which acts as the tokens for all BF application platform, circulates within the system for all applications, such as Cloud Copyright Block, Anti-counterfeit Block, Streaming Block, GPS Game Block, and Monetary Exchange Block.

3. Exchange Rate for BFcoin to BFtoken

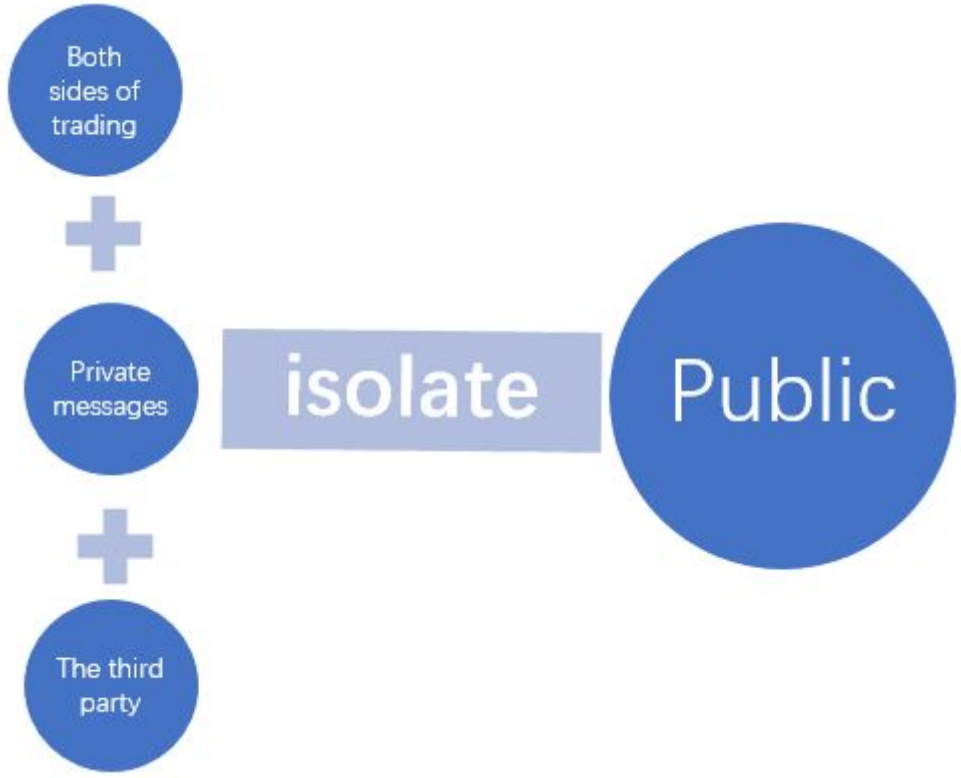
Use the following Recursive Function f() for BFcoin and BFtoken exchange, we may apply candy plans and handling fee later. Here, y is for Year, IR(y) is for US Annual Inflation Rate, INT is for Integer Rounding Function.

a) y < 2018, f(y) = 0 ;
b) y >=2018 && y <2022, f(y) = 100;
c) y >=2022, f(y) = (1 + IR(y-1)) * f(y-1);

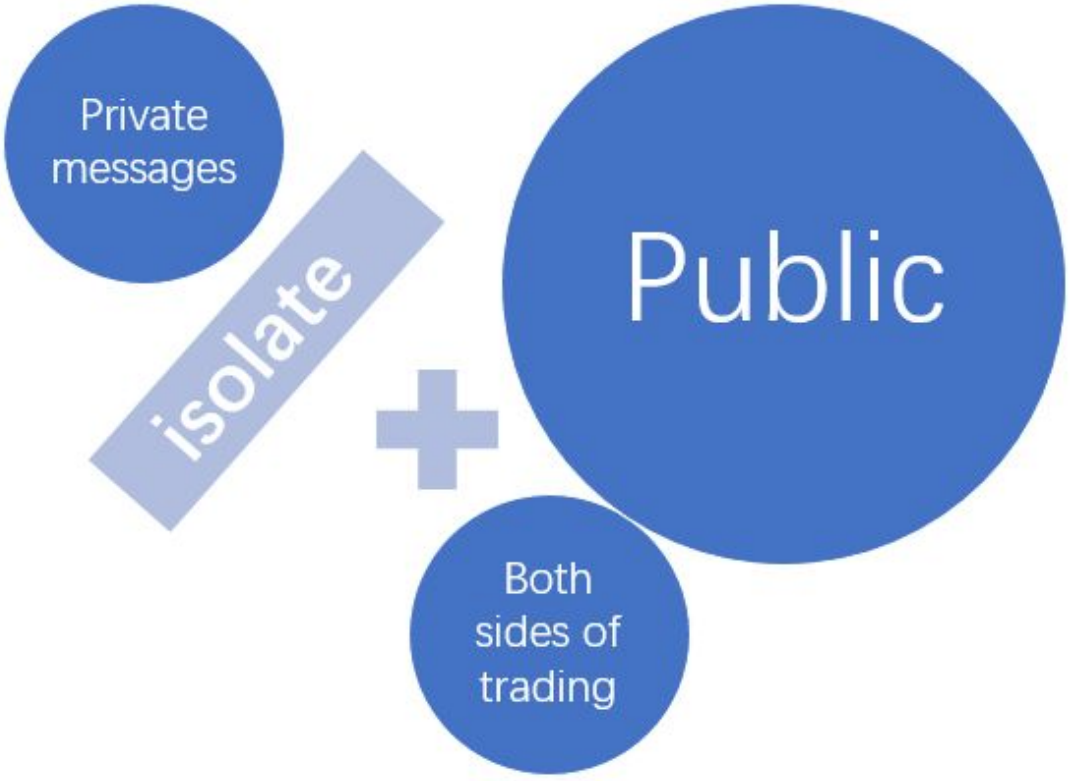
#BFtoken = INT (# BFcoin * f(y));

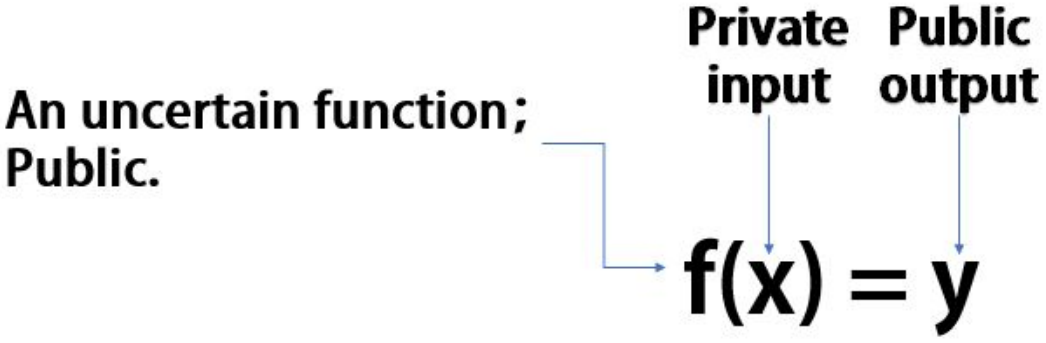
4 Privacy and Security

Privacy and security are the biggest considerations for the BFchain. How can we protect the privacy in BFchain? The privacy of traditional currency transactions is that the identity of the traders and the identity of other parties can be kept confidential from each other. Because these transactions are isolated from the public, the transactions are also kept confidential from the public too.



Privacy of the digital currency world has special characteristics: identities of the traders are separate and secretive, but the transactions are open to the public.





BFchain uses Zero-Knowledge Proof to address the issue of privacy and publicity. For zero-knowledge proofs of knowledge, the protocol must necessarily require interactive input from the verifier, usually in the form of a challenge or challenges such that the responses from the prover will convince the verifier if and only if the statement is true. This is clearly the case, since otherwise the verifier could record the execution of the protocol and replay it to someone else: if this were accepted by the new party as proof that the replaying party knows the secret information, then the new party's acceptance is either justified—the replayer *does* know the secret information—which

means that the protocol leaks knowledge and is not zero-knowledge, or it is spurious—i.e. leads to a party accepting someone's proof of knowledge who does not actually possess it. In cryptography, a zero-knowledge proof is a method in which one party can prove to another party that they know a value without conveying any information apart from the fact that they know the value. Another way of understanding this would be: Interactive zero-knowledge proofs require interaction between the individual or computer system proving their knowledge and the individual validating the proof. No matter if this equation is encrypted or not, if everyone can see this equation is true, then this is zero-knowledge proof. There is no need to do any data processes in order to pass the verification.

5. BFwallet & BlockNAS

5.1 BFwallet - Could be the most secure digital currency wallet in the world.

BFwallet provides a more effective alternative to current security measures. The entire equipment system includes hardware and software packages and a hot and cold wallet system. It connects to any computer with an adapter and a digital hard-key, and embeds a secure OLED display to double-check and confirm each transaction with a single tap on its buttons. The advanced version will come with finger scanning verification. BFwallet uses hierarchical deterministic design so that both hot and cold sides can generate public key / private key pairs to improve the system security and fast dock when connected. BFwallet comes with perfect hardware technology solutions, software solutions, and advanced crypto algorithm solutions. It has registered global patents and could be the world's most secure digital currency wallet.

5.2 BF BlockNAS

BlockNAS (Block with Network Attached Storage) is a decentralized dedicated Network data storage server. It integrates NAS and P2P through cloud service and block nodes. The NAS consists of multiple nodes in a relatively integrated P2P block that consolidates nodes on the cloud server into client blocks.

NAS clients and peer nodes of the P2P network share information with each other. Moreover, the client node can use the P2P network to provide content resources to other nodes, and also acts as a server to provide computing

bandwidth for the network. NAS reduces the burden through the client's participation. NAS server as a super node in a P2P network can also provide P2P network with closer (logical / physical) network resources. This near-way access to resources ensures access to resources and thus improves overall system performance. Moreover, the management of nodes through PoW and PoS proves that the added nodes can gain operational benefits and make the transaction more transparent and fair. The integration of blockchain payments has made it possible for the secure and efficient currency exchange platform.

Most of the current cloud computing power in the market simply involves miners or mines renting their own computing power. In fact, the buyer is not a miner, but a consumer, who is incentivized by potential returns from digital currencies such as Bitcoin, Ether, and BFcoin. BF BlockNAS is well designed with the hardware and software to support Cloud CPU mining and make full use of surplus network resources.

6 Solution & Business Focus

When BFchain was originally launched, the team had several goals in mind based upon past experiences developing blockchain solutions. BFchain is developed in three levels: the infrastructure network, intermediate protocol, and application services. With the further optimization and evolution of the infrastructure network and the intermediate protocol layer, there are more and more innovative technologies and scalable applications can be adopted into this application oriented ecosystem.

6.1 BFchain for Copyright Protection : The Next Generation Copyright and Anti-Counterfeit Application

6.1.1 Principle

BFtoken Identity uses Public Key Infrastructure (PKI) and X.509 (commonly known as PKIX). The X.509 standard and public key encryption system provides a digital signature solution; the customer may generate the

fingerprint of the information that extends to the cloud's copyright blockchain. The original work is reflected in the uniqueness of the public key; the customer’s signed address is encrypted and stored into the related private key. We also incorporate other anti-counterfeit technologies, thus making the BFchain more secure and efficient.

6.1.2 Original Verification Application Scenario

The author of the article can publish the original works on the BF article publishing platform. After authentication process, the public key and private key are generated. The public key is recorded by BFchain as the unique identifier. The private key is kept by the author. The system gives anyone the power to gain and sell BFtokens, which are tokens distributed by “upvote” and “like”-based algorithms and can be integrated with websites to align incentives and spur growth, while websites are empowered to adopt sustainable, currency-centric revenue models. The system will do the registration and confirmation on the blockchain ecosystem - BFchain. The system tokenizes the work, and eventually rewards the customer with BFtokens. We enable publishers to create tokens that help to monetize content and grow communities.The workflow and timestamps of all digital currencies, such as Bitcoin, Ether, and BFcoin, etc., are permanently recorded in the distributed BFchain seamlessly. If the BFchain publishing platform discovers that work is not original, we will notify the original owner and reserve the legal rights to impose penalties on his/her user account.

6.1.3 Anti-counterfeit Application Scenario

The decentralized nature of BFchain determines the openness and equalness of the nodes that maintain data. With the 51% attack theory, the signature generated after private key and public key pair verification and the time-stamping information added to the BFchain will be permanently

recorded, and a single node will not be able to modify the data. Genuine providers can register with the BF platform and generate the public and private key after the authentication process. The system quickly registers and certifies the product within BFchain. Consumer can query the the product information in BFchain via BFbrowser. If counterfeit goods are found, the BF platform immediately notify the original owner for further actions.

6.2 Cloud Media Application Scenario

The cloud streaming media blockchain application enables creators and users to access and share video content. The creators upload the original videos to the BF cloud disk, and the system generates the public and private key after the authentication process. Then, the system registers the content in the Cloud Streaming Media Chain, then tokenizes the content and records the time stamp information. Users can use BFcoin or other digital currencies to motivate and reward the video owner. BFchain records the authenticity of the content ownership. As a result, both content providers and users can reduce cost and have better services.

6.3 WagwagDogChain Gaming Scenario

The BF team is developing a global blockchain online game - the Encrypted Wagwagdog Game (BFdog). The game comes with many scalability features, combined with BFchain elements(BFcoin, BFtoken, smart contract) and the GPS and AI solutions. The game platform accepts different currencies and other digital currencies for exchange purposes.

6.4 Community Welfare Platform Scenario

The BFchain can also provide general services such as smart rental contracts, community activities, and targeted donations for any community welfare platform. For example: BFchain can help students' social platform for old textbooks sales. It also allows the system to tokenize each item with the advanced smart contract. Users can be rewarded with BFtoken if desired.

7 About BF Team

The payBF platform provides a smooth experience to apply the power of blockchain technology globally. By joining payBF's global network, customers can verify copyrights for their original products and take advantage of anti-counterfeit technology solutions instantly, reliably and cost-effectively. The BFteam has also invented industry-leading advanced products and core technologies with international patents, such as the highly secure digital currency wallet, BFwallet.

Summary

BFchain is an Encrypted Application Oriented Digital Currency Ecosystem that rewards network participants with BFtokens. Inherited all the benefits from blockchain 1.0 and 2.0, BFchain comes with the unique distributed LAN ID system that makes the system more application oriented, secure, and efficient. BFchain supports smart contracts, BFtoken, side chains and other advanced security mechanisms. BF team welcomes the involvement of those who are interested and reserves a reward program for future partners who join and make special contributions.

References

Patricia Tree https://github.com/ethereum/wiki/wiki/Patricia-Tree

Merkling in Ethereum
https://blog.ethereum.org/2015/11/15/merkling-in-ethereum

Ethereum Whitepaper https://github.com/ethereum/wiki/wiki/White-Paper

Merkle Patricia Tree (MPT)
http://blog.csdn.net/zslomo/article/details/53434883

Introduction to Smart Contracts
https://solidity.readthedocs.io/en/latest/introduction-to-smart-contracts.html

Corda: A distributed ledger
https://docs.corda.net/_static/corda-technical-whitepaper.pdf