BitNew-Chain

BTN Tech-White Paper

Next-generation decentralized application platform for commercial applications

V1.1

18th, March ,2018

Overview & Motivation

With the popularity of Bitcoin, entrepreneurs and developers began to recognize that the blockchain technology behind Bitcoin has vastly greater potential than simply as the basis for a new digital currency. Within just a few years, dozens of new decentralized applications (Dapps) have been built upon the blockchain technology, including encrypted messaging (Bitmessage), decentralized exchanges (Bitshares), trustless gambling (Peerplays), cloud computing (Golem), and social media (Steem).

One challenge for Dapp developers in this new blockchain economy is the difficulty of actually building a new blockchain application from scratch. In order to solve this problem, the idea of smart contract platforms was developed and implemented. Smart contract platforms, such as Ethereum, can be thought of as decentralized platforms for developing and running decentralized applications.

Unfortunately, current smart contract platforms still have various limitations, such as limited scalability, limited privacy and high usage fee/gas rates, which seriously hinder their widespread adoption. Furthermore, as most current smart contract platforms lack built-in resource segregation support, all computing and storage are performed on-chain, which is prohibitively expensive for large commercial applications. Governance over blockchain itself is also chaotic, which makes it impossible to quickly reach consensus on urgent issues or updates.

Here we present BitNew-Chain (BTN), a next-generation decentralized application platform for commercial applications that addresses all aforementioned problems. BitNew-Chain (BTN) aims to build a next-generation decentralized platform with several key improvements. BTN is designed with higher scalability, a more flexible fee/gas model, less storage/computing constraints, and better governance protocols. All core functionalities, such as decentralized storage and computing, are integrated into a unified platform. Therefore, commercial applications such as decentralized games and IoT systems can be built smoothly using the BTN platform without dependency on any other third parties, which makes BTN an ideal platform for Dapps.

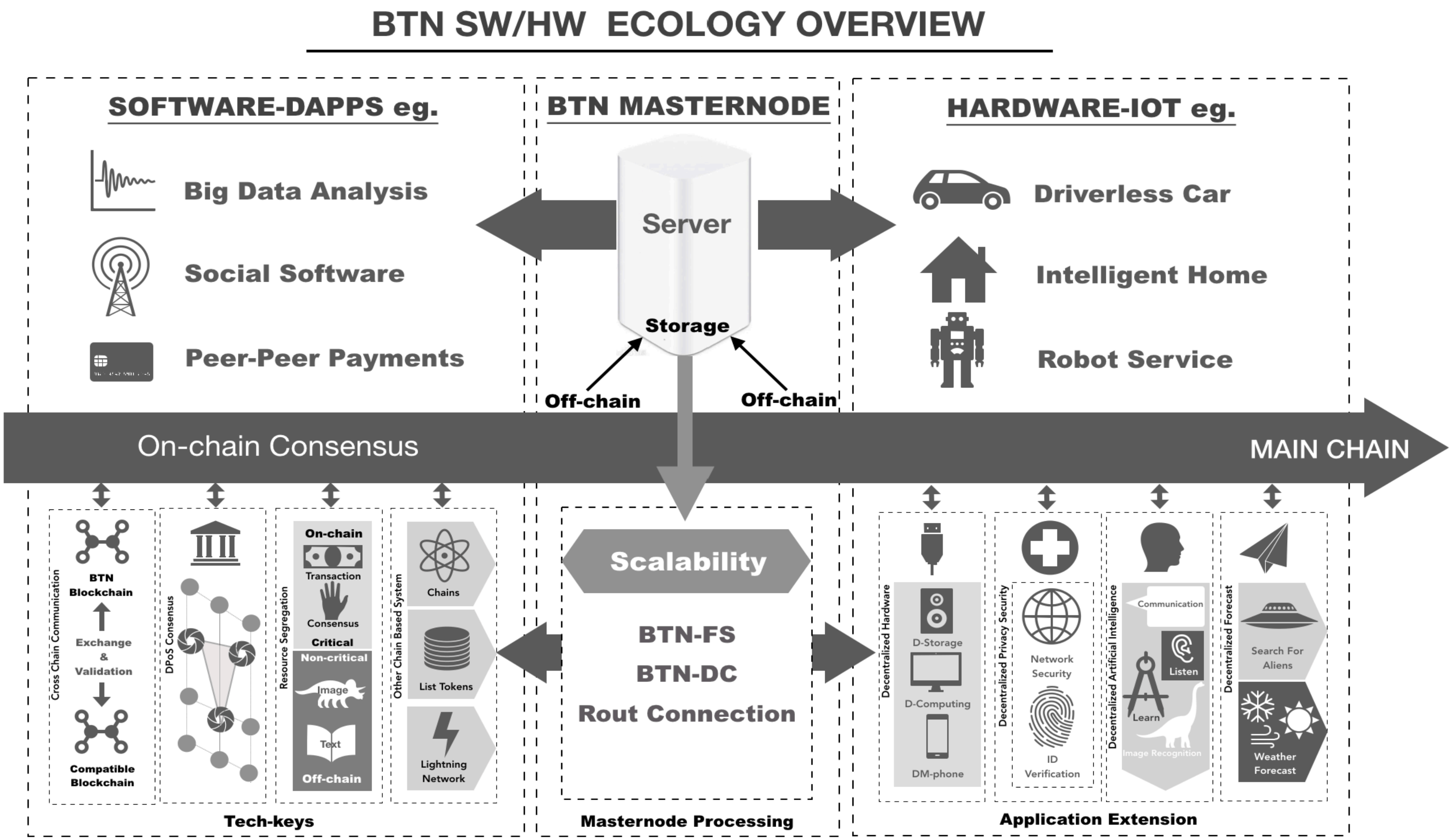

Figure 1: Overview of BTN SW/HW Structure

Key Design Objectives

As a next-generation decentralized application platform, BTN is designed to meet the following key objectives, which are critical for commercial applications:

Decentralized Application OS

We designed BTN as a highly efficient and customizable OS for decentralized application. Leveraging blockchain and other decentralized techniques, BTN resolves the most fundamental and time-consuming parts of decentralized application development, allowing developers to focus on application scenarios and customer needs. Based on BTN's core functionality and standard interface, developers can delivery commercial Dapps with only hundreds of lines of code.

Decentralized Hardware Support

BTN aims to build a decentralized ecosystem for both software and hardware. By providing standard interface and hardware specifications, BTN simplifies the development of decentralized hardware, allowing any partners to produce BTN- compatible hardware.

Scalability

Scalability is always a bottleneck for commercial applications. Currently Bitcoin can only process nearly 7 transactions per second (TPS). However, commercial applications such as Uber, AirBnB and Facebook need to handle tens of millions of daily active users. To support such real-world scenarios, BTN is built to support millions of transactions per second with low latency.

Resource Segregation

On-chain storage and computation are expensive for current smart contract platforms such as Ethereum, as every full node needs to store blockchain data and perform computations.

To pursue a balance between security and efficiency, BTN divides both data and computation into two categories, namely on-chain and off-chain.

- Storage: Critical data should be recorded on the blockchain, which will be downloaded and identified by all full clients. Non-critical data, such as text and images, do not need the same level of consensus as monetary or financial transactions. Thus, non-critical data can be stored off-chain and referenced by hash-based content address. BTN provides built-in support for such decentralized storage, which allows users to control the balance between redundancy and reliability.

- Computation: Computationally heavy tasks are prohibitively expensive to run on-chain due to cost constraints. Similar to a storage system design, BTN allows users to delegate non-critical expensive computation off-chain with the help of built-in verifiable computation support.

Other Features

■ Flexible Transaction Fee Model

Popular web services, such as Google and Facebook, are free for end users. However, most of current smart contact platforms require users to pay for the services. BTN will provide more fee strategies for developers, who can offer free services for end users to gain more widespread adoption and usage.

■ Advanced Governance Protocol

Blockchain based techniques are evolving rapidly. However, the currently chaotic state of governance for decentralized systems will limit the development of new technologies. The well-known segwit2x upgrade for Bitcoin failed due to a lack of governance protocol. In fact, many of Bitcoin Improvement Proposals (BIP) will never be realized due to the same reasons. BTN is designed with clearly defined voting and update mechanisms for feature enhancement and bug fixes.

Privacy Enhancement

Bitcoin stores pseudonymous transactions in a public decentralized ledger, with clear relationships between the addresses of senders and receivers. It appears to be totally secure, as the originator of the transaction is difficult to track because there is no real-world identity attached to the address. However, much information can still be deduced through public data, such as web trackers and cookies. Once the connection between the pseudonym and real-world individual is made, the secret is revealed. BTN is designed to provide a higher level of privacy, building up a truly anonymous decentralized platform.

Cross-Chain Communication

In addition to having a powerful main blockchain, BTN is also designed to facilitate cross-chain communication for further extension.

Parameter	BTC	BTN
Confirmation time with comparable security under Satoshi equivalence	10 minutes	3 second

Minimum confirmation time for a reversal probability of 0.1%	20 minutes (2 blocks)	4.5 seconds
Max. Transaction per second	3.3 TPS (assuming an average size tx)	10000 TPS at launch, scalable to millions of transactions per second.
Current average cost for users for a standard transaction	6 cent Adduming -1.5 TPS	No fee for transaction
Resource Segregate	NO	YES

Figure 2: BTN Cross-Chain Communication Advantage

BTN Architecture

Two-tier Network

Full nodes are servers running on a P2P network that allow peers to use them to receive updates about the events on the network. Full nodes are very important to the health of the network as they provide clients with the ability to synchronize and quickly propagate of messages throughout the network.

To provide better service for the BTN ecosystem, BTN adopts a two-tier network design. In addition to the main network (analogous to Ethereum), BTN adds a secondary network, known as the BTN masternode network. With economic incentives, BTN masternodes will have high availability and provide a required level of service to the BTN network.

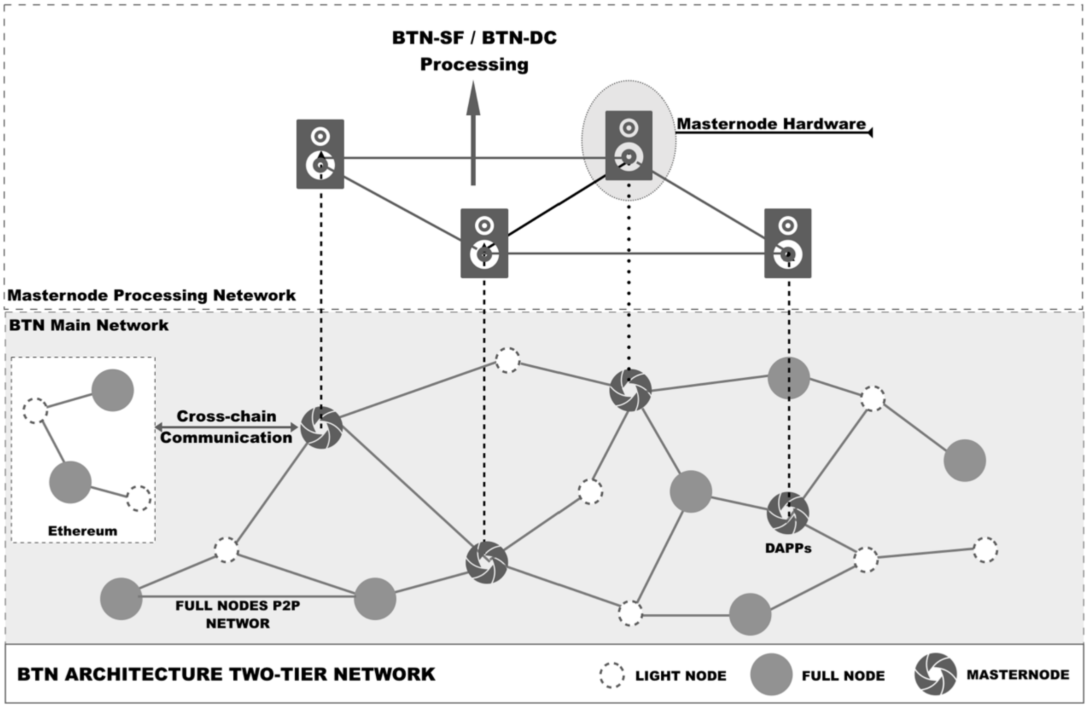

Figure 3: BTN Architecture of Two-tier Network

Masternode Network

The masternode network consists of masternodes, which are full nodes except that they must satisfy the following requirements to serve as a qualified masternode:

- have a bond of deposit
- satisfy BTN hardware specification
- provide the decentralized storage service: BTN-FS
- provide the decentralized computing service: BTN-DC
- provide the privacy improved transaction service

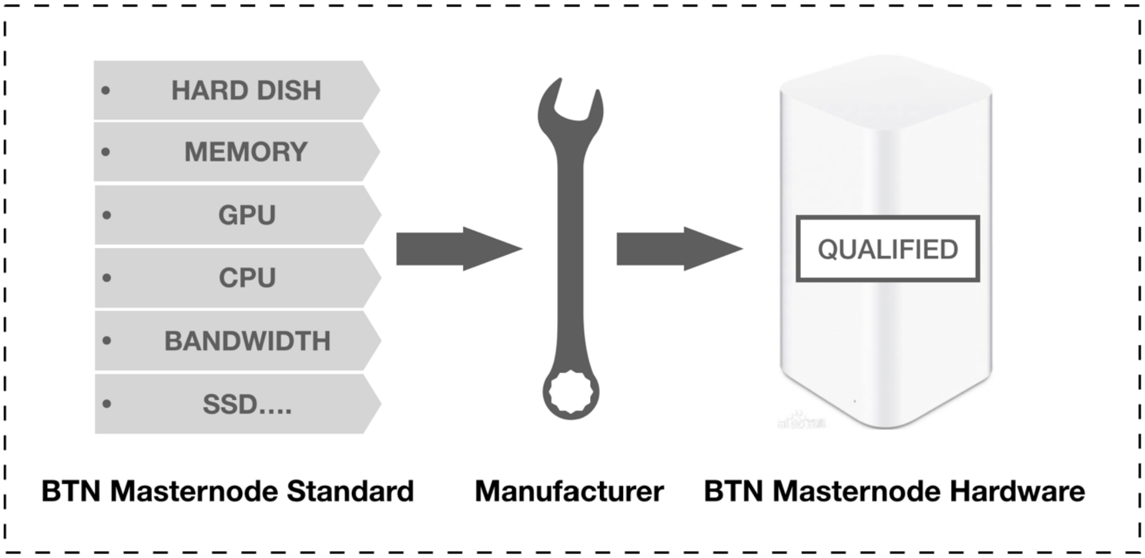

Figure 4: BTN Masternode Manufacturing Specification

In summary, the node must store 20,000 BTN and provide required services to clients on the network to run as a masternode. When active, masternodes are paid in the form of a dividend in return.

- Masternode Reward Program

Full nodes require significant amounts of traffic and other resources that carry substantial costs. As a result, a steady decrease in the amount of these nodes has been observed on the Bitcoin network.

To encourage more users to participate in the masternode network, BTN provides a masternode reward program which pays approximately 50% of the total block reward to all masternodes. The reward paid to each masternode is proportional to its deposit. Each masternode can deposit at most 0.05% of the total BTN in circulation, which prevents the centralization of masternode network. Thus, the masternode reward program allows the masternodes to pay for the expense and earn a return on investment.

Privacy Improved Transaction

Privacy improved transactions employ a similar strategy as the DASH Private Send. Privacy improved transactions utilizes the fact that a transaction can be formed by multiple parties and made out to multiple parties to merge funds together in a way where they cannot be uncoupled thereafter.

Main Network

The BTN main network is a blockchain based network like Ethereum, which acts as the backbone of the whole system.

Consensus Mechanism: Delegated Proof of Stake (DPoS)

BTN utilizes Delegated Proof of Stake (DPoS) as the decentralized consensus algorithm, which has shown promising performance.

In DPoS, token holders elect block producers, who are responsible and rewarded for generating blocks. The elected producer will be given an opportunity to produce blocks proportional to the total votes they have received. The voting process is continuous, therefore, producers have an incentive to carry out their function to the highest standard or they risk losing their votes.

BTN delegates 2N+1 mining nodes. Exactly one producer is authorized to produce a block at any given point in time. At the start of each round 2N + 1 unique block producers are chosen. The top 2N by total approval are automatically chosen every round and the last producer is chosen proportional to their number of votes relative to other producers. The selected producers are shuffled using a pseudo-random number derived from the block time.

Hybrid Mining

Based on DPoS Consensus Mechanism and Masternode Reward Program, BTN adopts a hybrid mining mechanism, namely Delegated Proof of Stake (DPoS) + Prove of Masternode (PoM). DPoS ensure the efficiency of the main network while PoM encourage more masternodes to participate.

Economic Model

Unlike Ethereum, BTN utilizes an ownership model like EOS. Holding BTN tokens gives users a proportional share in network resources, such as bandwidth, storage, and processing power. This means that if someone owns 1%

of BTN tokens, they will always have access to 1% of the network bandwidth, regardless of the load on the rest of the network.

Furthermore, since the network will have zero transaction fees, there is no network development cost, except for the initial purchase of BTN tokens. However, BTN tokens can of course always be sold in order to reclaim the initial investment if desired.

Decentralized Storage Subsystem: BTN-FS

BTN has an IPFS-like subsystem (BTN-FS) for decentralized storage. BTN-FS indexes the data through file content hash rather than path/url.

The main improvement of BTN-FS over IPFS is the manipulation of the file reliability. BTN-FS allows the user to set the reliability requirements of the file based on the desired balance between redundancy and reliability. Based on the economic incentives of masternode reward program, stable and reliable decentralized storage services will be provided by the masternode network.

Decentralized Computing Subsystem: BTN-DC

Similar to BTN-FS, BTN has a TrueBit like subsystem (BTN-DC) for decentralized computing. BTN-DC has both solvers and verifiers, which are randomly selected from the masternode network. Solvers are compensated for performing computation and verifiers are compensated for detecting errors in solutions submitted by solvers.

In the event of a challenged solution, the computation is performed on-chain to decide whether to penalize the solvers or the verifiers and a security deposit will be charged from the misbehaving masternodes. BTN-DC also allows the user to choose the reliability requirements of the computing.

Turing-complete Virtual Machine: BVM

BTN utilizes a virtual machine independent architecture for smart contract system. Thus, multiple virtual machines can be supported and new virtual machines or features can be added over time as necessary.

Currently, BTN has a two stage plan for BTN Virtual Machine (BVM) development:

- The Ethereum Virtual Machine (EVM) is the de facto standard for smart contract. Thus, the first version of BVM is planned to be op-code level compatible with EVM, allowing existing EVM contracts to run on BVM with little modification.

- For further versions, BTN is planned to emulate EVM by dynamically retargeting EVM opcodes to a subset of bytecode, which can bring BTN code execution to performance close to native code and support more programming languages.

Cross-Chain Technology

In the long term, we believe the cross-chain communication protocol will converge on one protocol as there was for IP and HTTP. BTN will switch to that standard thanks to its easy update feature. Currently, BTN is designed to support cross-chain communication with two approaches:

■ Cross-Chain Transaction Validation

Cross-chain transaction validation is achieved by a light client validation approach. Block headers of compatible blockchains can be saved in BTN-FS with high reliability, making it easy to generate proof of message existence and proof of message sequence.

■ Cross-Chain Token Exchange

Cross-chain token exchange will be implemented using the atomic swap mechanism. The compatible blockchains can thus easily exchange tokens with BTN.

Governance

BTN token holders are the network owners and managers, managing the network through delegating their rights to block producers. The delegated block producers are given checked authority to propose hard forking changes to the underlying protocol or other administrative operations. With the continuous voting of BTN holders, if the block producers refuse to make changes desired by the token holders then they can be voted out, which guarantee the influence of token holders.

BTN Eco-system

BTN aims to build a next generation Dapp platform for commercial applications. Therefore, BTN has proposed a technical blueprint with commercial applications instilled throughout the design.

In addition to these advanced techniques, the success of BTN also relies on widely commercial adoption and a sustainable ecosystem. We will pursue this goal by concurrently striving in two directions: open cooperation and business application.

Open Cooperation

Blockchain is a rapidly evolving field, with new ideas and techniques emerging on a daily basis. In order to build one of the best Dapp platforms, BTN will seek cooperation with the blockchain community, including:

- Cooperation with Other Leading Blockchain Projects

Blockchain techniques are still under active development, which needs the collaboration of the entire community. Thus, BTN treats other blockchain projects as collaborators instead of just competitors. BTN will cooperate with other technique-driven projects, such as QTUM, to accelerate the arrival of the Dapp era.

■ Cooperation with Leading IT Company

Large companies have billions of users and well-built infrastructure. BTN will actively look for cooperation with such large companies to achieve synergies and mutually beneficial relationships.

■ Build an Alliance for BTN Compatible Hardware

To speed up the construction of BTN decentralized hardware ecosystem, BTN aims to build an alliance for producing BTN compatible hardware. For example, by setting the minimum hardware specifications of masternodes, the performance of the BTN network can be guaranteed. In addition to producing qualified hardware with partners by itself, BTN also welcomes other manufacturers to produce the qualified hardware to contribute to the BTN ecosystem.

Business Scenario

BTN is intended to ultimately become the OS to support the next generation of decentralized businesses. With numerous potential applications, BTN will focus on fields that may be early adopters of Dapp solutions and help our partners to build commercial applications.

- Internet of things

BTN supports light nodes to delegate the computation/storage heavy tasks to the BTN masternode network, which reduces the computational requirements for devices connected to it. Relying on the BTN network, IoT devices can work without any centralized servers.

- Gaming

Gaming is one of the largest industries for the Internet. Blockchain increases trust and security in the gaming industry. Blockchain's decentralized system ensures that no particular individual or entity has a centralized advantage at any stage of the gaming process, which greatly improve the financial transparency. BTN will provide an ideal platform for decentralized gaming development.

- Cloud Resource Sharing

Blockchain technology can also be used to create a verifiable resource sharing platform, allowing users to share unused resources. This allows for the creation of a cloud computing market or distributed CDN, where any user can participate with their desktop, laptop or specialized server.

■ Finance

Blockchain has drawn a lot of attention in financial services industry as it significantly reduces intermediaries and improves the efficiency. Applications, such as cross-border payment, supply chain financing and insurance are all highly attractive fields to be disrupted by Blockchain.

■ Artificial Intelligence

Blockchain has the potential to transform Artificial Intelligence (AI). There are many opportunities for blockchain+AI applications. Projects like the AI Decentralizded Autonomous Organization (DAO) will accelerate the development of AI self-upgrading, and AI may be able to accumulate wealth in the future. BTN will provide a platform for those blockchain+AI experiments.

BTN Roadmap

• 2018.02.06	BTN Tech-white paper V1.0 release.
• 2018.03.10	BTN will gain support from first batch of application developers.
• 2018.03.18	A phase update of BTN main network，realize to Proof-of-stake (PoS) mining and smart contract chain. Release BRE21token Standard.
• 2018.05.30	There will be 2000 full nodes working on BTN network.
• 2018.08.30	Main network updated to DPoS and smart contract; Masternode hardware specification plan release.
• 2018.09.30	Launch first Dhardware, based on our own smart contract chain.
• 2019.03.30	Realize cross-chain communication, including token exchange and token transaction validation.
• 2019.06.30	Main network updated to resource segregation, realize decentralized computing and storage.
• 2019.09.30	Realize the extension of artificial Intelligent, explore decentralized applications of AI.

Summary

BitNew-Chain(BTN) is an innovation based on Satoshi Nakamoto's Bitcoin concepts. We hope to inherit the spirit of the Bitcoin Network and build a decentralized P2P cryptocurrency system and platform for decentralized applications. BTN will be a decentralized platform which supports Turing-complete virtual machine, with better scalability, improved privacy, advanced consensus and governance mechanisms.

BTN CORE TEAM

CONTACT US: info@btn.org

Reference

1. Bitcoin: A Peer-to-Peer Electronic Cash System

2. https://github.com/ethereum/wiki/wiki/White-Paper#mining

3. https://github.com/dashpay/dash/wiki/Whitepaper

4. RSK White paper Overview

5. https://github.com/EOSIO/Documentation/blob/master/TechnicalWhitePaper.md

6. http://docs.neo.org/en-us/

7. https://steemit.com/eos/@trogdor/eos-vs-ethereum-for-dummies

8. https://ethereum.stackexchange.com/questions/11589/how-do-oracle-services-work-under-the-hood

9. https://interledger.org/interledger.pdf

10. https://themerkle.com/what-is-a-hashed-timelock-contract/

11. https://news.coinify.com/blockchain-interesting-gaming-industry/

12. https://medium.com/@preethikasireddy/fundamental-challenges-with-public-blockchains-253c800e9428

13. http://zerocash-project.org/media/pdf/zerocash-extended-20140518.pdf

14. https://wanchain.org/files/Wanchain-Whitepaper-EN-version.pdf

15. Qtum White paper

16. http://dataconomy.com/2016/12/blockchains-for-artificial-intelligence/

17. https://www.finyear.com/attachment/690548/

18. https://www.ibm.com/blogs/internet-of-things/iot-blockchain-use-cases/

19. https://bitcoinmagazine.com/articles/understanding-the-lightning-network-part-building-a-bidirectional-payment-channel-1464710791/