Bitcoin Diamond

Whitepaper

2018.07

TABLE OF CONTENTS

Bitcoin Diamond

Unearthing Opportunity for All

Abstract

Bitcoin Diamond (BCD) is a fork of Bitcoin; at predetermined block height 495866, the new chain was created. As the original Bitcoin (BTC) blockchain continues on unaltered, this new cryptocurrency now operates on its own chain called “Bitcoin Diamond”. With Bitcoin Diamond, miners will begin creating blocks using a new proof-of-work algorithm which better serves Satoshi’s original goal of keeping Bitcoin decentralized. Bitcoin Diamond offers several technical advancements in scalability along with anti-replay protection and wallet enhancements. With these changes to the Bitcoin protocol, Bitcoin Diamond seeks to achieve Satoshi Nakamoto's vision for a peer-to-peer electronic cash system that’s accessible and usable to everyone, regardless of economic status or country of origin.

Introduction

After nine years of rapid development, Bitcoin can no longer meet the demands of its rising numbers of clients. Bitcoin has high transaction fees, slow transaction confirmations, and high thresholds for new miners. Furthermore, Bitcoin has still failed to adopt scaling solutions such as SegWit, with well over half of current Bitcoin transactions still using the older, less efficient protocol. As adoption for digital currency continues to outpace Bitcoin’s ability to scale, there is a danger that Satoshi’s digital cash will eventually fall behind other payment platforms.

Bitcoin Diamond addresses these flaws by implementing new technical improvements that resolve issues concerning BTC’s high transaction cost and slow confirmations. By combining Segregated Witness with an 8 MB block size, BCD is capable of performing over 100 transactions per second or 4.8 million a day, over 10 times the current speed of BTC. BCD prevents the centralization of mining power by using X13 Proof of Work, a mining algorithm that is resistant to ASICs and friendly to GPUs. In addition to these starting enhancements, the BCD development team is working on the implementation of the Lightning Network as well as wallet clients across multiple platforms.

Origins

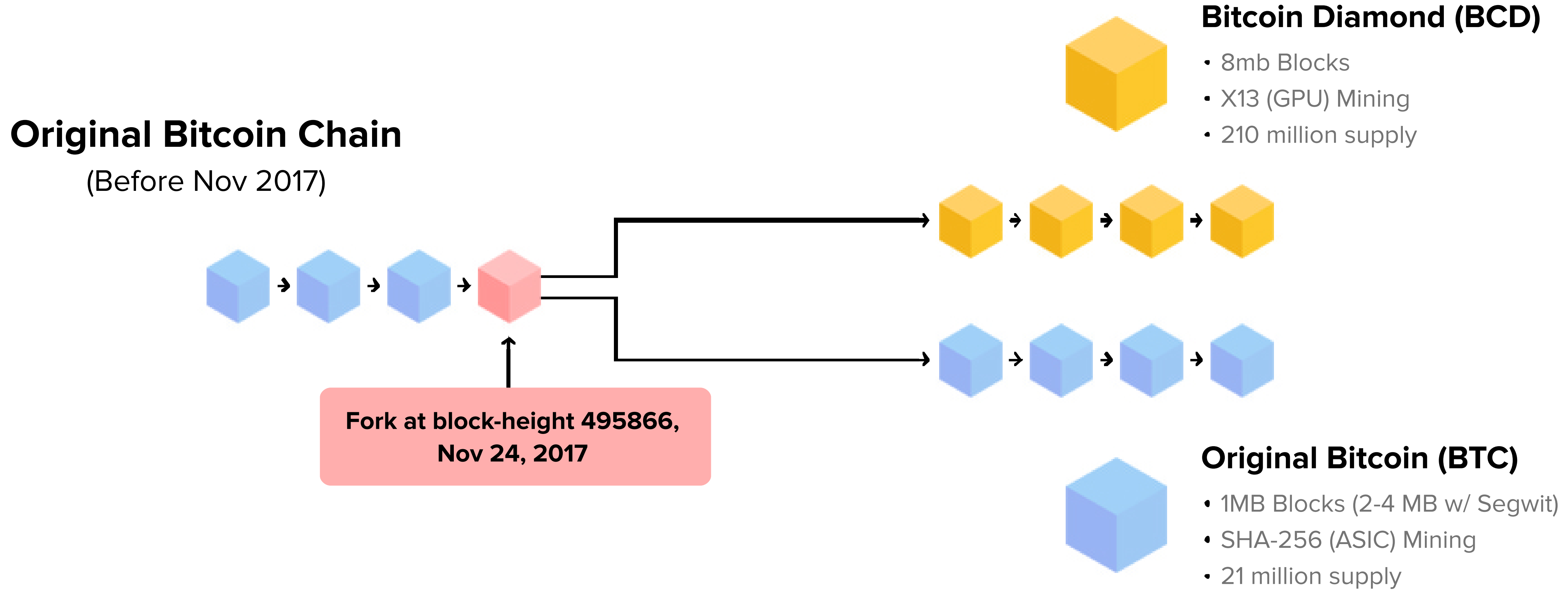
Bitcoin Diamond was forked off the Bitcoin (BTC) blockchain on November 24, 2017 at block height 495866 after Team EVEY and Team 007 partnered to develop the necessary upgrades to improve upon Bitcoin’s original framework. Bitcoin Diamond developers have incorporated a new proof-of-work algorithm and will continue to enhance original Bitcoin features with greater speed, protection, and scalability.

Bitcoin Diamond raised the block size limit from 2-4 MB to 8-32 MB as part of a massive on-chain scaling approach to create ample capacity for higher transaction storage. The transaction capacity of blocks will be increased five-fold and the ultimate goal is to improve transaction confirmation speed for the entire blockchain. With the addition of SegWit, transactions can now scale at a far greater pace than any Bitcoin chain before it. Bitcoin Diamond also offers replay protection as the format for transactions has been changed since the BCD fork. This means that BTC transactions cannot be replayed in the BCD network as a way to steal user funds.

BCD's objectives are to foster the widespread use of Bitcoin Diamond around the world, to empower unbanked people to use Bitcoin Diamond to build wealth for themselves and their families, to establish Bitcoin Diamond as the number one cryptocurrency used in emerging economies, and to make Bitcoin Diamond accessible and usable for everyday transactions. The total amount of Bitcoin diamond is ten times that of Bitcoin which translates into a cost reduction for new participation and a reduction of necessary thresholds. Regardless of scalability, a chain is only as strong as its consensus. To reduce the danger of mining centralization, Bitcoin Diamond uses an algorithm that makes it incredibly difficult for single entities to command large stakes of the processing power for block validation.

Hard Fork

In blockchain, a hard fork is a change to a cryptographic protocol that causes a permanent divergence from the previous version. When this change occurs, all users must decide whether to adopt the new protocol (fork to the new chain) or continue to support the old protocol. If enough users remain on the old chain, two blockchains will then exist which possess identical transactions from before the fork, but now run on separate chains with their own unique history, nodes and protocols. It was through this kind of hard fork that Bitcoin Cash, Bitcoin Gold, Segwit 2x, and now Bitcoin Diamond were created from the original Bitcoin chain.



Bitcoin Diamond was forked on November 24, 2017 when BCD nodes began to support the new protocol after block 495866 and branched away from the BTC chain. From this block onwards, BTC miners are no longer able to mine blocks on the BCD chain and vice versa. Since both chains share the same transaction history from before the split, anyone that owned BTC at the time of the fork would now own ten times the amount in BCD.

Comparison Chart

Name	***Bitcoin Diamond (BCD)***	***Bitcoin (BTC)***	***Bitcoin Cash (BCH)***
Max Supply (millions)	210	21	21
Distribution	Mining, Claiming	Mining	Mining, Claiming
Moving Algorithm	Optimized X13 (GPU)	SHA256 (ASIC)	SHA256 (ASIC)
Block time (minutes)	10	10	10
Max Blocksize (SEGWIT)	8-32MB	1MB (2-4 MB)	8MB
Blockchain Size	~135GB	~145GB	~135GB
Difficulty Adjustment	12 Hours	2 Weeks	2 Weeks + EDA
Maxtx / Day	~4.8 million	~1.2 million	~4.8 million
SEGWIT	Yes	Yes	No
Replay Protection	Yes	Not Necessary	Yes
Time of Establishment	November 2017	2009	August 2017
Lightning Network	Yes	Yes	No

Transactions

Larger Blocks for Faster Transaction Confirmations

Bitcoin Diamond raised the block size limit to 8MB as part of a massive on-chain scaling approach. There is now ample capacity for everyone's transactions to be processed. The transaction capacity of blocks will be increased five-fold and the ultimate goal is to improve transaction confirmation speed for the entire blockchain. With lightning fast transactions, highly diluted transaction fees, and ten times as much supply as other leading Bitcoin forks, Bitcoin Diamond's blockchain prioritizes trust, accessibility, and affordability.

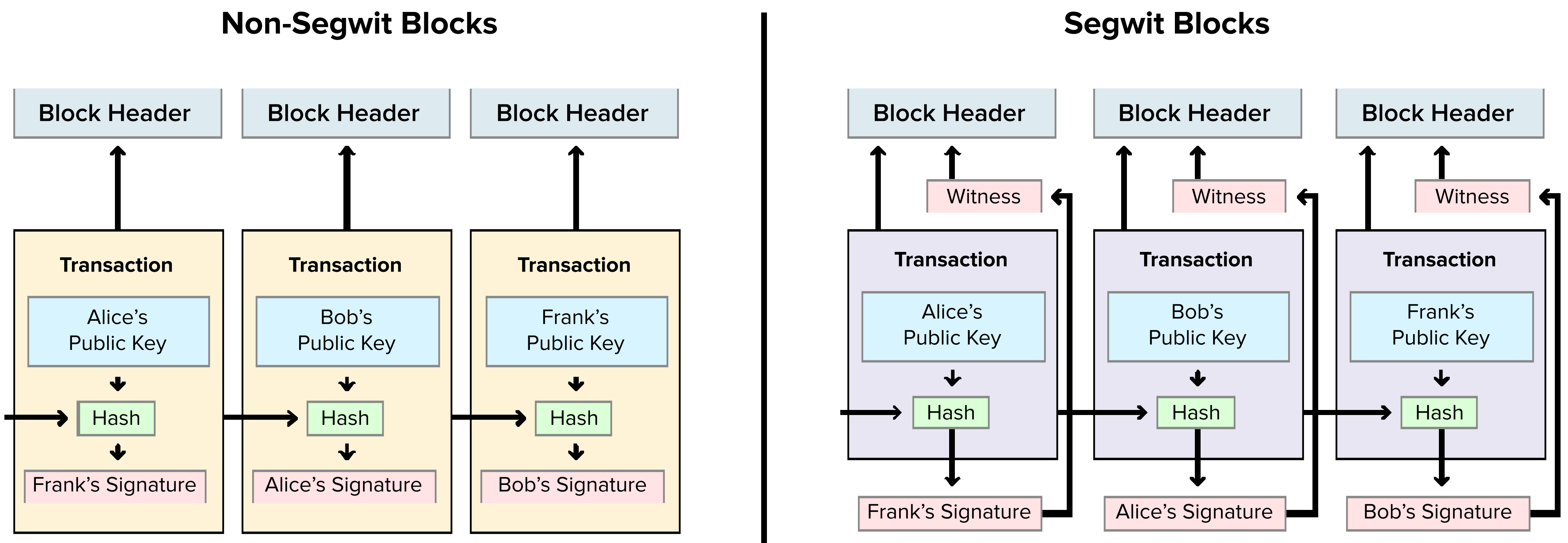
While there are concerns that large blocks may rapidly increase the blockchain's total size, the present number of transactions included in each block is still far from hitting the upper limit of the block size. In case of a future volume increase, additional mechanisms such as sharding are already being considered to reduce the problem of storing a colossal blockchain size.

Lowering Transaction Costs with a Larger Supply

Bitcoin Diamond reduces the transaction fees and the cost of participation: The total amount of BCD is 10 times that of BTC so that it reduces the cost of participation. BCD improves the situation of overpriced Bitcoin, increasing the total supply of BCD and lowering the price. This supply change increases circulation and helps emphasizes the use of BCD for small businesses and microtransactions. With relatively low transaction fees, a secure and private blockchain, and affordable coin prices, Bitcoin Diamond is well suited for making everyday transactions.

Segregated Witness to Optimize Storage

Segregated Witness (SegWit) is the process by which signatures in a Bitcoin transaction are “segregated” from the transactions data. SegWit defines a new structure called a “witness” that is committed to blocks separately from the merkle tree that holds transactions. By removing signature data in this manner, 65% of storage space is freed up so that block capacity for transactions is increased.



Transaction hash includes sender's public key and signature

Signatures are relocated away from the transaction hash in the "Witness" to increase capacity and curb mallleability attacks

In addition to optimizing storage, SegWit also prevents malleability attacks by which a receiver modifies a sender's transaction ID in order to get more coins. Since digital signatures are now separate under SegWit, the attacker cannot change a transaction ID without also nullifying the digital signature.

Anti-Replay Protection

A so-called replay attack can occur when valid transactions on the BTC chain are "replayed" on the BCD chain. Using this strategy, attackers could use valid BTC transaction to rob users of BCD even though both chains have forked. To prevent this, the transaction format of BCD has been changed since the fork so that BTC transactions cannot be mistaken as valid.

These changes to transaction format include:

- A new transaction version number of 12, rather than BTC's 1-3.
- A new field called "Present Block Hash" which contains the hash value of a block's header... For example, when the transaction sent at the height 500020, the field takes the hash value of block 500020, 500019 or 500018. The value is not strictly checked currently, so all transactions matching the format can be verified

Additional changes to BCD's transaction format are planned for the future. This will include features like transaction proofs and periods of transaction validity. You can compare the transaction format differences between BTC and BCD in the diagram below:

Transaction Format Comparison

BTC’s Current Format		BCD’s New Format	
Field	**Description**	**Field**	**Description**
version	Ranges between 1-3	version	Currently 12
tx_in count	Counter of input transactions	tx_in count	Counter of input transactions
tx_in	Array of input transactions	tx_in	Array of input transactions
tx_out	Array of output addresses	tx_out	Array of output addresses
tx_out count	Counter of output addresses	tx_out count	Counter of output addresses
lock_time	Blockheight needed to accept	lock_time	Blockheight needed to accept
		preblockhash	Current block’s hash value

Proof-of-Work Algorithm

Satoshi Nakamoto designed Bitcoin’s mining system as a way for majority decisions to be made on a peer-to-peer basis. This Proof-of-Work used CPU power to guarantee that nodes were fairly represented with “one-CPU-one-vote”.

Satoshi decided to use SHA-256 as the algorithm for this Proof-of-work, which worked well for several years. However, as Bitcoin gained popularity, the mining sector has become more and more competitive. The development of Application Specific Integrated Circuits (ASICs) now means that anyone with access to the latest mining hardware can outpace traditional CPU miners with ease.

For Bitcoin to remain decentralized, a new mining algorithm must be implemented that can resist attempts by hardware manufacturers to outpace traditional miners.

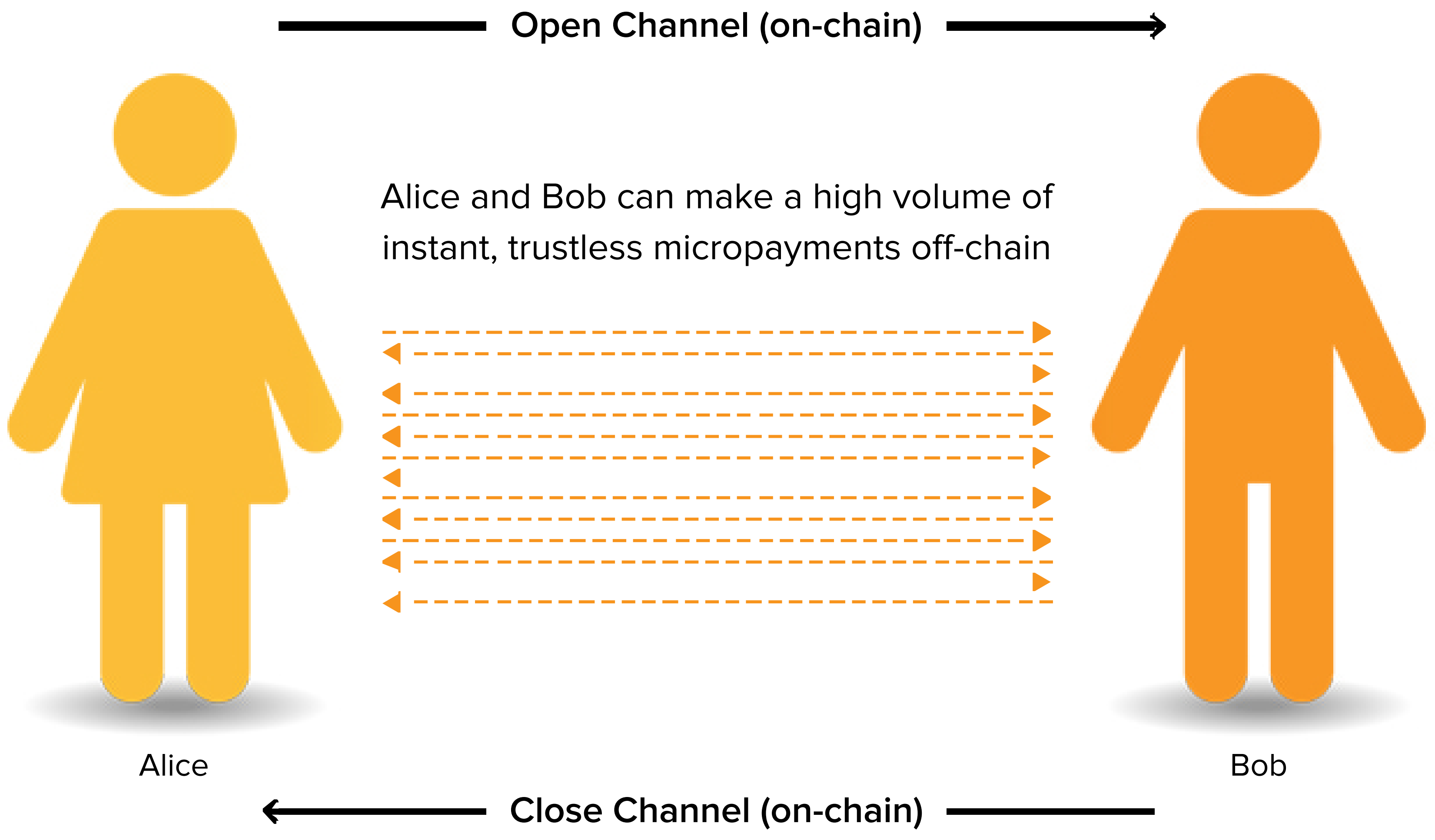
To restore fair mining practices, Bitcoin Diamond utilizes and has improved upon the X13 Proof-of-Work algorithm. This means that all ASICs designed for Bitcoin SHA-256 are now entirely ineffective on BCD. With X13, creating new ASIC hardware is made incredibly difficult by a high level of complexity, reducing the threat of mining centralization. X13 was specifically created for graphics card mining, a standard of hardware that is widely accessible so that competition for mining is fair for the average user.

While the X13 algorithm existed before BCD's launch, the X13 development team has added additional improvements to BCD's version to bolster and ensure security. This includes the SM3 hash algorithm, issued by the Chinese Cryptography Administration in 2016 as the national standard for cryptographic applications. Currently, BCD is the only cryptocurrency to utilize the X13 algorithm in this manner. As time goes on, BCD's development team will continue to improve its mining algorithm to ensure that Satoshi's original vision for distributed consensus remains intact.

Lightning Network

While Bitcoin Diamond protocol provides faster transactions, additional scaling solutions are still required for the protocol to compete with traditional payment methods. To accomplish this, the BCD development team is working to implement Lightning Network, a "second layer" payment protocol first proposed by Joseph Poon and Thaddeus Dryja in 2016. This solution allows users to open "payment channels" by committing an amount of Bitcoin that can then be sent to other participants on the channel without being confirmed on the main chain. Using Lightning Network, Bitcoin Diamond can enable users to make instant transactions at a nearly limitless pace for a very low cost.

Payment Channels on Lightning


Open Channel (on-chain)
Alice and Bob can make a high volume of instant, trustless micropayments off-chain
Alice
Bob
Close Channel (on-chain)

While development on a BTC-version of Lightning is underway using Golang, the BCD team has instead opted to write their implementation in the C programming language. C was chosen specifically for its portability and efficiency, allowing it to easily run on a range of different devices and consume less resources than its BTC counterpart. This version of Lightning Network has already passed functionality tests such as creating nodes and payment channels, declaring and paying transaction requests, confirming receipts across nodes, and testing payments between senders and receivers. A stable version is expected to be deployed on July 31, 2018, after a complete assessment by developers and testers.

Wallet Features

HD Wallet Generation

Hierarchical deterministic wallets, otherwise known as HD wallets, is a feature implemented on BCD to create multiple accounts from a single root key. With this rule, clients only need to save a master private key, which can generate multiple sub-private keys and sub-addresses. Clients can now easily manage the balances of all accounts under this one master private key and selectively issue child keys with limited access. This helps reduce the possibility of a master private key exposure, ensuring the safety of funds.

Electrum Integration

Electrum is a lightweight Bitcoin wallet that has been developed and supported since 2011. By operating in conjunction with servers that index the blockchain, Electrum clients can run with instant startup times and low resource usage. Electrum also offers a wide range of functionality including cold storage, multisig security and integration with hardware wallets. To capitalize on Electrum's feature-set, Bitcoin Diamond has released its own version of the Electrum wallet. After downloading the wallet, users can quickly connect to the BCD network and claim any coins that they may have earned from the November fork.

BCD Pay Mobile

To ensure that all users can easily perform payments, Bitcoin Diamond will be the first Bitcoin project to support an official mobile wallet. An Android wallet based on Electrum has already been released with an iOS version currently under development. Current wallet features include wallet name modification, account switching, and QR scanning. With BCD Pay, digital currency will be made accessible to millions of unbanked individuals in emerging markets, bypassing the financial barriers that had previously excluded them from the global economy.

How to Acquire Bitcoin Diamond

Users who held BTC at the time Bitcoin Diamond was created have automatically become owners of BCD. Please note that a wallet with 1 BTC will hold 10 BCD based on the supply change. Users may also earn BCD by mining with graphics cards or buying coins from an exchange or secondary market. To encourage the community to assist in the construction of BCD's ecosystem, contributors will receive specific amounts of BCD as a reward as well.

Roadmap

Bitcoin Diamond's purpose is to help unbanked and financially underserved people in ways that benefit them. The Bitcoin Diamond initiative will especially focus on people living in areas where other currencies and financial institutions have failed them, such as international transactions, security, and wealth storage. Ultimately, this will increase adoption and usage of Bitcoin Diamond and provide marginalized people with a currency that works in their interest. Our objectives include fostering the widespread use of Bitcoin Diamond around the world, empowering unbanked people to use Bitcoin Diamond to build wealth for themselves, establishing Bitcoin Diamond as the number one cryptocurrency in emerging economies, and making Bitcoin Diamond accessible and usable for everyday transactions. We seek to achieve our ultimate goal of Bitcoin Diamond becoming the "Bitcoin" that achieves Satoshi's vision of becoming a globally accepted digital cash. With this in mind, Bitcoin Diamond will strive to provide better solutions for financial services worldwide.

This plan (Dec 2017 ~ 2018 Q2) is generated by Bitcoin Diamond Community, based on the communication with the BCD development teams EVEY and 007.

As of July 2018, the Bitcoin Diamond TestNet is running smoothly, with new versions to be released soon that will integrate several updates. Updates that are expected to be in the next version include but are not limited to: new boost version requirements with a v1.47.0 minimum, upgraded ZMQ to Python3 support, Unify code style, ability to delete redundant priority judgement code, return error codes, modification of some misleading hints, reconstructing ZapWalletTxes to increase stability, addition of functions to create purses through JSON RPC requests, replacement of old syntax with new C++ features, optimization of namespaces, updated annotations, expansion of documents, and increased document readability.

2017

- Bitcoin Diamond is born at the hard fork at bitcoin block height: 495866.
- Bitcoin Diamond mainnet, wallet, nodes code, and API are released
- Update mainnet

2018

- Deploy Lightning Network and BCD wallet
- Building BCD application ecosystem, including BCD mobile app
- BCD Pay launch and implementation

2019

- Further improve Bitcoin Diamond and its functionality

Financial Strategy

Startup & Operational Expenses	
Early Development	0.6%
Global Market Expanding	1%
Community Construction	0.2%
Legal & Compliance	0.2%
Total	**2%**

Development & Ecological (Time-locked funds; 20% released per year)	
Development	1%
Ecological	3.6%
Total	**2%**

Startup & Operational Expenses

- Early Development
    - Mainnet & Wallet Development
    - Mining & Pools Program Development
    - Nodes & Servers Construction
    - System & Security Maintenance
    - Early Developers Rewards
- Global Market Expanding
    - Meetups/Developer Conferences
    - Global Advisory Recruitment
    - Joint Exchange Events
    - Social Media & Press Releases
    - Advertising
- Community Construction
    - Activities regularly held by full-time employees to implement the Global Community Rewards Program
- Legal & Compliance
    - Funds reserved for future global compliance issues

Development & Ecosystems

- Development
    - Core Development Team
        - Lightning Network
        - Basics of Ecological Construction
        - Technology Upgrades
    - Developer Reward Plan
        - Incentives paid in BCD for developers' open source code that meets certain requirements

- Ecosystem
  - Payments Ecosystem
    - Financial
      - Programs that finance pilot programs such as debit cards, ATM machines, and other forms of payment
    - Cross-Border e-commerce
      - Payment used to streamline traditionally slow cross-border payment and to solve foreign currency payment issues
    - Physical Distribution
      - Multinational physical distribution, while solving the issue of trust and swap foreign currencies
  - On-Chain Application
    - Including but not limited to application of chain ownership certificates, insurance policies and other construction-based BCD backbone
    - Achieve cooperation projects with other blockchain technology and resources for interoperability.

Conclusion

We have proposed a new system for electronic transactions with the mission to make digital currency accessible and usable for everyone, regardless of their economic status, country of origin, or level of ability. With lightning fast transactions, highly diluted transaction fees, and ten times as much supply as other leading Bitcoin forks, our blockchain prioritizes trust, accessibility, and affordability. In an age where many people are forced to serve money, Bitcoin Diamond is a currency that serves the people. With the BCD Pay initiative, we are able to help the unbanked and financially underserved people in ways that benefit them. The initiative will especially focus on people living in areas where other currencies and financial institutions have failed them, such as international transactions, security, and wealth storage. Ultimately, this will increase adoption and usage of Bitcoin Diamond and provide marginalized people with a currency that works in their interest. In order to maximize the adoption of Bitcoin Diamond in emerging markets, we have identified several action steps the Bitcoin Diamond Foundation should take. The BCD Pay initiative will include a range of offerings, including community engagement, educational initiatives, the BCD Pay International Marketplace, and online infrastructure. BCD will continue to work towards making the coin increasingly accessible and usable.

References

- Satoshi Nakamoto. Bitcoin: *A Peer-to-peer Electronic Cash System.* https://bitcoin.org/bitcoin.pdf, Oct 2008.

- Bitcoin Wiki: Taras (last edit). *Hardfork.* https://en.bitcoin.it/w/index.php?title=Hardfork&oldid=64319 Nov, 2017.

- Eric Lombrozo, Johnson Lau, Pieter Wuille. BIP-141: *Segregated Witness.* https://github.com/bitcoin/bips/blob/master/bip-0141.mediawiki, Dec, 2015.

- Wang Xiaoyun, Yu Hongbo. *SM3 Cryptographic Hash Function.* http://ris.sic.gov.cn/EN/Y2016/V2/I11/983# Nov, 2016.

- Joseph Poon, Thaddeus Dryja. *The Bitcoin Lightning Network: Scalable Off-Chain Instant Payments.* https://lightning.network/lightning-network-paper.pdf, Jan, 2016.

- Marek Palatinus, Pavol Rusnak. *BIP-44: Multi-Account Hierarchy for Deterministic Wallets.* https://github.com/bitcoin/bips/blob/master/bip-0044.mediawiki Apr, 2014.

- Neil Booth. *ElectrumX: Features.* https://electrumx.readthedocs.io/en/latest/features.html Apr, 2018.