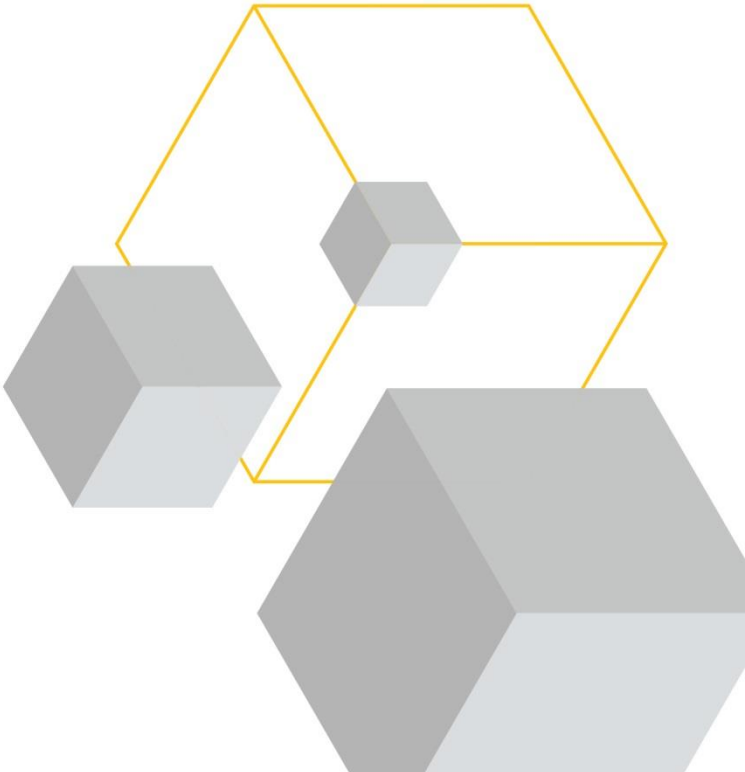


dbos

DISTRIBUTED BLOCKCHAIN OPERATING SYSTEM

WHITEPAPER

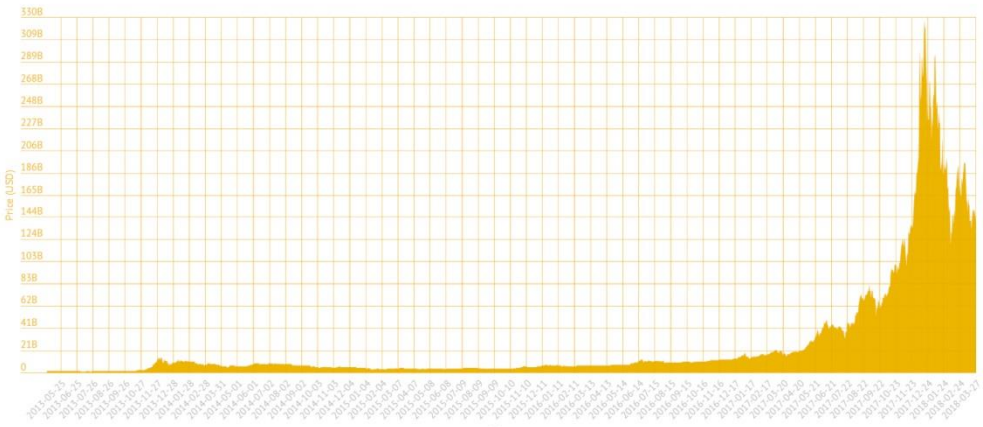
Table of Contents

1. Preface

1.1 What is Bitcoin?

Bitcoin is a digital currency that was released by unknown actor(s) under the pseudonym of Satoshi Nakamoto in the year 2009. The underlying technology seems to have at least partially addressed the Byzantine Generals problem; a problem of how to keep data passing through an untrusted network from being tampered with. Bitcoin has ensured a majority consensus (>50% of actors) by using cryptographic methods in order to simultaneously sign chains of messages and add astronomical computational complexity towards the faking of those signature chains. Bitcoin is revolutionary in the sense that it enabled any given amount of parties to reliably communicate, and transact on a trust-less peer-to-peer system, without the aid of a centralized server or database.

1.2 Bitcoin Market Performance



2. Drawbacks of Current Technology

2.1 First Generation (Satoshi Protocol)

- Transaction throughput of approximately 7 transactions/s/MB of block size is insufficient for decentralized applications/smart contracts, and even day to day purchases for the masses. Although this can be increased somewhat by tweaking blockchain parameters it comes with the side effect of increasing data inflation.
- Creation of “lightning networks” threatens to develop into a heavily fee based market to process transactions quickly; the result of which is that the poor can scarcely afford to use the system.
- Groups of miners threaten to fork the chain if the parameters of the chain are modified such that it threatens their investment in specialized mining hardware.
- Unsuitable for private networks such as internal corporate networks, due to lack of security with low number of nodes/risk of IP exposure if ran publically.

2.2 Second Generation (Smart Contract)

- Typically high confirmation and propagation latency (too much delay) with regards to network receivership due to excess data.
- Users receive all data whether they opt into it or not, resulting in too much unnecessary data propagation and therefore adding to the problem of data over-inflation.
- Improvement on transactions per second is minor.
- Fundamentally not designed for applications and services but being used for this purpose at a great detriment to performance anyways.

2.3 Third Generation (Probabilistic confirmation and others)

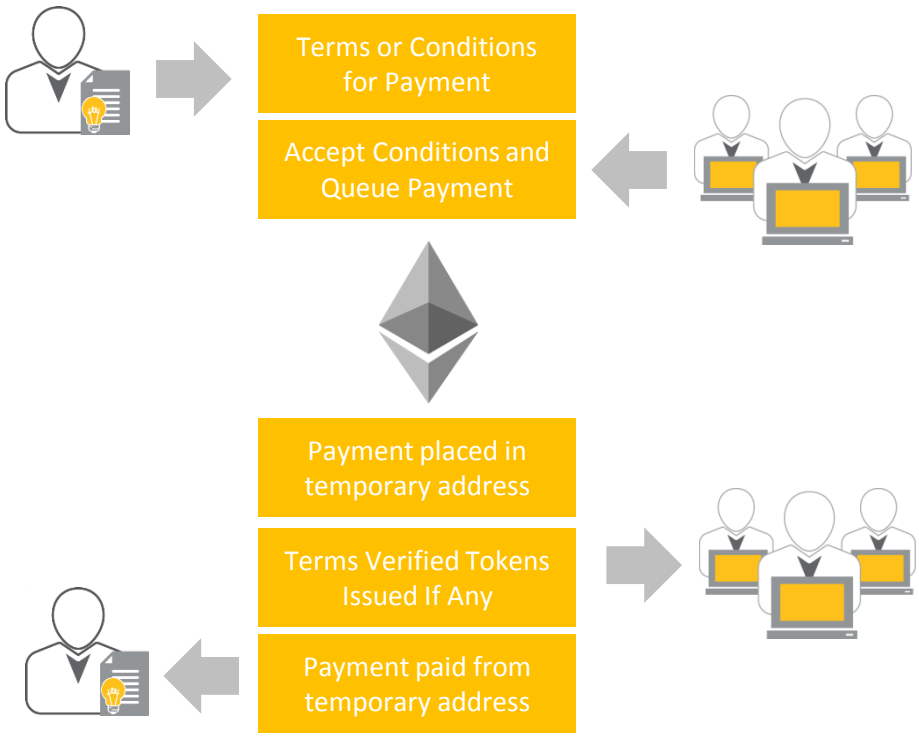
- Possess dubious, unproven, and often cryptographically unsound confirmation practices and are likewise typically not professionally cryptanalyzed.
- Often times based on a patented algorithm which may result in future legal issues with adoption into various platforms.
- Not always open-source/open-tech, and may come with more restrictive licensing.
- Generally not optimized for unified execution of applications, services, and databases.

3. Current Technology vs Proposed Technology

3.1 Current Technology

Traditional Blockchain

Traditional Smart Contracts



3.2 Proposed Technology

We propose to change from the traditional singular linked chain concept to a block-tree type concept. By block-tree we mean that instead of having a single block-chain we choose to have a network of interconnected block chains supported by a single main-chain. To elaborate further, we use the main-chain to provide the majority of the peer to peer network security, whilst side-chains can be optimized for application specific needs.

The difference between our approach and previous attempts to implement a system similar to this are as follows:

3.2.1 Block-tree

Self-Pruning network of inter-linked block-chains, this is analogous to a tree where the trunk of the tree is the main chain, branches are side chains, and leaves are content in any chain. Old branches and leaves specifically referring to content in the network that has not been accessed for a long time(ie: stale) fall off, that is to say they are no longer actively transmitted, and are therefore no longer a burden on the total size of the block tree (achieves space saving).

If an app-developer or other user wishes to, they can revive stale content by reconnecting to the network with the entirety of the defunct but intact chain. Afterwards the content will be broadcasted as available, but not part of the main download set for the block-tree, if another user on the network requests that content it will be revived and be part of the main set (subject to further expiry if it is not accessed again for a while). Content retention timespans may be dictated by a formula that takes into account such variables as number of accesses per day, amount of requests per IP subnet, as well as the overall burden on the network to maintain this information.

3.2.2 Main-chain

The main chain represents the iron-clad records of the network, whenever there is a conflict between different representations of a side-chain, the main chain's rule is law. The idea is to have the main chain be stable software that is actively scrutinized and rarely subject to change. This will ensure the security of the network-wide decentralized checkpointing system which is in place to minimize and possibly prevent potentially bleeding edge technology side-chains from being attacked. This means that side-chains are free to develop whatever features they wish, and still have the security assurance of the main chain should they make a mistake.

In our concept, an interface is established that will allow communication between side-chain apps and the main-chain, the use of the check pointing system will require the use of DBOS coins.

The fees will be set automatically by a formula on the main chain. The end user needs not concern themselves with how much fees to send.

3.2.3 Side-chain

Side-Chains are either decentralized applications, servers, or other uses which wish to take advantage of the security provided by the main chain.
Notably Side-Chains are different from the Main-Chain in that they are configurable in more than one way. Side-Chains can choose to use the Main Chains checkpointing POW system, or devise their own method. They also have a configurable buffer chain that can be used to facilitate low-latency applications.

3.2.4 Buffer-chain

The purpose of a buffer chain is to act as a low latency memory for the chain with minimal proofs. This chain is to be constantly filled by end-applications and be emptied by requests from the side or main chain to sync respectively. When a sync is performed only data marked as permanent is actually written to the side-chain, and then all data at the point of sync is deleted from the buffer chain to prevent bloating.

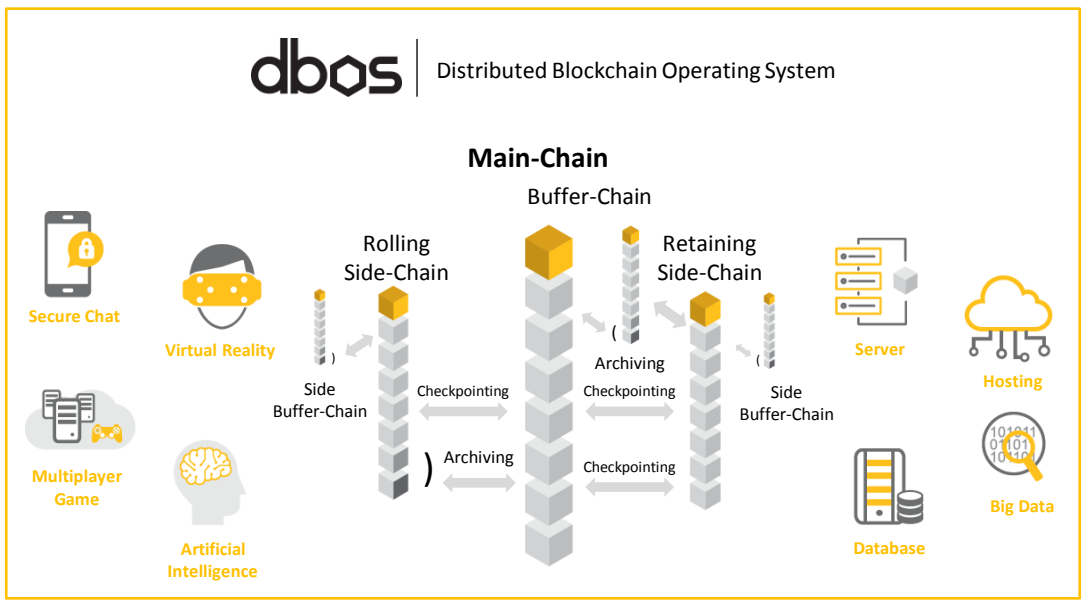
3.2.5 Additional Comments

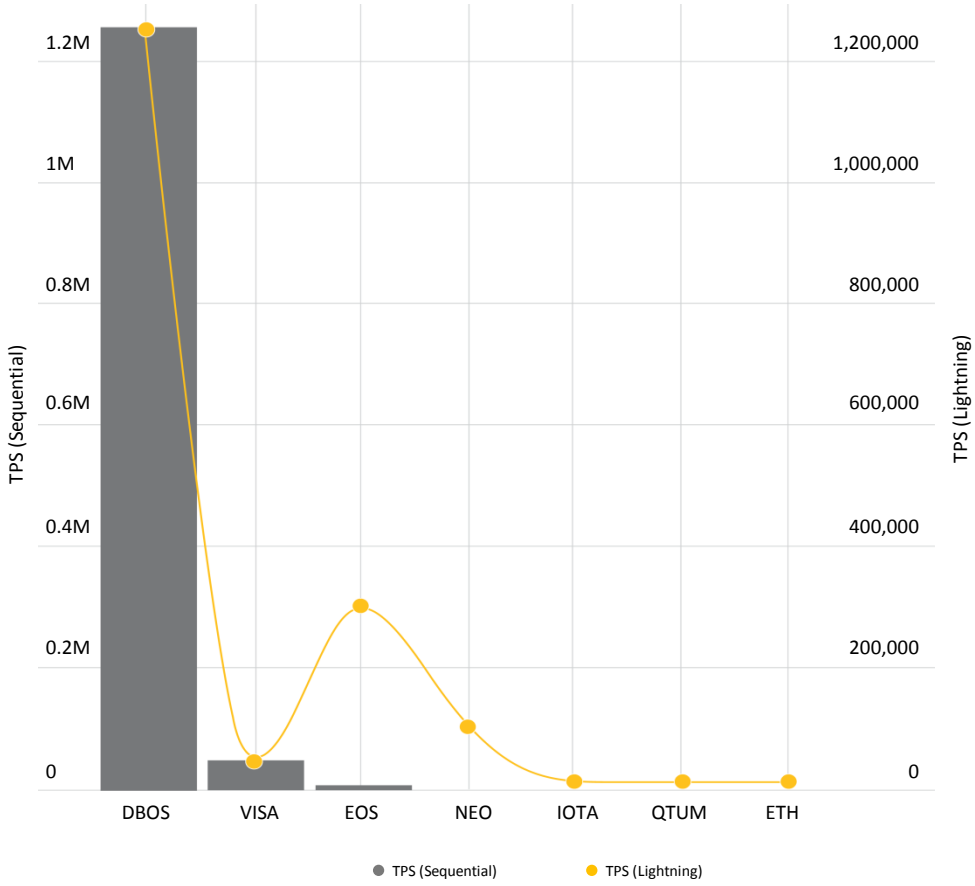
The main chain, has a single buffer chain that facilitates synchronize requests from side chains. Side chains can also have their own configurable buffer-chain.

- Facilitate the main-chain and side-chains to be mined simultaneously by the side-chain users.
- Allow for inter-communication between the main-chain and all side-chains connected to it via a distributed API.
- Scale to multi-million requests or transactions per seconds.
- Facilitate low-latency decentralized applications, services, and databases.
- Reduce network bloat through automatic, intelligent, and reversible pruning.
- Provide some measure of resistance to the threat of future potentially polynomial speed up provided by advances in Quantum Computing.

We will additionally provide the following to facilitate adoption:

- Software for other organizations to build their own side-chains on top of our technology.
- Examples that act as easy to use templates for different types of applications, services, and data.
- API documentation.
- Source code (after an initial marketing settlement period).
- Exchange-Partner fast-track program.




1.2M
1M
0.8M
0.6M
0.4M
0.2M
0
TPS (Sequential)
1,200,000
1,000,000
800,000
600,000
400,000
200,000
0
TPS (Lightning)
DBOS
VISA
EOS
NEO
IOTA
QTUM
ETH
TPS (Sequential)
TPS (Lightning)

4. What D.B.O.S. Enables

Next-generation, decentralized applications (DAPPS) and services

Databases

Databases can be created as side-chains, taking advantage of collation of SQL type statements; multiple statements can be grouped and executed at once to negate the downside of a 200ms response time for high frequency write operations.

Servers and Web Hosting

Requests can be serviced from side-chains, where-by each node can provide a portion of the requested information/data, leading to a system akin to server load distribution but the advantage of being peer to peer; namely being massively distributed.

Low Latency Voting Systems

By leveraging the main-chain's security, private voting systems can be made that can be independently verified without trusting a given governmental entity, or organization. Furthermore, a semi-private system is also possible, whereby voter identity is kept secret but is still checked for uniqueness/validity in the application.

Games

Distributed Peer to Peer game servers can be setup as the buffer-chain technology will allow latency as low as 200ms in a decentralized and virtually immune to denial of service fashion. Drastically lowering the cost of having a consistent world-wide experience game service and eliminating the need for cloud hosting in various geo-locations.

Smart Contracts

Both the main-chain and the side-chains can provide trust-less middleman services for all sorts of contracts, agreements, service for a fee and patent exchange.

Patent Recording

Designs can be time-stamped by the network, resulting in virtually free trustworthy notary equivalent timestamps on patents.

Payment systems

Payments can be handle through both main-chain and side-chain applications; further through smart contracts, custom tokens may be issued without additional software.

Supported Platforms

- Web (Modern Browsers)
- PC Operating Systems: Microsoft Windows 10, Ubuntu Linux, Mac OSX (Java)
- Android (Java)
- IOS client to come (Objective C)

5. Coin Use, Distribution and Sale

5.1 DBOS Coin

DBOS's Coin (DOC) is used for setup of a side-chain, transactions on the main chain, payment for check pointing and API Services (whether coin generation is automatic by shared mining or by lump sum payment by developer for quota.

5.2 Usage Scenario

Used to "buy" security from the main chain, via check-pointing rights as well as archiving rights, by paying for API calls. Also used for DOC transaction fees.

5.3 Proof of Work

Mining on the main chain is done via transaction hashing. This is the same system that other coins like Bitcoin use and has been proven to be a secure method. The blockchain system relies on the leveraging of computational processing power to ensure that the portion of the network, that is in consensus, with the largest amount of hashpower is the custodian of the blockchain. This means that in order for an attacker to gain control of the network, he or she will need at least 51% of the network's hashpower.

We will use a quantum-computer resistant hashing algorithm that will be further elaborated upon in the technical whitepaper. Transaction fees go to miners, lowering coins given over time to side-chains.

5.4 Initial Distribution

Total Supply of BOT will be 500,000,000 Coins.
Private Sale: 25,000,000 are premined, rest are minable.
1% of the rest of the coins are minable per year, over a span of 100 years.

5.5 Usage of Funds

- 57.5% Operations (Ops, BD)
- 30% R&D
- 10% Marketing
- 2.5% Legal

6. Team & Advisors

6.1 Team

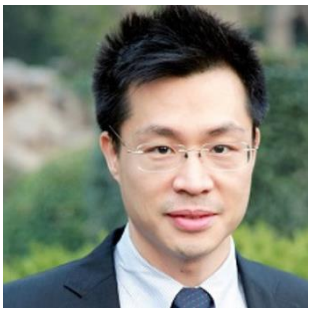
Amir Eslampanah

Chief Architect

Currently regarded as one of the world's top 10 experts in Blockchain and cryptography, Amir has been coding since he was eight years old. He graduated with Honours from the Sir Robert Borden High School and he was a candidate in the University of Waterloo's Honours Software Engineering COOP program for 2 years, where Ethereum founder Vitalik Buterin was a former school mate.

Amir proceeded to drop out of the program and went on to become the lead developer of GoldCoin (GLD). He is credited as the founder of the "Golden River Mining" algorithm. Amir was also part of the initial group known as the "fontas btc-e pump group" that pioneered LiteCoin (LTC). Litecoin started at 0.7 cents and has achieved mind-boggling growth since inception.

6.2 Advisors



Richard Wang

Advisor

Richard Wang is a partner of Draper Dragon and is in charge of investments in artificial intelligence, blockchain, Internet of Things, etc. He was also a part of and invested in YeePay, Nanosic, Innodealing, Epticore, ZGMICRO, IdeeBank and blockchain companies such as Haopu Information and Technology Co. Ltd, Vechain, Metaverse, RedPulse, Chinapex, Alphacat and DAF.

Apart from having over 20 years of experience in technology research and development, Richard is also involved in marketing and holds other key positions mainly in the areas of electromagnetic field research.

He founded EDT Inc. that specialises in the development and sales of telecommunications products. Subsequently, he founded QunZhong E-Commerce and as CEO successfully opened up new sales channels via mobile internet and IPTV. With partners from Silicon Valley, he also founded OLEA Network, a company that researches and develops wireless intelligent ECG sonar by using Doppler radar principles.

Over the past few years, Richard has been focusing on integrated circuits and the Internet of Things in relation to industrial applications. Currently he is embarking into the areas of artificial intelligence and blockchain technology.

Nicholas Ng

Advisor

Mr. Nicholas Ng has over 25 years of experience in the banking and finance industry. As a veteran in the financial industry, he has concluded a wide range of financial transactions, including IPOs, privatisations, and mergers and acquisitions, on behalf of corporations throughout the Asia Pacific, supported by a global network of strategic and institutional investors. His professional career path spans across reputable banks and corporations including stints as the Managing Director of Citicorp Investment Bank for Citibank Singapore, the Regional Asia Head of Investment Banking for Rabobank International and the CEO of Deutsche Morgan Grenfell Securities Singapore. He has been on the board of directors of many companies in Singapore, Malaysia, Canada and Australia.

Mario Singh

Advisor

A widely sought-after thinker in the finance industry, Mario has appeared more than 40 times on international media CNBC and Bloomberg, each time giving his market views to an estimated 350 million viewers worldwide.

As an accomplished corporate consultant, Mario has been brought in by some of the biggest banks in the world to speak to their traders and clients. Some of his clientele include ICBC - China's biggest bank, Julius Baer - the third largest Swiss bank and OCBC – ranked by Bloomberg as the world's strongest bank in 2011.

His two best-selling books "17 Proven Currency Trading Strategies" and "Unlocking the World's Largest Financial Secret" are endorsed by global billion-dollar fund managers like Dr. Mark Mobius, Executive Chairman of Templeton Emerging Markets Group, and David Kotok, Chairman of Cumberland Advisors.

7. Roadmap

2018

May
Lab Setup
Technical Team Formation

July
Initial Product Design

November
Scrum

2019

November
MPV Demo Release
Alpha Desktop Release

December
Alpha Mobile Release
Testing (Desktop and Mobile)

2020

January
Release Beta

March
Release Version 1.0
Future Developments - Smart Contracts DAPPS etc

8. Legal

The purpose of this Whitepaper[henceforth document] produced by the DBOS Foundation [henceforth DBOS Team] is to provide a current overview of the plan for the DBOS Project [henceforth Project].

This document contains copyrighted graphical images that are hereby declared to be either original works or were licensed from their appropriate copyright owners. They may not be reproduced in any way, shape or form, whether in whole or in part without explicit permission from their respective owners.

Furthermore, the diagrams and designs describing the DBOS Project are declared to be copyrighted and patent-pending by Amir Eslampanah.

DBOS Project is declared to be licenced conditionally to DBOS Foundation by Amir Eslampanah as of the date of the creation of this document.

However, the DBOS Project is subject to eventual release under MIT License (see: https://opensource.org/licenses/MIT) and or comparable free patent licence at a further, currently undisclosed, date.

DBOS Team asserts that this document is subject to change with or without notice, and that this document shall in no way, part, or whole, entail a legally binding agreement and or statement with respect to any party regarding the DBOS Project. This document is provided as-is and without any disclaimer of warranty or of the prospective truthiness of the claims, and dates made there-in to the extent of applicable law.