WebDollar

A Peer-to-Peer Blockchain directly in WWW

DRAFT 0.2

Alexandru Ionut Budisteanu
alexandru@budisteanu.net

Abstract. WebDollar is a Browser (WEB) Peer-to-Peer version of cryptocurrencies that would significantly increase the worldwide adoption in order to receive and send payments online directly from one party to another one without going through a financial institution, while the confirmations of transactions are without a Web Server/RPC intermediary that may present security risks. All **cryptocurrencies** are very **hard to be used, requiring** to **install specific terminal applications** for running nodes and mining, **downloading** the **entire blockchain before starting** to mine, and **dedicated wallets software**. To solve the worldwide adoption challenge, WebDollar must be simple to be used by regular people too. **Integrating electronic crypto payments** represent a **difficult challenge** for **web developers** because **Web Applications** have to **communicate** with an **internet protocol** that is **not native** to the **browser** and **HTTP.** Usually, most web applications validate transactions by communicating with an intermediary Web Server (API/REST) that runs a full node and then communicate blockchain results through JSON RPC or WebSockets opening to ??? a new security risk. A Browser (WEB) Peer-to-Peer solution would **simplify** the **usage** of the entire cryptocurrency system because everything (Wallets, Blockchain, Transactions, Payments, API) are handled in Javascript running in every browser, node.js server and Operating System in the world. Javascript is by far the programming language of the World Wide Web. By this way, every browser in the world can i) run and connect as a full-node to the entire blockchain network ii) instantly mine through Pools iii) electronic wallets iv) send and confirm payments.

1. A brief history of currencies and cryptocurrencies.

At the time of writing this White Paper, Bitcoin is peaking at the historical value of 6,000 USD. The market capital value is reaching the psychological value of 100 billion USD, after a 800% surge for the past year.

However, if we put those numbers in the context of the world financial system, they seem meagre - the **entire Bitcoin capitalization is little as 0.11% of the total financial value in the world**. If we add all the other cryptocurrencies to the mix, we don't even get to 0.2% of the total amount of money in the world. This is partly due to the fact that cryptocurrencies are still a fringe and technical topic, requiring specialized technical knowledge from their users.

The usage of cryptocurrencies is very limited and this excludes the older generations, less IT literate people etc. WebDollar aims to tackle this issue by creating world's first browser cryptocurrency, where mining, wallets, transactions and other features are all browser based, providing a level of simplicity never met before.

Ever since the invention of the first currencies, minting coins was the privilege of the ruling power. The face of the king engraved on gold coins was an act of embleming centralized power. That mark of power gained even more importance as the coins, traditionally made out of precious materials, were replaced by paper banknotes transferred their value from material values stored in a bank.

From then, the concept of money slowly turned away from any corresponding objective value, as the nations slowly gave up on the gold standard at the beginning of the 20st century. The digital revolution only sealed this process, giving rise to the digital money, purely fiat currency, with no corresponding real life value whatsoever.

This led to a highly centralized power distribution, in which all the value was created and manipulated by central banks and the ecosystem of commercial banks.

The centralized banking institutions were prone to abuse and not once lead to financial crises, socio-economic disparities and even social conflicts.

Unlike conventional currency, cryptocurrencies are not controlled/regulated by an authority, their value is determined entirely by market. They are also impossible to counterfeit thanks to the complicated mathematical models that encrypt transactions with digital signatures, ensuring complete anonymity and utter safety to every user.

The real breakthrough came in 2008, when an anonymous programmer, known as Satoshi Nakamoto (I truly believe Satoshi is Hal Finney), proposed a new peer-to-peer Prof-of-Work blockchain coin. [1] The benefits includes decentralization, anonymity, finite supply and a matured blockchain infrastructure. The solidity of the currency he created stood the test of time in the last 9 year, and despite a few forks, a bad reputation (unjustly associated with the dark web) and knowing wild fluctuations in value, managed to not only thrive, but also provide a model for a host of other cryptocurrencies that followed it. As of October 2017, there are over 900 cryptocurrencies valued at a total market capitalization of 171 billion USD. [2]

2. WEB Blockchain

Bitcoin is an internet application, but a desktop software that you have download and install it on your computer in order to run the Bitcoin Node. **Without internet, Bitcoin can't be used,** but in the same time **Bitcoin is NOT a Web Application (HTTP)** that works in the Browser and this is the **reason why Bitcoin** is hard to be integrated in real life Web applications of electronic payments. **Difficult development of applications for Bitcoin** is making the Bitcoin blockchain **limited** to **reach massive adoption** by the general public**.** Bitcoin and all Altcoins are very hard to be used by the mainstream. In order to mine Bitcoin or check a transaction, you need to download the Full Node software which is desktop software application, to install in the terminal, configure your miner to a Pool (for mining) and then to download the entire blockchain (200GB in 2017, respectively 70 GB for Ethereum). Converting the desktop software for Blockchain into a Web Application, will make the blockchain accessible to everybody, by just a simple click.

Making the Blockchain available by a single click in the browser, on the World Wide Web, will boost the mass-adoption by individuals and disrupt the Blockchain applications making them to be real-time and easy to develop.

Webdollar is a **Web Blockchain Protocol making the blockchain to be used directly in the browser.**

To include the WebDollar library in a webpage, you just need to write one line:

<script src=”cdn://NodeWebDollar.js”>

Then, on any website that includes the WebDollar library, with just a simple click, you Mine, have Wallets, send payments, check Balance, etc. directly in the browser.

Web is scalable. Desktop is not scalable. For Yahoo! Messenger or mIRC it took 10 years to get traction and disappeared because it was an desktop software that uses internet while, Facebook Messenger is a web application, online, easy to use, anywhere, on any device, compatible and it was in the WEB.

2.1 WebDollar Protocol Solution

WebDollar white paper proposes a blockchain (or mini-blockchain) Proof-of-Work, peer-to-peer scalable solution in Javascript that works directly in any web browser using Websockets and WebRTC.

2.2 Peer-to-peer directly in Browser

For some security reasons, even in the year of 2017, the Websocket Server is not allowed to listen to incoming connections in any of browsers. Moreover, the firewalls and routers make opening Listening Servers a difficult challenge to solve. The only solution to listen to other connections is to use the newly introduced Peer-to-peer WebRTC protocol.

Peer-to-peer protocols for online payments couldn't be done directly in the Browsers before the introduction of WebRTC protocol (2011 first introduction in Chrome) and their adoption by other browsers (Internet Explorer 2015 and **Safari 2017)**. In 2008, when Satoshi proposed the Bitcoin Blockchain, it was totally impossible for him to make Browsers to support Peer-to-Peer communications and back in that time, all browsers didn't support either Websockets and WebRTC protocols.

2.3 A simpler approach for P2P Blockchain in the Browsers

WebDolar (WEB)- Disrupting Bitcoin making it easy to use and develop software

- Cryptographic Software (WEB)
  - Blockchain
    - Nodes (NPM modules and .js dist scripts)
      - **Node-WebDollar Browser**
        - Websocket Client only and WebRTC
        - **IndexedDB** to download p2p the blockchain directly in browser. It can be done with a similar p2p protocol approach like the one done in the WebTorrent, even if the blockchain may have 200GB in a few years.

      - **Node-WebDollar Terminal**
        - Websocket Client & Server, and WebRTC
        - Signaling Server
  - Website
    - Frontend that enables:
      - Hash Mining
      - Pool Mining
      - Running Node

Three types of Nodes:

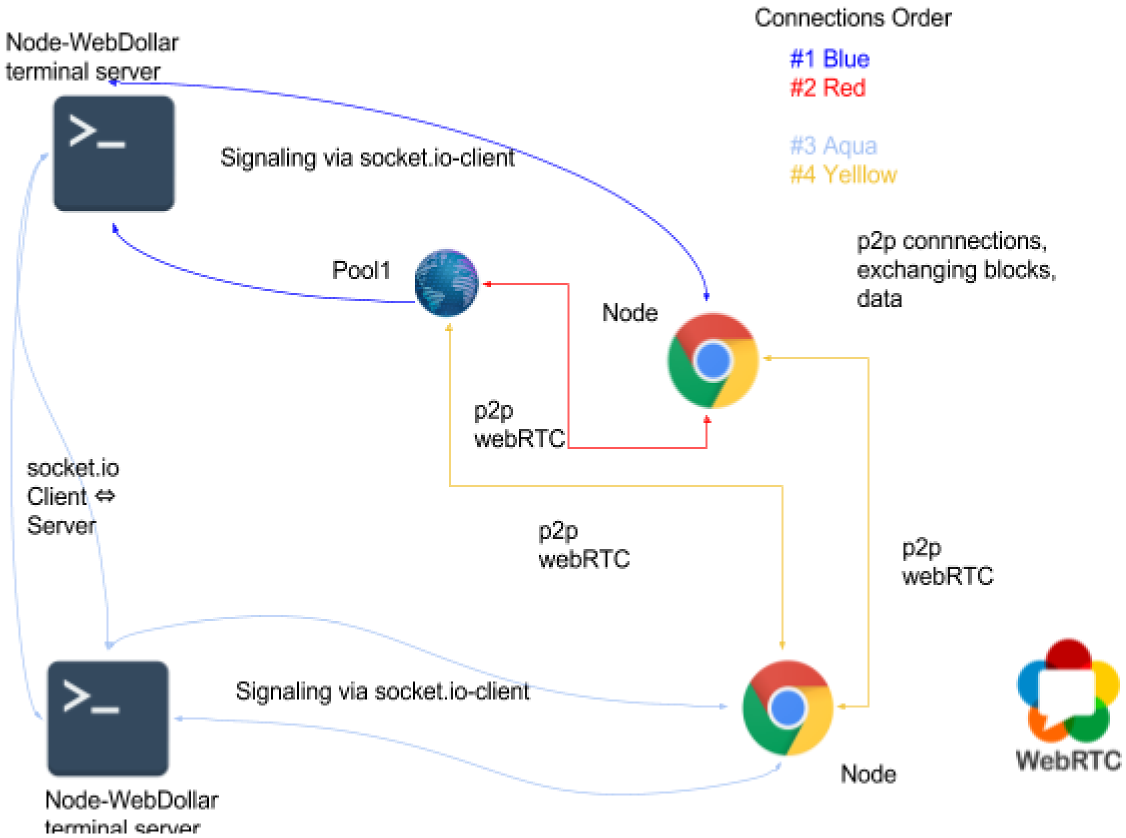
- Nodes
  - Propagate transactions
  - Blockchain
- HASH Miners
  - Argon2 - Hash Functions
  - Processing Hash Functions to distribute the data *
  - Accept Puzzles from POOL Nodes
  - POOL Nodes are picked randomly by the Blockchain miners or via a drop down list
- POOL Nodes
  - Distribute Puzzles to the HASH MINERS
  - **Service** Wallet Information
    - Show your Balance. Randomly picked they communicate with a random Node "Database"

2.4 Signaling Protocol facilitating WebRTC peer-to-peer protocol to work directly in Browser

To use WebRTC protocol and establish peer-to-peer connections between the two browsers, it is required for the two browsers to connect first to a common Signaling Server for acknowledging (signaling) each other. WebDollar is proposing a new solution to this problem by making a special compiled Bundle called "Node-WebDollar Terminal" that runs in Node.js terminal and this bundle can open directly a websocket server directly in the terminal.

After the signaling process is done and the WebRTC connection is established between the two browsers, each Peer will also become a Signaling Server for the other Web Peers connected to them in order to propagate. This will maximize the number of WebRTC peer-to-peer connections in the browser.

WebDollar peer-to-peer protocol for using WebRTC in a Web Blockchain


Node-WebDollar terminal server
Signaling via socket.io-client
Connections Order
#1 Blue
#2 Red
#3 Aqua
#4 Yelllow
p2p connnections, exchanging blocks, data
Pool1
Node
p2p webRTC
socket.io Client ⇔ Server
p2p webRTC
p2p webRTC
Signaling via socket.io-client
Node
WebRTC
Node-WebDollar terminal server

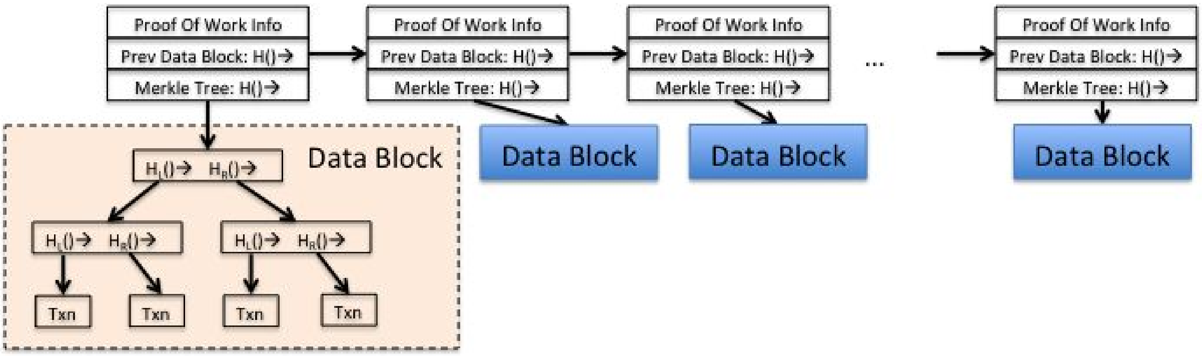
2.5 Javascript

The WebDollar was developed in Ecmascript 6 and using Babel and Browserify, we were able to transpile the library into a pure Javascript bundle that can be executed by every browser in the world. Javascript enables every Mobile, Tablet, Laptop, Computer in the world to execute the Blockchain library directly in the Browser with just one click for: Wallets, Transactions, Balance Check, Blockchain (full node), Mining, and other applications.

2.6 Mini Blockchain for Accountant Tree

2.6.1 Blockchain

Bitcoin is using Blockchain as a data structure in order to keep a track of all the transactions done in the system involving valid bitcoin transfers [1]. The Blockchain introduces the notation of Transaction, but it doesn't have any specific notation for Balance. Merkle Trees are built in order to keep a public ledger of all the previous transactions validating them. The balance of an address is done by processing the Merkle Trees to find and validate previous transactions associated to the specific address. In this way, the balance of an address is calculated every time at request in order to validate the funds of a specific transaction. To calculate the balance, the blockchain system requires to have the entire blockchain downloaded and stored on the hard drive and then for each transaction it needs to track down all the previous transactions involved for the requested address, and so on. This lead many times to access multiple blocks and check multiple Merkle Trees in order to validate just a simple transaction.



A diagram showing the proposed solution of Satoshi's Blockchain concept and a sample Merkle Tree that contains the hashes of a couple of transactions. [1]

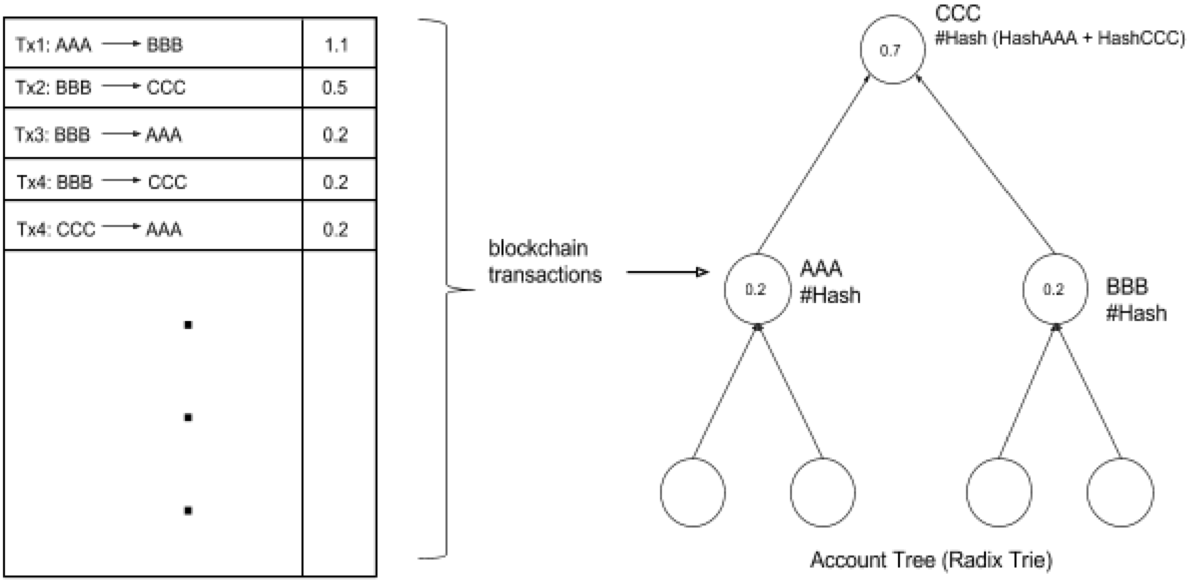
The challenge that comes with Blockchain is that over the time, the size of the blockchain increases exponentially due to the fact that blockchains accept micropayments and the size of keeping Merkle Trees is very large. For example, after just 8 years, Bitcoin blockchain size is 200GB of data, while Ethereum is 80 GB of data and they are still growing.

Because we aim to do Blockchain in the Browser, Pools and Full Nodes (but not Miners) will have to download the entire blockchain data, and in case WebDollar will be adopted in mass by the general public it the blockchain will lead to 200 GB of data in just one year.

2.6.2 Mini blockchain Scheme

Mini blockchain Scheme [3] is a different implementation of a blockchain solution that eliminates the concept of transactions and introduces a new concept of **balance**. The mini blockchain scheme introduces a new data structure namely Accountant Tree in order to keep track of balances of all non-zero addresses.

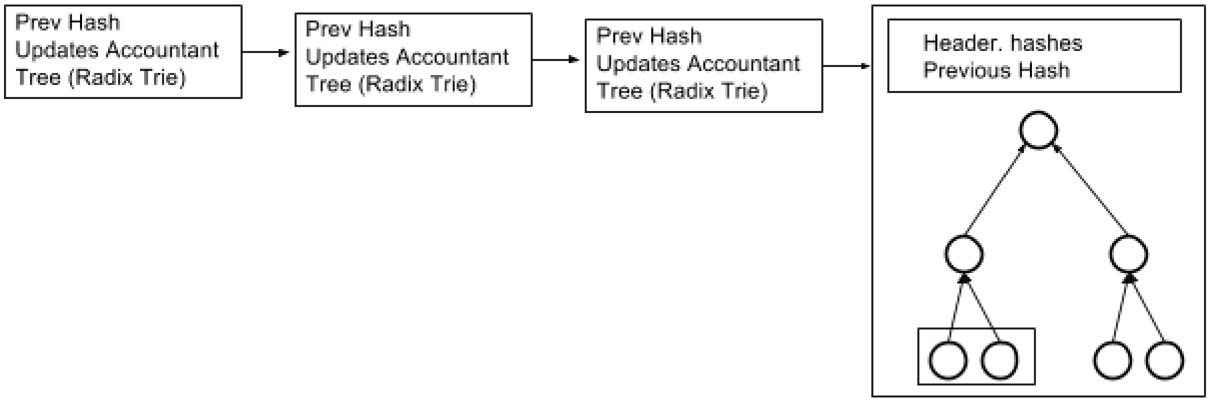
The accountant tree is just **Radix Trie** of storing the balances for all non-zero addresses. So, instead of storing the transactions and a Merkle Tree of the transactions, the mini blockchain scheme stores a Radix Trie for the balanaces of all non-zero addresses.



Tx1: AAA → BBB	1.1
Tx2: BBB → CCC	0.5
Tx3: BBB → AAA	0.2
Tx4: BBB → CCC	0.2
Tx4: CCC → AAA	0.2
. . .	

The blocks in the mini blockchain scheme contains header hashes for validations (like in the normal blockchain scheme) and instead of transactions, the blocks contain the changes that must be done to the Accountant Tree and the new hashes.

Mini blockchain scheme



Prev Hash
Updates Accountant Tree (Radix Trie)
Prev Hash
Updates Accountant Tree (Radix Trie)
Prev Hash
Updates Accountant Tree (Radix Trie)
Header. hashes
Previous Hash

Another advantage in Mini blockchain is that anonymity is maximized because the transactions are not kept in the blocks, but the changes done alongside with their hashes for the Accountant Tree.

2.7 Proof-of-Work Mining ASIC resistant

WebDollar is designed to be a Proof-of-Work blockchain like Bitcoin. The only difference is that we propose the mining to be ASIC resistant for mass-adoption by users. We want to avoid mining farms because this will make the network and mining more centralized and profitable only to a few who invest large sums in dedicated computers. Using ASIC resistant hashing, we want to have more and more people involved in the mining process. At the moment, we propose Argon2 as a Hashing function mining because in 2017, Argon2 is probably the best ASIC resistant hash function. WebDollar community should also take in consideration to adopt other ASIC resistant hash functions in the near future for avoiding ASIC or dedicated mining computers (quantum, etc.).

Each Block, Transactions and Merkle Tree (Account Tree/Radix Trie) is hashed through a Hashing function in order to validate it and the previous blocks making the network to choose only the largest blockchain fork of the network.

A "hash" is an injective and non-invertible function $h(x) = y$. Usually $x = (M, S)$ where M is the message we want to hash, and S is a salt (a random string) . A hash has a few more properties: i) Determinism ii) Defined range iii) Continuity iv) collision resistance (injectivity) v) Compression

A hash function $h(x) = y$ to be ASIC resistant must be memory intensive, where a memory array $B[]$ must be filled with a compression function G and indexing functions $\varphi i()$:

$$B[0] = H(M, S);$$
$$B[i] = G(B[\varphi 1(i)], B[\varphi 2(i)], \cdots, B[\varphi k(i)]) \quad i = 1, t;$$

Argon2 [4] is based on a internal permutation compression function G with two inputs of 1024-byte, a 1024-byte output and an internal a $Blake2b$ hash function H. For avoiding parallelism, the function G is iterated m times. To be memory intensive, at the step i a block with index $\varphi(i) < i$ is taken from the memory array $B[]$ and $\varphi(i)$ is either determined by the previous block in Argon2d.

The generalization of Argon2 ($t > 1$) is described in [4], where it clearly shows the memory intensive usage:

$$B^t[i][0] = G(B^{t-1}[i][q-1], B[i'][j']) \oplus B^{t-1}[i][0];$$
$$B^t[i][j] = G(B^t[i][j-1], B[i'][j']) \oplus B^{t-1}[i][j].$$

where, $\oplus$ is XOR and block $B[i'][j']$ may be either $B^t[i'][j']$ for $j' < j$ or
$B^{t-1}[i'][j']$ for $j > j'$

Once the T iterations have been done over the entire memory array $B[]$, it is necessary to compute the final block B_{final} by XOR-ing the last columns

$$B_{final} = B^T[0][q-1] \oplus B^T[1][q-1] \oplus \cdots \oplus B^T[p-1][q-1]$$

It is obvious that Argon2 is memory intensive to calculate B_{final} in order to get the output of the hash function. This property of being memory intensive, at the moment in 2017 put great challenges for semiconductor manufacturers to create fast and optimized Application-specific Integrated Circuits. By using Argon2 or in the future other memory intensive hash functions, WebDollar would be mined by the computers of individuals and not by mining farms.

2.7 Advantages

- **WEB** - It was Designed and Oriented for Web Application Development
- **Online** directly in your browsers.
  - Full Nodes in Browser
  - Wallets online
  - Mining online - 5 sec to start mining
  - Transactions
  - Receive payments - confirmation
  - **Ballance**
- **Referral systems 2 types**
  - Recommending others to mine in your pool
  - Mining in users' browser when they access your website
- **No Installation**
- **No Download**
- **No Terminal**
- Javascript - Everything is in Javascript and executed in the browser or directly by Operating Systems (Android, iOS).
- **ASIC Resistant** using Argon2
- **Additional Informations** (it is like on Ethereum Protocol with smart contracts)
  - **OnSuccess payment**
  - **OnFailure payment**

Make a separate website Node service that checks for the confirmed blocks and after everything is confirmed run the events.

- You can check your Balance online asking 5 different miners from 5 continents
- Validate Addresses

2.7 Mining Difficulty

WebDollar is a blockchain Proof-of-Work decentralized solution and we propose this Mining Difficulty inspired from the Bitcoin.

The Bitcoin Difficulty is adjusted every 2016 blocks ($2 \cdot 7 \cdot 24 \cdot 60\ min \cdot 1\ /\ block_{time}$, where $block_{time}$ is $10\ min$). The difficulty can described as if the ΔT to get 2016 new blocks was less than 2 weeks $\Rightarrow$ higher Difficulty, otherwise $\Rightarrow$ lowering Difficulty **[5]**

2.8 Controlled Supply

New coins are created each time a user "discovers" a new block that matches the global mining complexity. Rewarding block . There are two types of controlled supplies.

2.8.1 Control Supply based on Scarcity

Bitcoin controlled supply is based solely on a scarcity model. The rate of block creation is adjusted every 2016 blocks to aim for a constant 2 week adjustment period. The number of bitcoins generated per block is set to decrease geometrically, with a 50% reduction every 210,000 blocks, or approximately 4 years. The result is that the number of bitcoins in existence is not expected to exceed 21 million. The block reward adjustment can be approximately modelled by the following equation: [6]

$$\frac{\sum_{i=0}^{2^5} 21\cdot \frac{50.10^{8}}{2^{i}}}{10^4}$$

The decreasing-supply algorithm was chosen because it approximates the rate at which commodities like gold are mined in the real world. This decreasing-supply algorithm increases the value of the coin based on scarcity.

This decreasing control supply leads to astronomical price value like 6,000 USD of Bitcoin as it is now in 2017. At the moment, only about 5 million people had used Bitcoin to make a real financial transaction for a service or good. In case Bitcoin would have been used by 1 billion people, probably the price of 1 Bitcoin would be 5 million USD. This decreasing control supply based on scarcity will lead to **astronomical fees and prohibitive prices** for 1 BTC. Because WebDollar is aiming a global adoption, the controlled supply requires to be adjusted taking in consideration a worldwide adoption by people (hundreds of millions of users even billions).

2.8.2 Control Supply based on demand

WebDollar proposes a controlled supply based on the demand in order to solve problems of Bitcoin like high transactional fees and prohibitive prices of just 1 coin. To avoid scarcity, the WebDollar introduced a new notation of inflation. The inflation needs to exists in the Controlled Supply Rewarding algorithm, but in the same time it must be controlled to make the inflation to be lower and not affecting the price to go down.

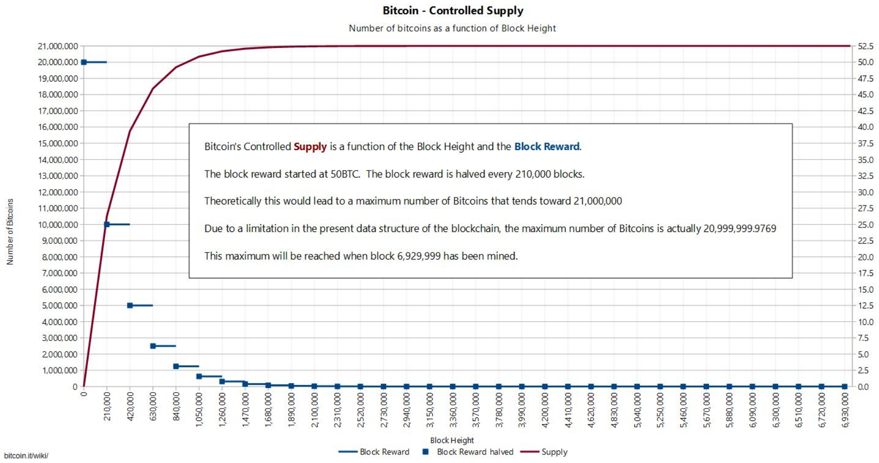
Because WebDollar is using an ASIC resistant hashing algorithm, the mining is more decentralized, thus as the hashing rate θ grows, the number of distinct user miners grows. Because the hashing rate grows θ, the mining complexity ε increases giving a representation of the global hashing rate. Rewarding more coins as the global Hashrate grows will create a small inflation to adjust the price for avoiding WebDollar to become prohibitive.

$$\Lambda (Block_{Index}) = F (\Delta Index) + G (\varepsilon)$$

Where Λ is the Block Reward, F is the decreasing supply control and G is the inflation function, θ is the current hashrate, ε is the mining complexity.

$$F (\Delta Index) =$$

$$G (\varepsilon) =$$


Bitcoin - Controlled Supply

Number of bitcoins as a function of Block Height

Bitcoin's Controlled Supply is a function of the Block Height and the Block Reward.

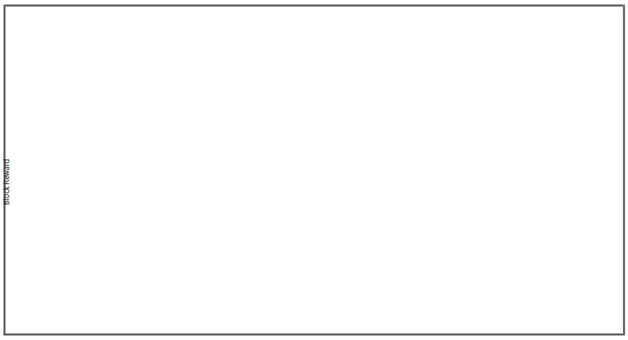
The block reward started at 50BTC. The block reward is halved every 210,000 blocks.

Theoretically this would lead to a maximum number of Bitcoins that tends toward 21,000,000

Due to a limitation in the present data structure of the blockchain, the maximum number of Bitcoins is actually 20,999,999.9769

This maximum will be reached when block 6,929,999 has been mined.

bitcoin.it/wiki/



[6] Bitcoin Controlled Supply based on scarcity

WebDollar Controlled Supply

2.8 Security concerns

2.8.1 Security in Blockchain

WebDollar is inheriting all the security advantages from the blockchain solution proposed by Satoshi (Hal Finney).

For hacking the blockchain, the attacker needs to build a longer valid blockchain. To build a longer valid blockchain, the attacker will need 50%+ of the blockchain network hashrate. Because of this, the attacker is in a competition with others and it will be more profitable for him to become a miner instead of remaking the blockchain from scratch or even forking the blockchain to keep the rewards.[1]

For hacking the entire blockchain, the attacker needs to build a longer blockchain starting from the genesis block, and for this is almost impossible to due fact he needs to dominate a large the network for a longer period of time. In case the attacker hasn't a next generation technological advantage (quantum computer), the attacker must have the network domination over a similar ~timespan since the genesis block.

2.8.2 Security in Mini-blockchain scheme

Another implementation that is taken in consideration for WebDollar is using mini-blockchain of storing the Accountant Tree instead of using Transactions Merkle Trees. The security concerns for using the mini-blockchain are very similar with Satoshi's Prof-of-Work Blockchain solution. [3] [2]

3.1. Built-in Scarcity May Support Value and protect against inflation

Most cryptocurrencies are hardwired for scarcity – the source code specifies how many units can ever exist. In this way, cryptocurrencies are more like precious metals than fiat currencies. Like precious metals, they may offer inflation protection unavailable to fiat currency users. Inflation is almost non-existent in the cryptoworld, but it still exists to financially incentivize the production of blocks. The adoption of Proof-of-Stake protocol will further decrease inflation and make cryptocurrencies even more valuable (the Ethereum network will adopt hybrid POW/POS at the end of 2017). The most important part here is that the inflation is known, this number is not hidden by anyone. In case of central banks, the inflation rate is not known, the banks irresponsibly print a lot of fiat without general population approval. This is one of the major reasons true believers are hyped about cryptocurrencies.

3.2. Loosening of Government Currency Monopolies

Cryptocurrencies offer a reliable means of exchange outside the direct control of national banks, such as the U.S. Federal Reserve and European Central Bank. This is particularly attractive to people who worry that quantitative easing (central banks' "printing money" by purchasing government bonds) and other forms of loose monetary policy, such as near-zero inter-bank lending rates, will lead to long-term economic instability.

In the long run, many economists and political scientists expect world governments to co-opt cryptocurrency, or at least to incorporate aspects of cryptocurrency (such as built-in scarcity and authentication protocols) into fiat currencies. This could potentially satisfy some cryptocurrency proponents' worries about the inflationary nature of fiat currencies and the inherent insecurity of physical cash.

3.3. Self-Interested, Self-Policing Communities

Mining is a built-in quality control and policing mechanism for cryptocurrencies. Because they're paid for their efforts, miners have a financial stake in keeping accurate, up-to-date transaction records – thereby securing the integrity of the system and the value of the currency.

3.4. Robust Privacy Protections

Privacy and anonymity were chief concerns for early cryptocurrency proponents, and remain so today. Many cryptocurrency users employ pseudonyms unconnected to any information, accounts, or stored data that could identify them. Though it's possible for sophisticated community members to deduce users' identities, newer cryptocurrencies (post-Bitcoin) have additional protections that make it much more difficult.

3.5. Harder for Governments to Exact Financial Retribution

When citizens in repressive countries run afoul of their governments, said governments can easily freeze or seize their domestic bank accounts, or reverse transactions made in local currency. That's not possible with cryptocurrencies, whose decentralized nature – funds and transaction records are stored in numerous locations around the world – effectively prevents state seizure. It's a bit of an oversimplification, but using cryptocurrency is like having access to a theoretically unlimited number of offshore bank accounts.

3.6. Generally Cheaper Than Traditional Electronic Transactions

The concepts of block keys, private keys, and wallets effectively solve the double-spending problem, ensuring that new cryptocurrencies aren't abused by tech-savvy crooks capable of duplicating digital funds. Cryptocurrencies' security features also eliminate the need for a third-party payment processor – such as Visa or PayPal – to authenticate and verify every electronic financial transaction.

In turn, this eliminates the need for mandatory transaction fees to support those payment processors' work – since miners, the cryptocurrency equivalent of payment processors, earn new currency units for their work in addition to optional transaction fees. Cryptocurrency transaction fees are generally less than 1% of the transaction value, versus 1.5% to 3% for credit card payment processors and PayPal.

3.7. Fewer Barriers and Costs to International Transactions

Cryptocurrencies don't treat international transactions any differently than domestic transactions. Transactions are either free or come with a nominal transaction fee, no matter where the sender and recipient are located. This is a huge advantage relative to international transactions involving fiat currency, which almost always have some special fees that don't apply to domestic transactions – such as international credit card or ATM fees. And direct international money transfers can be very expensive, with fees sometimes exceeding 10% or 15% of the transferred amount.

3.8 Transparency

Another great point is transparency. You cannot cheat the system without letting others know about that. This is why Bitcoin or Ethereum had their rough days with someone exploiting the loopholes, but due to the fact that everyone could see what was happening, the loopholes were closed in a short period of time with the determination of community and developers.

4. Shortcomings of current cryptocurrencies

As with any emerging technology, and moreso, socio-economic construct, cryptocurrencies still have a lot of challenges and hurdles to face. As diverse as they are, they can be gathered into 3 main categories:

4.1 Regulation aspects

Traditionally, states and state-backed centralized banking institutions had the monopoly over creating currency. And since that monopoly is not only an attribute of power but also the main source of it, they want to keep the status quo going. That is the main reason why there are so many reglementation hurdles for cryptocurrencies today. Not all hope is lost though, as in the battle with monolithical colossi the cryptocurrencies have the support of individuals and history proven not once that over time, the will of individuals can overcome institutions.

4.2 Technical aspects

vulnerability to DDoS attacks, Blockchain size, and bandwidth TPS (transactions per second), creating a mechanism for token allocation to counteract Sybil attacks.

4.3 Architecture of consensus and lack of a chargeback system.

PoW leads to mining centralization and technological centralization, PoS makes it possible for the attacker to maintain parallel block chains without high costs. Also, the entire concept of decentralized anonymity leads to the impossibility to get money back in case you did a wrong transaction or if your private key is exposed. For example, Visa and Mastercard issuers fund "Zero Liability" protection to protect cardholders against loss if their account information is lost or stolen. In the cryptocurrency world, each (average) user is on their own and if they lose their funds, the money is basically gone. There's no dispute or chargeback system if a user's account is hacked.

4.4 Economic issues

We should mention the challenge of **hyper-volatility**. In conditions of limited supply, the rate will depend on demand. And this value is directly related to the subjective attitude of the users, which can change as only humans can. You cannot do any kind of quantitative easing with bitcoin, since coins are only created as fast as processing networks can solve blocks.

Between January 2013 and November 2013, the price of Bitcoin rose 8,313%, the collapsed to half of it's value. These types of price fluctuations make it incredibly difficult for businesses and consumers to make their financial decisions. Because of this volatility, cryptocurrencies are highly used by speculators and not often used for long term savings. There are some incredibly high rewards available for speculators, and this has positioned most cryptocurrencies as more of an investment than a means of payment.

Unfortunately, if cryptocurrencies truly want to be the payment system of the future they need to reward people who use it for its intended purpose – a means of payment.

Another major problem is that money Is Created at A Depreciating Rate.

Changing the rate at which currency is created is a common way for governments to regulate the economy. In times of economic hardship, more money is printed. Although this causes inflation, this allows more currency to flow into the economy. The rate at which money is printed is closely controlled by the government to best stimulate the economy.

Most cryptocurrencies do not follow this system. Money is instead created at a quickly depreciating rate. In the case of bitcoin, by 2025 there will be no new coins on the market. Once every coin has been released, the currency could experience hyper-inflation.

But perhaps above all the previous issues, the main disadvantages arresting the adoption of Bitcoin and other cryptocurrencies is their poor rate of absorption/use at the level of the global population.

According to a report by Juniper Research, the number of active Bitcoin users around the world could reach 4.7 million people by the end of 2019, and even now the network has reached the capacity limit of 250 thousand transactions.

At a similar time in its history, PayPal had over 100 million active accounts, despite the fact that it started with a less developed infrastructure and required passport details to use. That’s a massive difference, even though there are stark differences in the ease of use of PayPal compared to Bitcoin.

The technical jargon, the esoteric functioning of mining, wallet administration and many other crypto concepts are hard to swallow for the average citizen and require a steep learning curve. At a certain point, this was one of the bragging points of the IT elite, but in order to have a real impact in the society, cryptocurrencies must be redefined as being extremely intuitive and simple to use.

That means solving the following problems:

- Loss of your wallet password means you lose your money. Generating, administrating and operating with a wallet should become as intuitive as using a credit card, if not easier. As long as this problem is not solved, convertibility will be impacted - It is still too difficult for the average person to find the "right" wallet and purchase currency.
- Very large database file necessary for verifying transactions. This hinders the use of bitcoin mining on mobile devices, restricts the access in the network of people with less modern PCs and overall, it is a waste of resources.
- The injustice of early adopters. The Bitcoin craze begun with a very small community of geeks, getting tens of thousands of Bitcoins with their PCs, while today the miners can’t get even thousandth of Bitcoin using similar resources as the early adopters, due to the decreasing reward system in a limited supply economy.Perhaps it is time for another cryptocurrency to offer a restart of the “gold rush”, with the fairness provided by easy access to a simple cryptocurrency, devoid of technical jargon and steep learning curves.
- Achieving the network effect. To have a stable and sustainable ecosystem, you need to include incentives for people to invite their peers into the network. While there are indirect incentives to help the network grow, usually cryptocurrencies ignored the social mechanism of incentivising sharing and inviting.

WebDollar Transactions

1) **Sending Funds**

Alice → Bob

Public Address ALICEXXX1 Public Address BOBYYY1

Amount 0.5 WBC
GasMiner 0.000000000000001 WBC
GasMinerDB 0..000000000000001 WBC

```
Additional Information{                    (like Ethereum smart contracts)
    msg: "Payment Done to Bob"
    onSuccess:  "http://CurrencyApp.com/api/paymentSuccess"
    onFailure: "http://CurrencyApp.com/api/paymentError"
}
```

Validation Digital Signature using SHA11 Private Key (like on Bitcoin)

Sample **HTTP POST**

```
onSuccess(sourcesAddresses, destinationAddresses, transactionId ){
      The reason why Value is not included is to don't allow fake requests allowed

       Amount = Transactions.get (transactionId)
       Or
       TotalAmount = Ballance.get (destinationAddresses)
}
```

2) Setting Account Information

Alice
Public Address ALICEXXX1

Gas 0.0 WBC

```
Additional Information{
    emailAddress: test@test.com
    handle Name: unique_username_cool
}
```

REWARDS

1. Miner is rewarded with 25 WEB

Implementation:

Node.js
Argon2

2.9 Steps to Achieve WebDollar

1. Generator of Public Addresses and SHA256 private keys
    a. Better and Longer Public Address for better Security
    b. Prefix "WEB_" for address like WEB_ sau WEB#
2. Nodes
    a. Block Node (middleman)
        i. Websockets - connect Network
            1. Discover other Block Nodes creating a complete Graph (p2p)
            2. Propagate Transactions through the Network
            3. Propagate new Blocks
        ii. **Websockets Services** like:
            1. New Transaction
                a. Change Username/Email
            2. Calculate Balance (pick 5 random DB Nodes and ask them about balance)
    b. Pool Node
        i. Websockets - connect Network
            1. Connect to Block Nodes
            2. Discover other Pool Nodes creating a complete Graph (p2p)
            3. Propagate Blocks through the Network
            4. Propagate new Blocks
                a. Read New Blocks
                b. Mitigate New Blocks (in case there are multiple blocks)
                    i. Exactly like Bitcoin
                c. Propagate New Blocks
                d. Solve HTTP Events **Obs1** - OBSOLETE
            5. Calculate and Adjust New Complexity **2**
        ii. Hard Disk usage
            1. Read/Write data from Hard Disk using **Merkle Tree**
                a. To Read/Write data in the browser on the HDD we can use the browser technology used in WebTorrent
                b. Bitcoin blockchain requires 200 GB (at the moment). In 2013, it was 20 GB
        iii. **Websocks Services** to return data like

         1. Balance using Computed Hashes
      iv. Pooling (tutorial)
         1. Websockets to communicate with Miners
         2. Generate Merkle Tree
            a. Retrieve new Transactions from the Block Nodes (middleman) and filter by Fees
            b. Create Merkle Tree grouping Transactions into a new Block
            c. Calculate Merkle Tree Hash (transaction Hash)
         3. Generate New Puzzles Taks
         4. Send Puzzles to Miners
         5. Retrieve puzzle answers from Miners and data
            a. Validate Puzzle Answers
            b. Store Performance of Miners in a local DB (Cookie/File)
               i. Retrieve Pay Day Address
         6. When Block solved propagate the solved block to Pools Nodes
         7. When Requested or Miner didn’t have any activity in last 30 days, send his money to his address
         8. Calculate New Complexity **2**
   c. Mining Node
      i. Websockets - connect Network
         1. Discover Pools Miners (p2p)
         2. Connect to Pool
            a. Get Puzzle
            b. Start Solving Puzzle
               i. Hashing
            c. Communicate Answer Puzzles and Your Address
         3. Calculate New Complexity **2**

3. Pool
   a. Websockets - connect Network
      i. Communicate with Nodes
      ii. Coordinate Available Mining Nodes

Problems of Bitcoin:

1. To calculate the Balance you need to process all previous blockchain data (transactions). It is a desktop software application in terminal
2. To send transactions, you need to communicate with these Nodes terminal applications via sockets
3. Hard to write Web Apps
    a. Send money - needs to communicate with the Nodes
        i. No Notification if the money has been sent successfully. Theoretically you have to wait at least 10 minutes to receive a notification.
    b. Receive money - needs to communicate with the Nodes
        i. Check balance (either download the Blockchain data or use JSON RPC)
            1. No Notification if the money has been received successfully. You have to check it yourself - manually. Theoretically you have to wait at least 10 minutes to receive a notification.

Although 6 years has passed from 2009, only **1-5 million people used** Bitcoin. The reason why so few people used Bitcoin is because it is **hard** to use the Blockchain in real time web applications and solutions.

To send money is easy, but to receive money is harder.

Special thanks:

Special thanks to **Adrian Mihai Stratulat** for helping writing this White Paper

References:

[1] Satoshi Nakamoto (Hal Finney) - Bitcoin: A Peer-to-Peer Electronic Cash System

[2] Bitcoin's Market Cap Is Now More Than $100 Billion https://www.forbes.com/sites/cbovaird/2017/10/20/bitcoins-market-cap-is-now-more-than-100-billion/#41bc4eea2b8b

[3] J.D. Bruce - The Mini-Blockchain Scheme

[4] Alex Biryukov, Daniel Dinu, and Dmitry Khovratovich - Argon2: the memory-hard function for password hashing and other applications

[5] Bitcoin Difficulty - https://en.bitcoin.it/wiki/Difficulty

[6] Bitcoin Controlled Supply - https://en.bitcoin.it/wiki/Controlled_supply

[7] Bitcoin Controlled Supply Chart - https://en.bitcoin.it/w/images/en/4/42/Controlled_supply-supply_over_block_height.png