WebDollar

Cryptocurrency Native to the Web

DRAFT 0.4

Alexandru Ionuț Budişteanu

Abstract WebDollar (WEBD) is a Browser-based Peer-to-Peer cryptocurrency that aims to significantly increase the worldwide adoption of decentralized currencies. WebDollar offers the possibility to send and receive payments online on any Browser, directly from one party to another, without going through a financial institution, while the confirmations of these transactions are secure on the blockchain without passing them through potential vulnerable channels like a Web Server or RPC intermediary as in BTC. **Cryptocurrencies** have been very **technical, requiring** the **installation of specific terminal applications** for running nodes and mining, **downloading** the **entire blockchain before starting** to mine, and **dedicated wallet software**. To solve the worldwide adoption challenge, WebDollar focuses on three core advantages:

1. Simplicity - offering an intuitive and non-technical user experience, meant to not only be used by IT-savvy crypto-enthusiasts, but by regular people, as well.

2. Lightness - WebDollar introduces a **trustless light node** of the blockchain for mining and verifying transactions without requiring to download the entire blockchain history from Genesis, but only the hardest proofs and blocks that distinguish attackers to honest nodes (miners) who keep the correct blockchain. This breakthrough light version of the Blockchain is called Non-Interactive Proofs of Proofs of Work (NiPoPoW) and was proposed by some researchers. [2]

3. Ease of integration with the Web - **Integrating electronic crypto payments** represent a **difficult challenge** for **web developers** because at the moment **Web Applications** have to **communicate** with an **internet protocol** that is **not native** to the **browser** or the **HTTP** layer**.** Most web and mobile apps validate transactions by communicating with an intermediary Web Server (REST) that runs a full node and communicates blockchain results through JSON RPC or WebSockets opening the apps to new security risks. 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 trustless running in every browser, node.js and OS. As such, every browser in the world could i) run and connect as a light node to the entire WebDollar blockchain network trustless in seconds ii) instantly mining iii) Referral Pools iv) digital wallets in browser iv) send and confirm payments.

1. A brief history of money and cryptocurrencies: evolution, devolution, and revolution

Money responds primarily to the need for indirect exchange. This need is natural and emerges immediately as an economy grows past the most basic levels. As soon as the nexus of exchanges becomes greater than a few families and types of goods exchanged, the problems of *non-coincidence of wants* and *indivisibility* of directly exchanged goods become significant.

When two individuals want to exchange two goods and have one of the aforementioned problems, a third good is the solution. Exchange becomes a two-step process instead of a one-step process. First you buy an intermediary good with the good you want to sell. Then you exchange *some* of the intermediary good (or medium of exchange) for the good you want to buy, *now or later*.

Conceptually and historically, we can see and understand how society selected a money out of the goods it already produced. A medium of exchange that is selected for its marketability out of other means of exchange and becomes accepted in virtually all exchanges and for all goods can be finally called money. What money can offer that less adopted means of exchange cannot is social calculability. This is a detail of tremendous importance. When there is a constellation of prices obtained in de facto exchanges intermediated by a type of money, it is possible for people to start thinking entrepreneurially in terms of that money and the possibilities for complex businesses are open.

This generalized adoption process is accompanied by a gradual increase in the purchasing power of money, because more and more people demand it for its monetary services until virtually everybody has some of it on stock. [9] There was a long process of selection out of which the precious metals gold and silver were singled out for their qualities of being easily standardized, checked for authenticity, divisible, fungible, relatively scarce – sand has all the other qualities – and, not to take humans for less the emotional beings that they are, for their sound and esthetics – precious metals are traditionally called sound money for this reason.

Commodity money was the money of the free market. Precious metals were produced and minted by merchants or local rulers in their effort to establish their brands and gain wider circulation in a competitive process. Later, it was merchants and bankers that started issuing money substitutes such as deposit certificates and banknotes to help with long distance payments, clearing, safe keeping, and divisibility.

Parallel to this evolution there was a *devolution* of money. The state has always hijacked, usurped and destroyed for its own interest what the market produced in the interest of people. It happened with money, too. The king's monopoly on minting, the royal branding on coins, debasement, legal tender, exchange rate controls, fractional reserve banking, fiduciary substitutes and finally fiat money without any backing are all poisoned fruits of this devolution.

The juxtaposition of the dire state of money and banking, on the one hand, and the technological advancements of the internet, on the other hand, prompted a revolutionary step. The breakthrough came in 2008, when an anonymous programmer, known as Satoshi

Nakamoto, proposed a new peer-to-peer Proof-of-Work blockchain coin [0]. The benefits include 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 seeing wild fluctuations in value, managed to not only thrive, but also provide a model for a host of other cryptocurrencies that have followed. As of January 2018, there are over 1400 cryptocurrencies valued at a total market capitalization of $740 billion USD.

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

At the time of writing this White Paper, Bitcoin is at the historical value of 14,000 USD, while market capital value is reaching the psychological value of 250 billion USD. However, if we put those numbers in the context of the world financial system, they seem meager - the *entire Bitcoin capitalization is just 0.6% of the total financial value in the world*. If we add all the other cryptocurrencies to the mix, we barely get to 2% of the world total. This is partly due to the fact that cryptocurrencies are still a fringe and technical topic, requiring specialized knowledge from their users.

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

2. WEB Blockchain

Bitcoin is not a web application, but a desktop software that you have to download and install on your computer in order to run the Bitcoin Node connecting to the network. **Without the internet, Bitcoin can't be used,** but at the same time **Bitcoin is NOT a WWW/Web HTTP Application** that runs in the Browser and it requires one to download the entire blockchain history that is 140 GB of raw data. These make **Bitcoin** hard to be integrated in real life Web applications for P2P electronic payments. **Difficult development of applications for Bitcoin** is stopping Bitcoin from **reaching massive adoption** by the general public**.** Bitcoin and all the Altcoins to-date are still very hard to use by the mainstream. In order to mine Bitcoin or check a transaction, you have to manually install the Full Node software, which is a desktop software application; install it in your terminal, configure your miner to a Pool (for mining) and then you need to download the entire blockchain history (140GB in 2017, respectively 70 GB for Ethereum).

WebDollar's solution, to convert the desktop blockchain software into a Web Application, together with a simple UI, devoid of technical terms, will make the blockchain accessible to everybody. A research paper proposed by Aggelos, Andrew and Dionysis proposes a new blockchain architecture called Non-Interactive Proofs of Proofs of Work [2] introducing

interlinks pointers making the WebDollar to be very light and in the same time trustless. Getting rid of the necessity to download the full blockchain also allows for smaller, portable devices to be used for mining, such as tablets and smartphones, whose vast processing power lays mostly dormant.

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 current Blockchain applications, making them real-time, and easy to develop in the world.

WebDollar is a **Web Blockchain Protocol allowing p2p transactions directly in browsers.**

To include the WebDollar library on a web page, you just need to write *one line*:

<script src="cdn://WebDollar-Protocol.js">

Then, your website, with just a single click, can mine, have wallets, send payments, check the balance, etc. directly in the browser, trustless using the NiPoPoW light blockchain.

To include the WebDollar User Interface on a web page, you just need to write *one line*:

<script src="cdn://WebDollar-User-Interface.js">

Then, automatically your website will have the entire User Interface functionality to mine webdollars, verify transactions, send transactions, buy sell WEBD, etc.

The Web is scalable, while the Desktop is not. For mIRC, it took 10 years to get traction, and eventually it became obsolete because it was a desktop software that used the internet. While Facebook Messenger is a web application thats online, easy to use, anywhere, on any device.

2.1 WebDollar Protocol Solution

This WebDollar white paper proposes a mini-blockchain scheme combinated with a light trustless blockchain based on the Non-Interactive Proofs of Proofs of Work [2], and a peer-to-peer scalable solution in Javascript that works directly in any web browser using WebRTC and Websockets for signaling only.

2.2 Mining in WebDollar

1. Mining Pools – light nodes that use NiPoPoW proofs to verify proving the authenticity of the last K blocks without relying on a trusted party. The Mining Pools will have to synchronize to the main network every time they start operating their mining pool.
2. Mining Nodes – receive tasks of new proposed serialized blocks to mine from the Mining Pools (Light Nodes). They just generates tons of nonces and apply the PoW Hash Function to see if the blocks' nonce respect the Mining Global Target (Difficulty) $H(block + nonce) > Target$. The Mining Pools manage and receive the puzzles to generate the next blocks.

2.2 Peer-to-Peer directly in the Browser

For security reasons, even in the year 2018, the Websocket Server is not allowed to be initiated to listen to incoming connections on any browser. Moreover, the firewalls and routers make opening Listening Servers a difficult challenge to solve namely most machines will need to use either a STUN (Session Traversal of User Datagram Protocol) or TURN (Traversal Using Relays around NAT) to connect each others directly in case one of them has symmetric NAT. The only solution to listen to other connections in the browser is to use the newly introduced Peer-to-peer **WebRTC** protocol alongside with a simple Signaling Protocol and a list of public STUN/TURN servers.

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 to enable Browsers to support Peer-to-Peer communication and now Bitcoin cannot be used directly in the Browser.

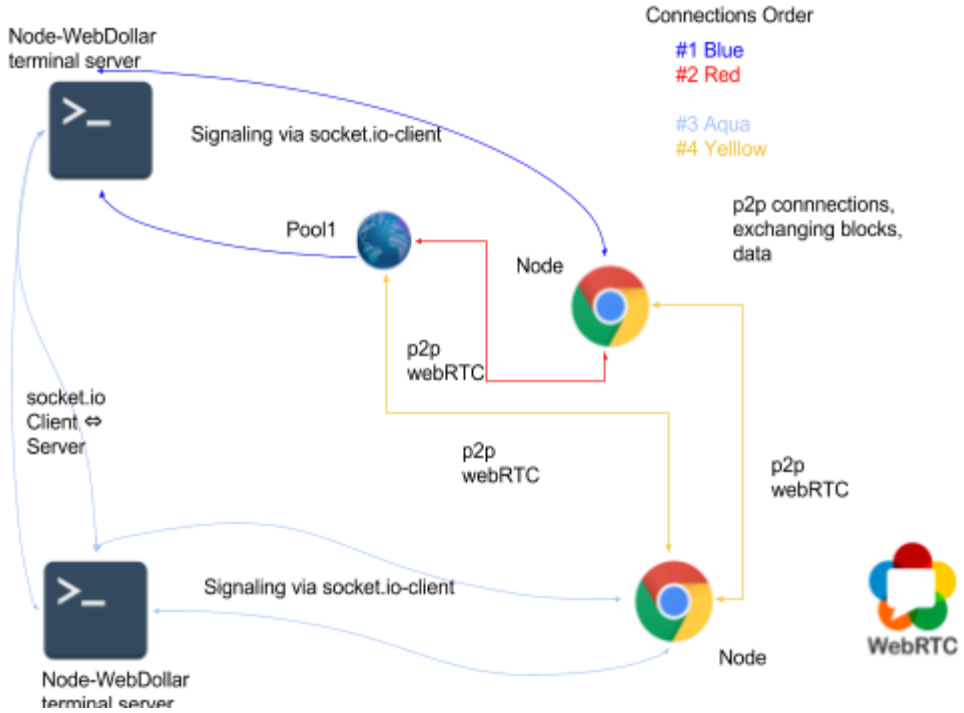
2.4 Signaling Protocol facilitating WebRTC peer-to-peer protocol to work

WebRTC protocol to establish peer-to-peer connections between two browsers requires that the two browsers connect first to a common *Signaling Server* for acknowledging (signaling) each other. WebDollar is proposing a new solution to this requirement by making a special compiled Bundle called the "WebDollar-Protocol", that runs also in the Node.js servers. This

bundle can open a Websocket server directly in the terminal facilitating the browsers to connect each others.

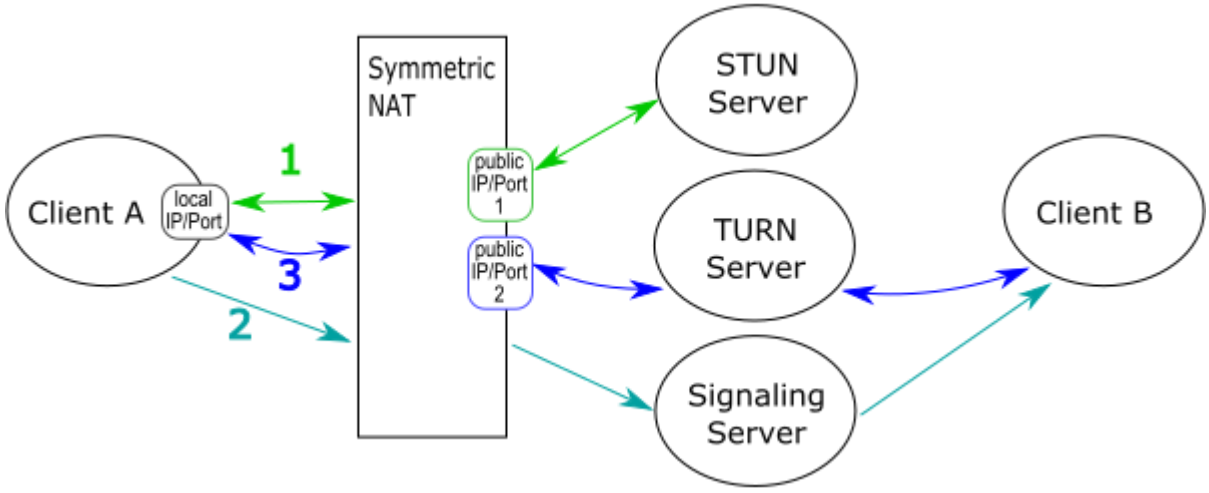
After the signaling process is done and the WebRTC connection is established between the two browsers, each Peer will also become a Signaling Server for the other Web Peers connected to them in order to propagate. This will maximize the number of WebRTC peer-to-peer connections in the browser.

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

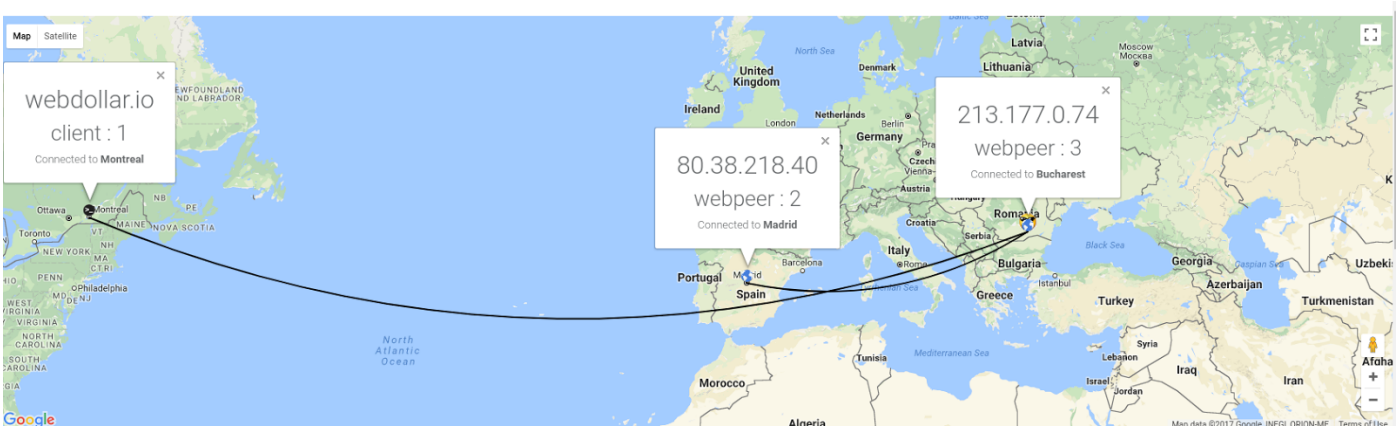


2.4.1 Facilitating for Symmetric NAT

WebRTC Protocol has to use STUN and TURN ICE servers to allow browsers to generate ICE candidates connecting the browsers each others, because otherwise it wouldn't be possible to identify themselves automatically.



Here is a list with some computers connected through socket.io (client:1), while the others (webpeer2 and webpeer3) are using WebRTC. Some computers couldn't connect because no TURN ICE server was provided.



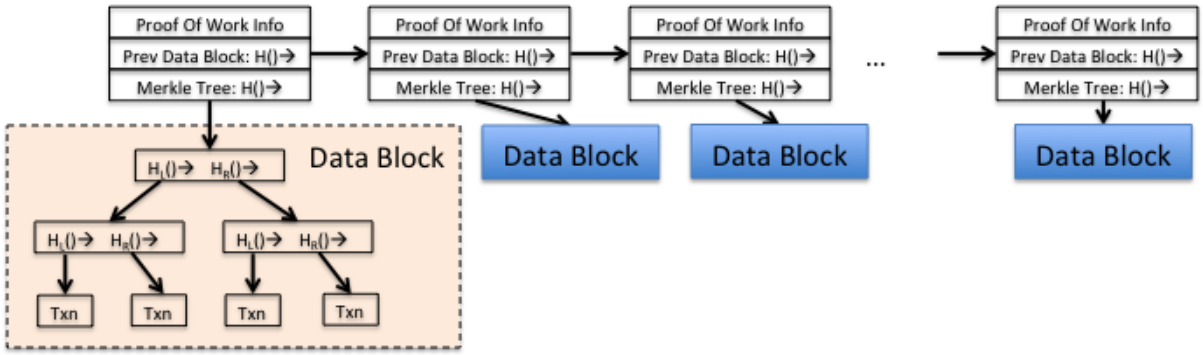
2.5 Javascript

The WebDollar was developed in Ecmascript 6. Using Babel and Browserify, we were able to transpile the library into a pure Javascript bundle that can be executed by every modern 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 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 and allowing SPV (Simple Payment Verification). The balance of an address is done by processing the Merkle Trees to find and validate previous transactions associated with that specific address. In this way, the balance of an address is calculated every time when requested 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 drive and then for each transaction it needs to track down all the previous transactions involving the requested address, and so on. This leads to having to access the same multiple blocks many times and check multiple Merkle Trees in order to calculate a simple balance.



The above diagram shows the proposed solution of Satoshi's Blockchain concept and a sample Merkle Tree that contains the hashes of a couple of transactions.

The challenge that comes with Blockchain is that over time, the size of the blockchain increases exponentially due to the fact that blockchains accept micropayments and each of these transactions requires Merkle Trees which are also large in data. . For example, after just 8 years, Bitcoin blockchain size is 140GB of data, while Ethereum is 80 GB of data and they are still growing.

Because we aim to run the Blockchain in the Browser, only Full Nodes (*but not Miners and Light Nodes*) will have to download the entire blockchain data, which will further promote WebDollar as a viable solution for mass adoption by the general public.

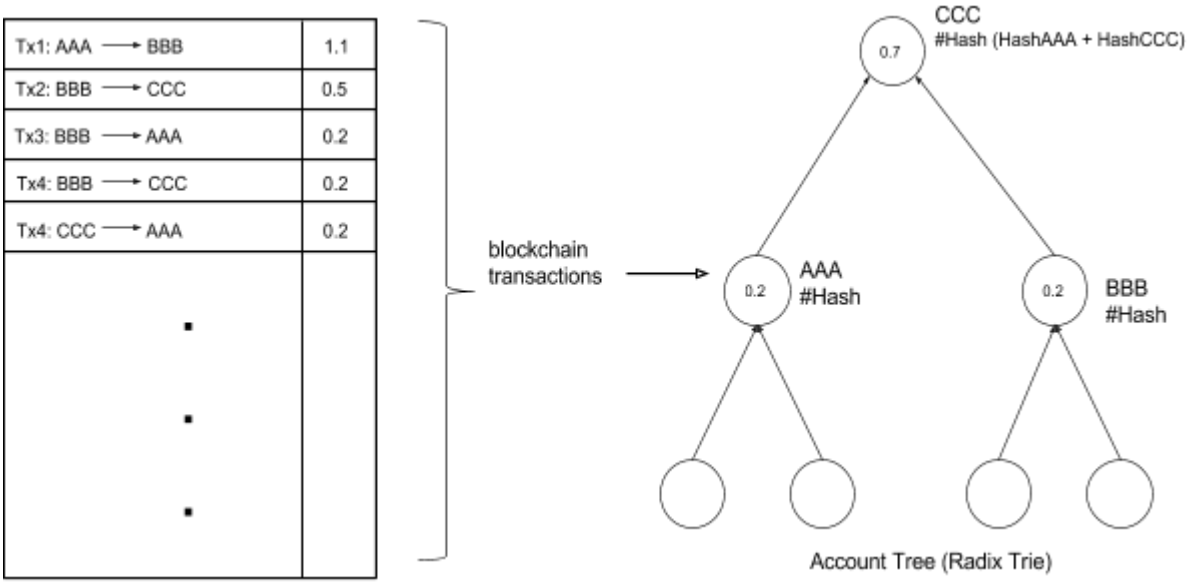
2.6.2 Mini blockchain Scheme

Mini blockchain Scheme [1] is a different implementation of a blockchain solution that "eliminates" the concept of unspent output transactions and introduces a new concept of **balance**. The mini blockchain scheme introduces a new data structure called an Accountant Tree in order to keep track of balances of all non-zero addresses.

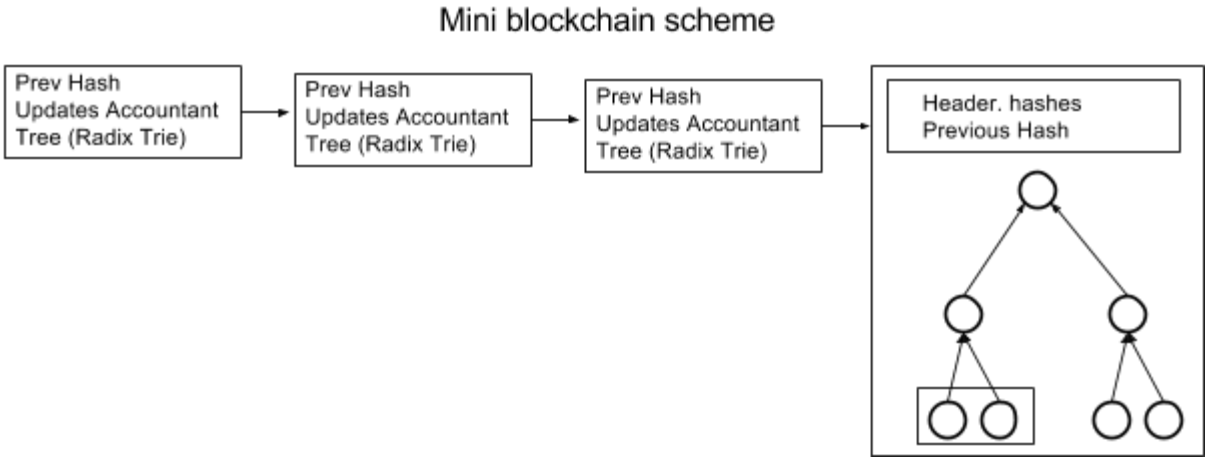
The accountant tree is just a **Radix (Patricia) Tree** of storing the balances for all non-zero addresses. So, instead of storing the transactions and a Merkle Tree of transactions, the mini blockchain scheme stores a Radix (Patricia) Tree for the balances of all non-zero addresses.

Radix (Patricia) Trees must be combined with a Merkle Tree to allow SPV (Simple Payment Verification) for ultra-light nodes, that will only download the NiPoPoW proofs and just a logarithmic number of hashes in order to validate a balance or to validate a smart contract.

Ethereum is the most known blockchain technology that uses Radix (Patricia) Merkle Trees.



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.



Pruning can also be done after a long period of time when the mini-blockchain ensures safety to prune very old blocks, but keeping a long not-pruned blockchain. By pruning the very old blocks, this will mean that some transactions can be discarded maximizing a little bit the anonymity of the addresses.

2.7 Non Interactive Proofs of Proof of Work

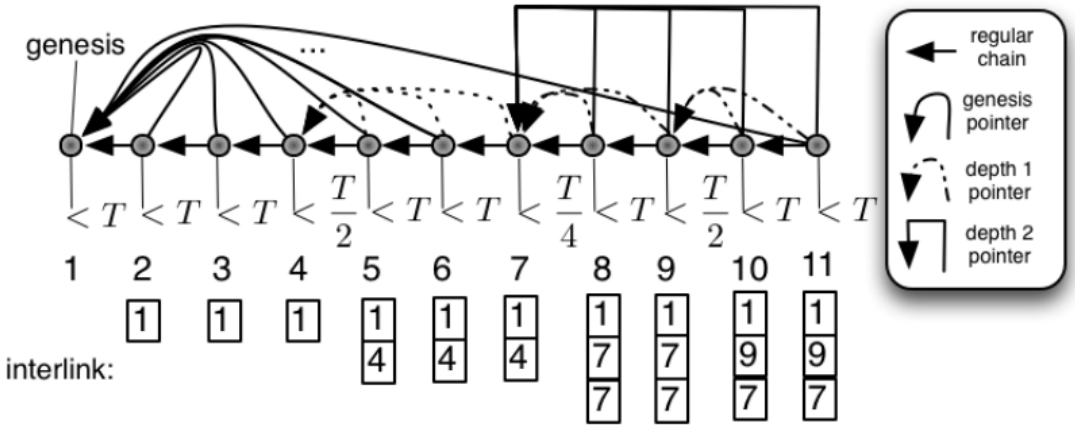
Non Interactive Proofs of Proof of Work is proposed by Aggelos Kiayias, Andrew Miller, and Dionysis Zindros [2].

WebDollar has two types of nodes:

1. Full Nodes (trustless nodes) - have a complete snapshot of the blockchain (or the last M blocks from the blockchain, where ΔT_M could be 1 year or 2 years), and they are used in the WebRTC signaling process to connect to browsers each others. The full nodes known also as **Provers** are able to generate NiPoPoW Proofs used by the light nodes.
2. Light Nodes (trustless nodes) - receive the NiPoPoW Proofs from multiple Provers and identify the honest nodes from attackers by verifying the proofs and determine the most difficult and valid proofs given from all nodes. Light Nodes are known also as **Verifiers**.

The first notion introduced in NiPoPoW by [2] is that they extends the Satoshi's [0] Blocks with a new data structure called **interlinks**, a vector containing pointers to multiple previous blocks, including the hash of the previous block. The interlink data structure contains pointers to more blocks than just the previous block [2]. So, every block instead of pointing only to the previous block, the NiPoPoW interlinks vector points to some previous blocks with the property that an algorithm presented in [2] can trace back to the Genesis Block. Given two hash functions H and G modelled as random oracles, the hash of a block is defined as $hash(Block) = H(nonce, G(Block_{data}, interlink))$. In WebDollar, H and G are to be proposed Argon2d as ASIC resistant and GPU not very friendly.

Valid blocks satisfy the proof-of-work condition: $hash(Block) \leq T$, where T is the global mining target from the main network. Some blocks will achieve a lower id. If $id \leq \frac{T}{2^{\mu}}$ we say that the block is of level μ. All blocks are level 0 (Genesis). Blocks with level μ are called μ-superblocks. μ-superblocks for $\mu > 0$ are also $(\mu - 1)$-superblocks. By convention, for Gen we set $hash = 0$ and $\mu = \infty$.



Graphical depiction of Interlink μ levels data structure stored in each block [13]

To describe the security properties of the blockchains that are equipped with the newly introduced interlink data structure, a few new concept of chain quality, inspired by the definition of this property called superchain quality were introduced.

(Locally good superchain). A superchain C' of level μ with underlying chain C is said to be μ-locally-good with respect to security parameter δ is defined as follows:

$$local-good_{\delta}\ (C',\ C,\ \mu),\ if\ |C'|\ >\ (1-\delta)\ 2^{-\mu}\ |C|\ ,\ \text{where}\ \ |C|\ =\ length\ of\ C$$

(Superchain super quality). The $(\delta,\ m)$ superquality property of a chain C pertaining to level μ with security parameters $\delta \in R$ and $m \in N$ states that for all $m' \geq m$, it holds the following property. That is, all sufficiently large suffixes are locally good.

$$local-good\delta\ (C\uparrow^{\mu}[-m'\ :\ ],\ C\uparrow^{\mu}[-m'\ :]\downarrow,\ \mu),\ \text{where,}$$

$C\uparrow^{\mu}$ is upchain defined as $\{B \in C \mid level(B) \geq \mu\}$

$C'\downarrow C$ is downchain defined as $C[\ C'[0]\ :\ C'[-1]\ ]$

(Multilevel quality). A μ-superchain C′ is said to have multilevel quality, written $multi-good_{\delta,k1}\ (C,\ C',\ \mu)$ with respect to an underlying chain $C\ =\ C'\downarrow$ with security parameters $k_1,\ \delta$ if for all $\mu' < \mu$ it holds that for any $C^* \subseteq C$, if $|C^*\uparrow^{\mu'}| \geq k_1$, then $|C^*\uparrow^{\mu}| \geq (1-\delta)\ 2^{\mu-\mu'}\ |C^*\uparrow^{\mu'}|$. In case it will not have the last property, then Multilevel quality will not exist.

(Good superchain). A μ-superchain C′ is said to be good, written $good_{\delta,k_1}\ (C,\ C',\ \mu)$, with respect to an underlying chain $C\ =\ C'\downarrow$ if it has both super quality and multilevel quality with parameters $(\delta,\ m)$.

NiPoPoW Verified algorithm for Light Nodes

Light Node = Verified ; Full Node = Prover

1. The Verifier starts to connect to the main network made of Provers and Attackers noted as P via Sockets and WebRTC
2. Thee Verifier starts to ask the Provers or other Light Nodes for the NiPoPoW proofs $(\pi,\ \chi)$, where π is the proof and χ last k blocks
3. The Verifier collects the NiPoPoW proofs $(\pi,\ \chi) \in P$ and starts validating the Proofs from the P set by checking $validChain(\pi\ \chi) \wedge |\chi|\ =\ k \wedge \pi \geq_m \widehat{\pi}$ and it will choose the

best (most difficult) proof $(\widehat{\pi}, \widehat{\chi})$ from the set $(\pi, \chi) \in P$ by using a defined operator $\geq_m$ that compares two different proofs π_A and π_B

4. After validation, in case there is a fork after last proven block $(\widehat{\pi}, \widehat{\chi})$, the Light Node needs to ask to receive the blocks after $\widehat{\chi}$ by validating these new blocks' interlinks. In case the fork is in the past and it is short, the Verifier can check the fork if it is right not, but in case the fork is longer than $\widehat{\chi}$, the Verifier will require another NiPoPoW proof for that fork.

$\pi_A \geq_m \pi_B$ operator compares two proofs and returns which underlying blockchain is longer from $ProverA$ or from $ProverB$

$$\pi_A \geq_m \pi_B = best-arg_m(\pi_A, LCA(\pi_A, \pi_B)) \geq best-arg_m(\pi_B, LCA(\pi_A, \pi_B)), \text{ where}$$

$$LCA(\pi_A, \pi_B) = (\pi_A \cap \pi_B)[-1]$$

$$best-arg_m(\pi, b) = max_{\mu \in M}\{2^{\mu} \cdot |\pi\uparrow^{\mu}\{b : \}|\}, \text{ where}$$

$$M = \{\mu : |\pi\uparrow^{\mu}\{b : \}| \geq m\} \cup \{0\}$$

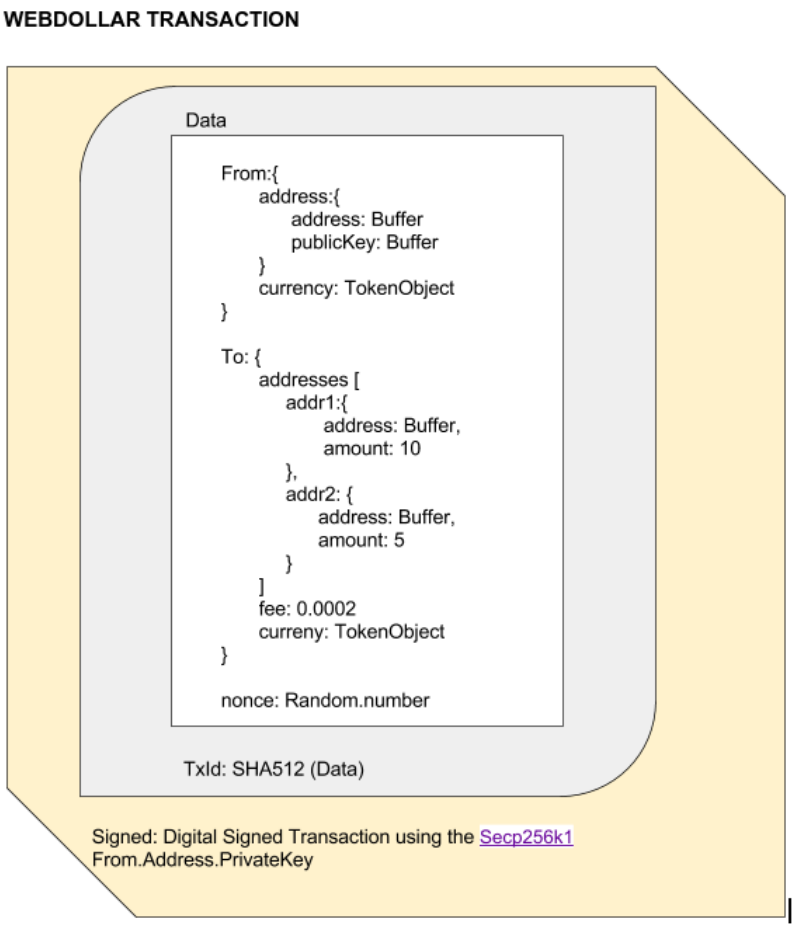
NiPoPoW Prover algorithm for Full Nodes

1. The Prover connects to a Light Node that may require a NiPoPoW proof (π, χ) and in case it already has the (π, χ) proof, it will just send it to the Light Node. In case it doesn't have (π, χ) already calculated, it will just generate the (π, χ) by the following steps.
2. It takes a μ-superchain and the last m blocks by filling a range of blocks with blocks from the superchain of level μ−1 below that respects the $good_{\delta,m}$ property, namely *Multilevel quality* and *Superchain super quality* All the μ-superblocks which are within this m blocks range will also be (μ − 1)-superblocks and so we do not want to keep them in the proof twice

2.6.3 WebDollar Transaction

The initial WebDollar transactions will enable to move funds from one address to an unlimited number of output addresses. The input of a WebDollar Transaction is just one address, while the output can be multiple output addresses. The transaction must be signed using an elliptic curve algorithm Elliptic Curve Digital Signature Algorithm (ECDSA). WebDollar test net used the secp256k1 elliptic curve used in the 2008 original Bitcoin implementation $y^2 = x^3 + 7$

Other remarkable ECDSA includes Schnorr signatures that agrees on a group G of prime order q, with generator of g, in which the discrete logarithm problem is assumed to be hard to crack on current computers (but not on quantum computers). A Schnorr signature is a hash function $H : \{0,1\}^* \rightarrow Z_q$



2.7 Proof-of-Work Mining ASIC resistant and GPU unfriendly

WebDollar is designed to be a Proof-of-Work blockchain like Bitcoin at least at the beginning. The only difference is that we propose the mining to be ASIC and GPU resistant, which will lead towards mass-adoption by users, not promote a hardware-intensive backbone. We want to avoid the clustering of large 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, creating a social layer on the mining process. We have analyzed a couple of ASIC resistant hash functions including Scrypt, Argon2 (Argon2d) and Cuckoo Cycle. At the moment, we propose an Argon2d function for Hashing, because in 2017, Argon2d is probably the best ASIC resistant hash function, but it is a little bit GPU friendly for the new video cards. The WebDollar community should also consider adopting other ASIC resistant hash functions in the near future for avoiding ASIC or dedicated mining computers (quantum, etc.) including CryptoNight that is only CPU friendly because of the high usage of the CPU 2mb cache. To avoid mining farms made by GPU, WebDollar community should adapt CryptoNight or other CPU cache intensive for the PoW Hash Function.

In PoW, each Block contains a Transactions Merkle Tree, respectively, an Account Tree/Radix (Patrcia) Tree for mini blockchain. The blocks are hashed through a Hashing function in order to validate it and the previous blocks, making the network 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 [3] 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 [3], 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 and to scale that memory on every device. By using Argon2d or in the future other memory intensive hash functions, WebDollar would be mined by the computers of individuals and not by mining farms. Satoshi had this idea of *"1 cpu 1 vote"*. ASICs and GPUs unbalance the mining, and this forces individuals to acquire

dedicated hardware for mining. This unbalance will push into a centralized mining by only controlled more and more by the people who has accept to acquire fast the best ASICs and best GPUs on the market.

2.8 Mining Difficulty

WebDollar is a blockchain Proof-of-Work decentralized solution and we propose this Mining Difficulty inspired from the Bitcoin. The difficulty of a block is noted as Λ , while timestamp of a block is noted as Γ

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 the following: if the ΔT to get 2016 new blocks was less than 2 weeks $\Rightarrow$ Difficulty will be increased, otherwise $\Rightarrow$ Difficulty will be reduced. The formula that recalculates the difficulty every 2016 blocks is based on algorithm that uses a modified Taylor series for the logarithm. **[4].** The disadvantage of Bitcoin's difficulty is that in case a large mining pool will just turn off their mining devices, the difficulty will be hard in the system for the next 2016 blocks (2 weeks), and the decentralized system will have a long pending list of transactions.

2.8.1 WebDollar Mining Difficulty

The first proposed WebDollar Proof of Work mining Difficulty is based on the Ethereum Homestead difficulty that adjust the next Target every block, (namely 15 seconds), but eliminating the "bomb" equation **[6]**

$$\Lambda_T = \Lambda_{T-1} + \frac{\Lambda_{T-1}}{2048} \cdot max(\ 1\ -\ \frac{\Gamma_T - \Gamma_{T-1}}{10}\ , 99)$$

where the division is integer division - the fractional part (remainder) is discarded, $\Delta T = 1$, Λ is adjusted every block, and $block_{time}$ is 15 seconds.

2.9 Transactions Per Second

Centralized Systems for the next years will still outnumber the decentralized systems. Ripple for instance, it is not a Blockchain technology and it is not decentralized. The bitcoin network's theoretical maximum capacity with the 1MB block size limit sits between 3.3 to 7 transactions per second (tps)[13].

Bitcoin: 10 min/block, 1 MB block size => 3.3 tps (low) or 7 tps (high)
WebDollar: 15sec/block, 1 MB block size => 132 tps (low) or 280 tps (high)

Future settings in the near future:

Block every 5 seconds, 1 MB block size => 396 tps (low) or 840 tps (high)
Block every 5 seconds, 8 MB block size => 3168 tps (low) or 6720 tps (high)

These are pure estimates based on the current Bitcoin scalability numbers.

By lowering the block time generator, it will create longer blockchain forks in the world. This can be achieved over the time, when the internet latency will lower.

By increasing the block size will make light nodes to download more data to validate the NiPoPoW (π, χ) proof. This can be achieved over the time, when the internet latency will lower.

Lightning Network and off-chain transactions are also taken in consideration to increase the number of transactions per second.

2.9 Fixed Supply

The medium-of-exchange function is the primary function of money. All others are secondary, such as store of value and unit of account. [10] For this primary function to be fulfilled, any quantity of money is sufficient. The pricing of money (establishment on the market of its purchasing power, or the formation of the prices for virtually all goods) is dependent on its supply and demand.

In the case of goods selected as means of exchange, the non-monetary use is less and less important than the monetary use. The monetary use involves transfers and preservation of substance, whereas in the case of non-monetary uses consumption involves substantive loss (from an economic point of view). Thus, the physical destruction of money through usage is insignificant when compared with other goods and, even in the case of commodity money, an increasing supply of it is not necessary. This is another reason why precious metals, whose supply is naturally difficult to boost, were considered suitable as money.

When discussing the monetary function, economists try to understand the laws that apply to monetary uses and ignore the non-monetary uses. Economists have argued since David Hume that any quantity of money is always optimal. Increasing the quantity of money does not increase the services rendered by money. This observation was only qualified by the fact that the non-monetary uses of money justified an increasing supply of it.

Cryptocurrencies are closer to being purely money in this sense, because their intangibility makes them less suited for non-monetary uses. The age-old observation about the optimality of any quantity of money is fulfilled even better in their case.

The WebDollar follows Bitcoin in adopting this model of a fixed supply with gradual release. Cryptocurrencies are rather like commodity money to the extent that their supply is

not discretionary. In the case of precious metals, production has to compete with all other uses that its valuable factors of production can service. It is in this way impersonal.

In the case of cryptomoney, this impersonal character is maximized with a fixed supply. Any inflationary model is a suboptimal solution, a compromise from scientific rigor, because it includes a particular judgement about how the new coins should dilute the value of old coins. A cryptocurrency that allows for any degree of discretion in the future is further compromised from the start. Having a fixed supply and a continually changing demand established by the market solves a problem of uncertainty and makes the price adjustment model simpler.

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 Ω adjustment can be approximately modelled by the following equation: [5]

$$\sum_{height=0}^{inf} \Omega\left(Block_{height}\right) = \frac{\sum_{i=0}^{2^5} 21 \cdot \frac{50.10^8}{2^i}}{10^4}$$

The decreasing-generation 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.

2.9.1 Deflation and hoarding: is there a reason to worry?

People erroneously refer to the model above as a deflationary model. Here, we need to clarify that there are two uses of the words deflation or inflation:

- inflation or deflation of money supply, or
- inflation or deflation of prices

The classical and relevant use in our case is the first. So, technically speaking, the WebDollar money supply is *fixed*. If less people would demand it then its purchasing power would be lower (prices expressed in WEBD would increase), so it becomes price inflationary – although early massive adoption would have price deflationary effects.

Markets can deal both with a general high level in prices and with a general low one. Price deflation does not lead to depression. [12] Hoarding is just an emotionally charged name for demand for money and there is no problem with it from an economic point of view. Intensive demand for money during the first phases of a worldwide adoption process is to be expected and welcomed, not countered.

One particularity of any cryptocurrency is that it is indefinitely divisible, because it is intangible. Gold could be minted in small coins only to a point beyond which it became impractical to use. The reason silver was adopted at times instead of or along gold to fulfill

the money role was its increased abundance and capability to serve in small everyday payments, despite its other disadvantages to gold (e.g., tarnishing). Such coexistence of moneys is impractical because it introduces the need to keep account of the exchange rate between to two metallic moneys. One major blight of monetary history was the inability or malevolence of authorities that enacted a fixed exchange rate between the two, also known as bimetallism. This fixed bimetallism often engendered Gresham effects – overvalued money replacing undervalued money on the market – to the great losses of market actors.

This flexible exchange rate between two moneys is not to be confused with the definitions of subdivisions in the case of one money that are always fixed, as with the relation between one ounce of gold and half an ounce, or 100 grams and 1 gram. Likewise, banknotes and deposits emerged as substitutes for metallic money, to solve payment, security, divisibility and portability problems. In the case of honest issuers, the issue was perfectly covered in money reserves and, again, there was a fixed definition of the substitute in terms of metallic reserves, not a variable price.

The arrival of the blockchain solves portability, security, and payment, to different degrees with different cryptocurrencies. Moreover – and the importance of this fact cannot be overemphasized – cryptocurrencies do not have the divisibility problem. As we can see in the case of Bitcoin, technically it is possible to divide one bitcoin into 100 million satoshis, with intermediary bitcents, milibits and microbits.

While not technical, the divisibility problem is rather psychological. In expectation of a very steep worldwide adoption curve, on a scale several orders higher than Bitcoin, we decided to assign to our one-time creation of the fixed WebDollar supply a corresponding granularity.

A technical problem that Bitcoin has not solved satisfactorily and WebDollar is designed to solve is the *portability* problem. The relatively low number of transactions is not caused by hoarding, but by the technical specifications of Bitcoin. We consider that this is the reason why we see such low transaction numbers and high fees for cryptocurrencies from the Bitcoin family.

2.10 Security concerns

WebDollar implementation is using the mini-blockchain scheme for storing the Accountant Tree instead of using Transactions Merkle Trees. The security concerns for using the mini-blockchain are very similar to Satoshi's Proof-of-Work Blockchain solution, and it has been proven to be safe in Ethereum.

WebDollar Full nodes are inheriting all the security advantages and properties from the blockchain PoW solution proposed by Satoshi Nakamoto in [0].

WebDollar Light nodes that download only the Non-Interactive proofs will inherit all the properties and security concerns from the NiPoPoW - Non Interactive Proofs of Proof of Work. [2] By having also a main net of Full Nodes (it is required to have node.js servers for

WebRTC signals), the attacker will also need to attack the honest Full Nodes from the main network or at least to either to generate better NiPoPoW proofs or suspend (stop) the connections with honest full nodes..

2.10.1 Security in Blockchain

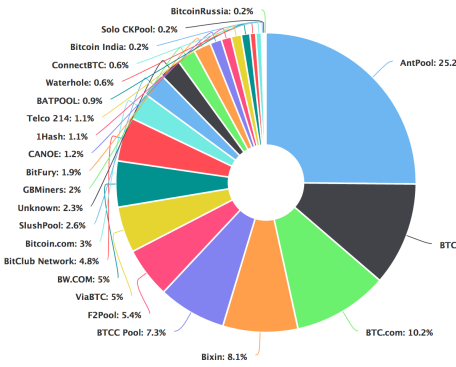
2.10.1.1 Change History Attack

To hack the blockchain, the attacker needs to build a longer valid blockchain. To build a longer valid blockchain, the attacker will need a considerable % of the main network hashrate. Because of this, in case the attacker will fail to have >= 50% of global hashrate, the attacker is in a competition with other honest miners and it will be more profitable for him to become a WebDollar miner instead of remaking the blockchain from scratch or even forking the blockchain to keep the rewards for himself. So, to change an old history is almost impossible for an attacker because it requires to own more than 50% of global hash rate and sustain in it in secret for a considerable time to make a successful fork that changes significant history. By this way, an attacker could maximum create a fork altering only recent events and keep the recent rewards from miners for himself.

In case the attacker hasn't a next generation technological advantage (quantum computer), the attacker must have the network domination over a similar ~timespan as since the genesis block began.

2.10.1.2 Double Spending Attack

Attackers that dominates a large percentage of the Main Network, can try to create some double spending attacks in the Blockchain Technology by creating and mining their own forks. Thankfully, Blockchain handles very well the double spending attacks making the attacks probabilistic and not guaranteed. Actually, Satoshi Nakamoto did even some computer simulations in 2008 [0] to calculate the probabilities of some double spend attacks with different percentages of the network dominance. In, reality the probabilities of success for an attacker are very small and, it would be way more profitable for him to mine the coin and not to try uncertain attacks that may lose money. Nowadays, Bitcoin is more vulnerable to Double Spending than never, especially because, the mining pools started to become more centralized. The top 4 mining pools (see diagram) are all from China, and they own over > 50% of the entire Bitcoin Global Hashrate. This means, a collaborative attack from these four chinese Mining Pools could have a significant probability to launch a successful Double Spending Attack, but not guaranteed.



WebDollar allows a user with just a click to create his own mining pool and can share a referral link to other people who would like to mine in his mining pool. By this way, WebDollar will decentralize the mining pools, reducing considerably the risks for Double Spending Attacks.

2.10.1.2.1 Double Spending Attack Solution #2

TBA

2.10.2 Quantum Threat

Absolutely, but absolutely all cryptographic functions used in Banks, Stock Exchange, Internet Security communications and Bitcoin are threatened in **20 - 30 years** by Quantum supercomputers. Although, Quantum supercomputers are not a today's' reality. D-Wave quantum computer is an Adiabatic Annealing Machine that can solve probabilistic only Adiabatic Equations are D-Wave is **NOT a General Quantum Computer**. So, Adiabatic Annealing Machines like D-Wave can not be used to generate 2^{256} or even 2^{128} to crack either the private keys or respectively the digital signatures by cracking the the elliptic curves (ECDSA, Schnorr) used in Bitcoin or in WebDollar. The only solution, in that very unlucky scenario in the next 20 years is to make the system more quantum resistance is that instead of working with 32 bytes private & public keys, 20 bytes for public addresses, the protocol should work with way longer private keys and addresses. But this is not ideally because of high memory usage in blocks, moreover also at the moment there is no real threat from adiabatic quantum computers, but also for the next years

2.10.2.1 Reducing Addresses' private key collisions from 2^96 down to 0

The biggest issue in Bitcoin is that although the total numbers of private keys and public keys are 2^{256}, the total number of unique addresses in the Bitcoin system is 2^{160}. This exploit appears because in Bitcoin, early Bitcoin programmer Hal Finney (Satoshi) used the $RIPEMD(SHA256(publicKey))$ function reducing the length of the addresses by converting the public address keys from 256 bits into 160 bits addresses. RIPEMD hash function initial purpose was to be used as a backup in case the SHA256 could have been cracked. The

problem is that RIPEMD160 is generating Bitcoin addresses making a lot of collisions, that all addresses have multiple private keys attached.

The birthday problem can be applied to estimate the probability of addresses collisions given the size of the hash function. [7] The Probability Calculations in Hashing [8] can be used tp to estimate the private key collisions in public addresses as follows:

To get all $k = 2^{160}$ addresses, it is enough to use:

$$k * ln(k) + k = 160 * 2^{160} + 2^{160} = 161 * 2^{160} = 2^{167.32} \text{ keys.}$$

If you use only 2^{160} private keys, you will have about 63% of all addresses [7]

Although 2^{160} seams a big number, by using the RIPEMD160, the system could be attacked by an early and primitive Quantum computer that can generate 2^{167} quickly and could crack all Bitcoin addresses. By extending the domain of the addresses from 2^{160} to 2^{256}, this will give WebDollar an extra buffer time, in case in the near future (10, 20 years), a real quantum computer will be invented and able to generate cracking the RIPEMD 2^{160} function, but it won't be able to generate 2^{256} so quickly as cracking 2^{160}.

2.10.2.2 Increasing Quantum Resistance

By replacing the RIPEMD160 with SHA256, the security exploit for a future Quantum computer still remains in. In order to solve this, we propose that WebDollar over the time should use more Quantum resistant cryptographic functions. The advantage is that , the community can create a hard fork replacing the obsolete ECDSA to use a Post Quantum Cryptographic (PQC) functions or to use functions like Winternitz signatures (~1.4kb) instead of using 256 bit Elliptic Curve Cryptography. At the moment, it is not very useful to switch to Post Quantum Cryptographic functions, because all PQC functions use way much memory to store the signatures than by using regular 256 bit Elliptic Curves.

3. The advantages of WebDollar

A. **Simplicity**

Our goal is to create and foster the mainstream adoption of cryptocurrencies. In order to make that vision a reality, we need to address all kinds of users, not just the tech savvy, like all the other cryptos do. For that, we aim to create the simplest possible user experience with regard to using cryptocurrencies. And in our quest to achieve that, we've come to the basic premise that while very few people know how to mine Bitcoin or install a software wallet, just about everybody knows how to use a browser.

This is why WebDollar was designed from day one to be native to browsers and to the World Wide Web. Written entirely in Javascript, WebDollar will be available directly in your browser. That means:

- **No Installation**
- **No Download**
- **Mining directly in the landing page.** Unlike any other crypto, you will be able to mine and create value for yourself in less than 5 seconds, just with a simple click on a button. Not only it is simple, but it is also fair. Our hash function of choice, Argon2d at the moment does not create a preference for specialized hardware and you can run it efficiently on any PC. Also, you can run as many threads as your hardware allows, having full control on the impact on your processing power.
- **Access your wallet fast and safe in the browser.** Without going through the hassle of installing dedicated, complicated software and generating private keys that you have to save somewhere else, you can generate a new wallet with a single click and easily access from there, all the needed functionalities, while not compromising security:
  - Send or receive payments
  - See your transactions
  - Check your balance

B. **Versatility of mining hardware**

In order to make it easy for everybody to use it, anytime and anywhere, we rely on a light blockchain structure, involving the usage of mini-blockchain scheme and Non Interactive Proofs of Proof of Work (NiPoPoW) consensus building. That greatly reduces the size of the data that has to be downloaded into the browser in order to be able to become consensus and start having a mining pool in the browser. In turn, this created the opportunity to mine on any PC or laptop, regardless of disk space, and even to mine on mobile devices, tablets and smartphones.

C. **Rethink mining from the bottom**.

Mining is a slang term for the verification of transactions. We have been using the term "mining" for so long, that sometimes we forget it is a social act – one that creates trust in the network without the need of a centralized authority.

The way the traditional POW cryptos were mined and the GPU/ASIC-intensive hash functions were used, over time, tended to stimulate the centralization of the network around large mining centers, where processing power and hardware have the ultimate say. This has created an undesireable situation in which the network is dependent on the political climate in certain countries. For example, for Bitcoin, 80% of the processing power of the network is based in China, and over 50% of the network control lies in the hands of the 4 mining farms.

This goes against the vision that Satoshi Nakamoto himself had for the Bitcoin – to be a decentralized coin. WebDollar wishes to return to that vision, by rethinking mining, from a hardware intensive activity, to a social activity. We do that by using a hash function that does not create a preference for specialized hardware (is ASIC-resistant) and by creating a referral system.

Everybody can easily become a pool, by loading the entire blockchain onto his PC. Then, he can invite friends to create wealth together, by mining in his pool. Through this social network approach, both the "regular miners" and the pool owner gain value – for each reward obtained by people mining in one's pool, the pool owner gains a small percentage. This encourages a strong stimulus to create, expand and maintain mining pools, thus decentralizing the network. It will also help create the initial awareness for WebDollar, by capitalizing on the early adopters' social networks.

4. **Create real value for content creators and monetize your social network**, by embedding a script in your webpage that harnesses the visitors' processing power to create value for you, in a consensual, transparent way. No more need to insert ads into your website or beg for support on donation sites. You can directly capitalize your traffic by easily inserting a script that creates value for you based on the frequency and duration of visits on your site, with users permission.

5. **Smart contracts.** The primary purpose of WebDollar is to act as currency on the World Wide Web, to truly become the currency of the internet. To expand on this view, WebDollar aims to support smart contracts, which will allow decentralized organizations to create their own tokens, taking full advantage of the technological upper hand of our protocol.

6. **Anonymity.** By using an optional, off chain solution, we will be able to provide to our users the benefits of full anonymity, far superior to the level of anonymity offered by Bitcoin or Ethereum.

7. **The speed of transaction confirmation.** In order to be a scalable digital currency, any crypto has to have a fast transaction confirmation time. To meet that objective, our protocol matches some of the fastest transaction confirmation speeds, generating a new block every **15 seconds.**

8. Logarithmic fees policy. WebDollar aims to become a widespread and very easy method of transferring value on the internet. In order to stimulate the flow of WebDollars, we devised a logarithmic function for calculating the fees. Starting from a very small value (we have implemented a Large numbers function, allowing for up to 18 decimals), the value of the fee, expressed as a percentage of the transaction value, becomes smaller and smaller as the value transaction gets larger. The fees for monetary transactions will be considerably less than current digital services, like Visa, PayPal or Western Union.

9. Integrated end-user app for money transfer. By using our peer to peer exchange facility, you will be able to send money directly from your account to someone on the other side of the globe, in their own account or crypto wallet, via an automatic off-chain exchange service using WebDollars.

10. **Controlled monetary emission might provide the silverlining between uncontrolled deflation (hoarding) and uncontrolled inflation (depreciation).**
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. With 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 excited about cryptocurrencies.
WebDollar aims to offer a mid-way solution that will start with a hard cap, allowing for an exponential increase in value, reaping many benefits for early adopters. Gradually, as the market capital increased, the rate of growth will be tempered via monetary emission, leading in the end to a stable, liquid real digital currency, not another investment asset that leads to hoarding.

11. Creating an inclusive, healthy and diverse ecosystem. Through the developments envisioned for the ICO, we aim to further expand the crypto-community by hardening the real economy behind the WebDollar value - integration for payments in real online services and creating a marketplace are two of the top actions to be undertaken in this direction.

WebDollar will build on Satoshi's original intention to create a truly decentralized coin, by rethinking mining from a hardware intensive activity to a social one. With WebDollar, your time IS money.

Contributors:

1. Special thanks to **Adrian Mihai Stratulat** for helping in writing this White Paper
2. Special thanks to **Prof. Tudor Smirna** for including chapters about History, Money, Deflationary systems.
3. Patrick McCullough for reviewing the White Paper

References:

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

[1] J.D. Bruce – The Mini-Blockchain Scheme

[2] Aggelos Kiayias, Andrew Miller, and Dionysis Zindros, Non-Interactive Proofs of Proof-of-Work https://eprint.iacr.org/2017/963.pdf

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

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

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

[6] Ethereum Improvement Proposal 2 "Homestead Hard-fork Changes", https://github.com/ethereum/EIPs/blob/master/EIPS/eip-2.md

[7] BitcoinTalk https://bitcointalk.org/index.php?topic=1895455.0

[8] Rosa Orellana, Dartmouth College, Probability Calculations in Hashing https://math.dartmouth.edu/archive/m19w03/public_html/Section6-5.pdf

[9] Carl Menger, The Origin of Money, Committee for Monetary Research and Education, Greenwich, Conn., 1984.

[10] Ludwig von Mises, Theory of Money and Credit, Liberty Fund, Indianapolis, 1981, pp. 46-49.

[12] Andrew Atkeson, Patrick J. Kehoe, Deflation and Depression: Is There an Empirical Link?, Federal Reserve Bank of Minneapolis, Research Department St aff Re p or t 331, January 2004.

[13] Aggelos Kiayias, Nikolaos Lamprou, and Aikaterini-Panagiota Stouka, Proofs of Proofs of Work with Sublinear Complexity,

[14] Bitcoin Scalability Problem https://en.wikipedia.org/wiki/Bitcoin_scalability_problem