WebDollar

FIRST BLOCKCHAIN DIRECTLY IN WEB

disrupting Bitcoin with simplicity

Or how to make your grandma use crypto

WHITE PAPER

Executive summary

At the moment of writing of this White Paper, Bitcoin, world's most famous and valuable cryptocurrency, is peaking at the historical value of 6000 USD per Bitcoin. And 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 represents only 0.11% of the total amount of money in the world. If we add all the other cryptocurrencies to the mix, we don't even get to 0.2% of the total financial value in the world. This is partly due to the fact that cryptocurrencies are still a fringe and technical topic, requiring specialized knowledge from their users. This excludes the older generations, the less IT literate people etc. WebDollar aims to tackle this issue by creating world's first browser only cryptocurrency, where mining, wallets, transaction systems and other features are all browser based, providing a level of simplicity never before met.

1. **A brief history of cryptocurrencies**
2. **Shortcomings of current cryptocurrencies**

Bitcoin - great it works well

- Cryptographic Software (DESKTOP) -
    - Blockchain
        - Nodes
            - Nodes (uses sockets)
                - Propagate transactions and blocks data
            - Miners (uses sockets)
                - Processing Hash Functions to distribute the data *
        - Wallet
            - Show your Balance *
        - Pools
            - Terminal Application
            - Web Interface
    - Terminal (written in C)
        - Linux ./
        - Windows .exe
        - Mac

Bitcoin protocol is a DESKTOP software (except the Pool Web Interface)

* Every Miner/Node has to download all the blockchain data (bitcoin has 200 GB at the moment)

Problems:

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.

3. A simpler approach - the advantages of web-based cryptocurrencies

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

- Cryptographic Software (WEB)
    - Blockchain
        - Nodes (NPM modules and .js scripts)
            - Nodes (websockets - browsers)
                - Propagate transactions
            - HASH Miners (websockets - browsers)
                - Processing Hash Functions to distribute the data *
                - Accept Puzzles from POOL Nodes
            - POOL Nodes (websockets - browser)
                - Propagate database about the previous transactions. It can be done in browser although it may take 200GB using the solution from WebTorrent!
                - Distribute Puzzles to the HASH MINERS
                - POOL Nodes are picked randomly by the Blockchain miners or via a drop down list
                - **Service** Wallet Information

- Show your Balance. Randomly picked they communicate with a random Node “Database”

- Website
  - Frontend that enables:
    - Hash Mining
    - Pool Mining
    - Running Node

WebCoin 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

GasMiner 0.0 WBC
GasMinerDB 0.0 WBC

Additional Information{
    emailAddress: alexandru@budisteanu.net
    handleName: unique_username_cool
}

REWARDS

1. Miner is rewarded with 25 WEB

Implementation:

Node.js
SHA256

Advantages:

- **WEB**

- Everything is in Javascript executed in the browser
- You can Mine online (earn free miners). Online with your browsers.
- Harder for ASIC because it needs HTTP requests :) - so no GPU compatibility.
- **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 countries
- SHA2 (2x bigger secured than Bitcoin SHA1) for Addresses
-

Why WEB is the biggest ADVANTAGE?

Simply: 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 offline application. Facebook Messenger is online, easy to use, anywhere, any device, compatible, WEB

Online Wallet (no software downloaded)

Online Miner (in 30 seconds, you can start mining :))

EASY TO BUILD CARTS because you receive HTTP ANSWERS

Security:

For hacking it, you need to build an entire and longer fake blockchain. It means you need to remake it from scratch

WHY ANOTHER COIN?

1. Bitcoin is an internet application. **Without, internet Bitcoin can not be used.** But **Bitcoin is not a Web Application (HTTP)** and this is the **reason why it can not reach more than a few million users.**

2. If Bitcoin would be used by 1 billion people, 1 BTC = $500K - $5 million . Why? Because there will be only 21 million bitcoins, for 1 billion people. But, I don't believe Bitcoin (terminal based app) will be used by 1 billion people.

3. Currencies or at least Digital Currencies and quite similar to **pyramidal schemes**. But there are **two major differences:**
    a. It adds real value to a lot of users
        i. Speculation - you can speculate the price
        ii. Pay products anonymously
        iii. Pay products with lower fees (BITCOIN not applicable anymore)
    b. The only way to loose money is only through Bear Market (Bubble pop) or through inflation (not the case)

Why pyramidal? You get Cryptocurrencies now with a small Market Cap at a lower price, if you make more people to use it or buy it (the Market Cap goes UP), the price goes UP. Buy cheap, hold it, sell when more people will use it (bigger market Cap, bigger price)

So theoretically the bubble will pop in 2 scenarios
1. Nobody will no longer use it or buy it. If less and less people will use it or buy it, then the price will go down (smaller Market Cap).
2. Everybody will have it, nobody new buys it (but that means a Market Cap of Trillions of Dollars). This means it is widely used by everybody and it is a global success.

4. We can be the next Bitcoin and the first people to use it!

5. Satoshi **===** Hal Finney. Explanation why Satoshi is out of the picture because Hal Finney died in 2014 of major health problems and cryogenized. A personal name that has the name of "Satoshi" is a neighbor worker of Hal Finney.

6. BITCOIN original code was written in C++ by Hal Finney in just 6 months. https://github.com/trottier/original-bitcoin/tree/master/src

7. There are 1000 coins. All of them are just copy-cats of the original Bitcoin. All of them have value. Even if WebCoin will not dominate Bitcoin, it will still have a value of hundreds millions of dollars.

8. Ethereum Creator (Vitalik Buterin) own wallet worth 400 million USD

TUTORIALS

1. https://marmelab.com/blog/2016/04/28/blockchain-for-web-developers-the-theory.html - watch also the video
2. https://www.youtube.com/watch?v=93E_GzvpMA0

4. **Webdollar ICO**
5. **Conclusion**

STEPS TO ACHIEVE WEBCOIN

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. **Websocks 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. Websocks to communicate with Miners
            2. Generate Merkle Tree
                a. Retrive 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

ASIC resistant algorithm (scrypt). Other ASIC reistant algorithms
http://altcoins.com/cpu-altcoins

https://github.com/zcoinofficial/zcoin/wiki/Proof-of-Work-Algorithm
https://github.com/zcoinofficial/zcoin/wiki/What-is-MTP-(Merkle-Tree-Proof)-and-why-is-it-an-ideal-Proof-of-Work-algorithm%3F
https://www.usenix.org/system/files/conference/usenixsecurity16/sec16_paper_biryukov.pdf
https://zcoin.io/what-is-mtp-merkle-tree-proof-and-why-it-is-important-to-zcoin/

MTP
https://www.quora.com/Cryptography-How-does-a-Merkle-proof-actually-work

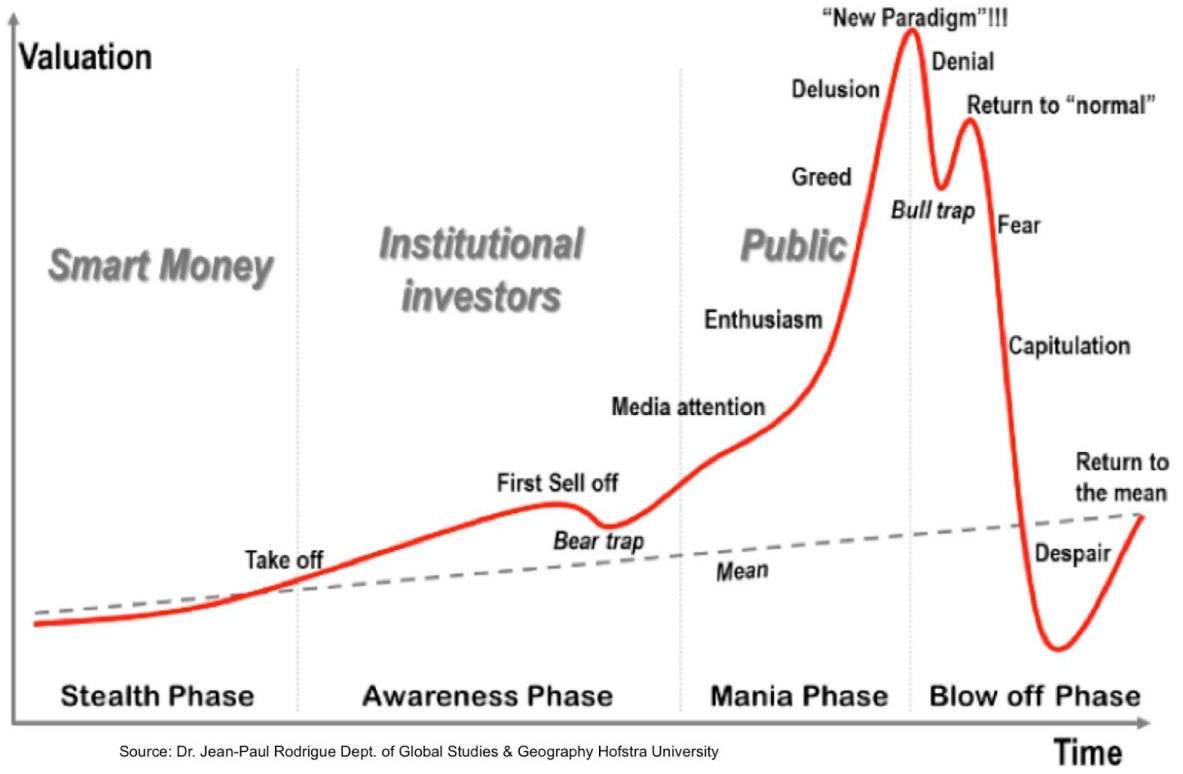
Argon 2 - very good solution it has demo
https://www.cryptolux.org/images/c/c5/Rwc-slides.pdf
https://github.com/antelle/argon2-browser
https://antelle.github.io/argon2-browser/

Obs:

1. onSuccess, onFailure Events will be called many times!!! (by every DB miner who got this new block will call it one time). We have to think about it.
    a. The events can be triggered by a separate Website/Service that process the blocks and generate onEvents, onSuccess
2. Bitcoin Difficulty is adjusted every ~ 2 weeks, after 2016 blocks. If the time to get 2016 new blocks was less than 2 weeks => higher Difficulty, otherwise reducing Dificulty **https://en.bitcoin.it/wiki/Difficulty**
3. For Balance use geolocation (group MinersDB into 6 lists based on their continent) + websocket subscribe to select 5 random MinersDB from the 6 lists to check a transaction ID. After that you can also build a separate website service that can process the blocks and generate onEvents, onSuccess.

    The continents lists should only contain nodes that sent valid blocks in the past!!!!

Bubble Phases (I have learned at Singularity University)



Source: Dr. Jean-Paul Rodrigue Dept. of Global Studies & Geography Hofstra University