WEBCHAIN:

A Blockchain for DApps, Secured via Websites

Abstract:

In Internet of Things era, why limit mining only to PCs with installed specialized software? Every device with spare resources (including PCs, smartphones and IoT devices), as long as the owner agrees, should be able to participate in securing the network. *Webchain* is a transparent web-mineable blockchain platform made to support *Decentralized Applications (DApps),* where websites can serve as a hardware-independent alternative to secure ERC20 & ERC223 smart contracts. We are presenting a working, fully functional, smart contracts enabled blockchain platform. On top of that, we feel committed to building tools that help attracting new projects into the cryptocurrency ecosystem. Webchain is a platform for projects that base their business model on mining via websites, for those that want to remain ASIC-resistant (and support egalitarian coin distribution), or anyone that wants to spread new revolutionary ways of website monetization. Webchain, and projects built upon it, will be the first real alternatives to Google Adsense monopoly and will introduce a completely new way for webmasters to generate revenues.

Blockchain Backgrounds:

Nine years ago, a technological and economic revolution began, triggered by a simple, yet transcendent idea: “an electronic payment system based on cryptographic proof instead of trust, allowing any two willing parties to transact directly with each other without the need of a trusted third party.” (Nakamoto, 2009).

Bitcoin introduced a revolutionary way to understand economics: transactions no longer based on third-party interventions or central overseers. Banks and any other financial institutions replaced by an ongoing ledger chain created from a hash-based proof-of-work (PoW), registering any transaction on an encrypted p2p network. Not too long after the success of this idea, Ethereum emerged; a new blockchain solution, built to extend *Bitcoin* reaches so that a distributed network of miners could process complex sets of smart contracts. When Bitcoin’s *sha-256* got dedicated *ASIC*, mining became unprofitable for many users due to the rapid increase of block difficulty.

None of the changes conceived as part of Ethereum solved or are going to solve this problem - they are currently vulnerable to ASIC mining (or even attacks) and later, they plan to move to Proof of Stake, which won´t ensure that Ethereum network remains egalitarian. In Proof of Stake, there’s no equal distribution since owners of many coins get rewarded the most, while those with few coins - the least. It starts to resemble the old banking model current world is built on.

Privacy-oriented blockchains can be an attractive environment for lawbreakers, that’s why holding transparent and public transactions is convenient for website-minable currencies - even when most privacy coin users are legit. Webchain team thinks that bitcoin's pseudo-anonymity was the solution from the beginning. Unnamed wallets help to prevent data theft and snooping, as it occurred in 2018 with Facebook-Cambridge Analytica scandal. At the same time transactions shouldn’t be obfuscated because transparency is very important in today’s world.

How would you like it if politicians received Monero-based donations from unknown donors? We support privacy, but not at the cost of the transaction transparency. Both things are important and both can be achieved. Not to mention, that there is a real risk in banning privacy coins by regulators —there are exchanges that already removed Monero and other privacy-based coins because of this[1]. All this could influence privacy coins price in future.

After the first blockchain projects were created, criticism and production of new ones proved that they were just part of a new technological revolution. A massive social recognition, mass-media coverage and a rollercoaster of opinions, caused cryptocurrencies and their creators (under real names or pseudonyms) to become popular, along with the idea of handling transactions through decentralized, trustless networks. Nowadays, there are many alternative blockchain networks and they are more than ledgers for financial transactions.

The current panorama:

The possibility of mining cryptocurrencies via websites emerged along with the creation of CryptoNight, algorithm designed to make CPU and GPU mining similarly efficient while completely restricting ASICs (CryptoNote Technology, 2018).

To make this possible, Webchain allows the use of javascript-based browser miners which websites can host to generate hashes on a visitor's machine. Even when there are several blockchains where these scripts can be used, none of them are platforms that allow users to create their own decentralized applications (DApps).

The current Dapp market is still young, with a huge potential to grow and disrupt the aging centralized Internet ecosystem that created giants like Google and Amazon and gave them huge control over the worldwide web. Through Dapps implementing the ERC20 and ERC223 standards, Webchain is proposing a simple way to help transition the web from the current monopoly-like ecosystem to a decentralized future.

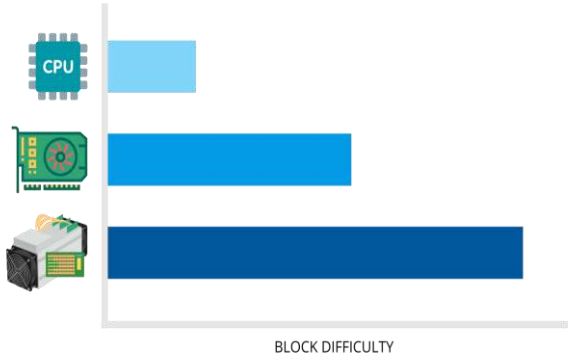
Even with the efforts invested to avoid it, CryptoNight and other blockchain projects like *Ethereum* and Monero got machines with Application-specific Integrated Circuit (*ASIC*) chips[2], which concentrate a greater processing power and profitability level than any unspecialized hardware, therefore allowing a monopoly in the blockchain production.

---

[1] Crypto Currency News. 2018. *Coincheck | The Japanese Exchange Drops Monero, Dash, & Zcash*. [ONLINE] Available at: https://cryptocurrencynews.com/daily-news/exchanges/coincheck-drops/. [Accessed 28 April 2018]. CCN. 2018. *Japan Wants Cryptocurrency Exchanges to De-List Anonymous Altcoins: Report*. [ONLINE] Available at: https://www.ccn.com/japan-is-pressuring-cryptocurrency-exchanges-to-de-list-anonymous-altcoins-report/. [Accessed 06 May 2018].

[2] CoinDesk. 2018. *Bitmain Confirms Release of First Ethereum ASIC Miners - CoinDesk*. [ONLINE] Available at: https://www.coindesk.com/bitmain-confirms-release-first-ever-ethereum-asic-miners/. [Accessed 10 April 2018]. Cointelegraph. 2018. *Bitmain Announces New Monero-Mining Antminer X3, Crypto'□□s Devs Say Will □□Not Work□□*. [ONLINE] Available at: https://cointelegraph.com/news/bitmain-announces-new-monero-mining-antminer-x3-cryptos-devs-say-will-not-work. [Accessed 10 April 2018].

Ethereum developers recently faced a dilemma regarding the modification of its protocol in order to restrict ASICs. Buterin (Ethereum foundation's main face) is against this change[3], claiming that security of transactions is not at risk and that Casper[4] will overcome any current ASICs via PoS; meanwhile, ETH users will have to accept the presence of ASICs mining in the network, unless they accept another fork. Although other developers in the Ethereum team seem to consider this possibility in a more serious way[5], there's no consensus or defined institutional statements regarding ASICs as a danger for Ethereum users nor is there any mention of the effect of PoS on the egalitarian distribution of new ETH coins.



Facing the enormous difference in block difficulty that the ASIC machines represent, and the fact that this increment is *designed*[6] to happen in order to face the hashrate growth, a new topic rose among miner users and coin/token holders about what to do: apply no changes, hence forcing some users to rely on ASIC providers, and making others to migrate, or ask developers to hard fork the algorithms in order to prevent ASIC miners from operating. Regardless of what option a developer and/or user goes for, this panorama just shows how legitimate and globally-shared concerns about the presence of ASIC machines in the blockchain networks are. Being this one of the reasons why we're proposing a new protocol.

Setting the context

Summarizing the above mentioned aspects, the current scenario of cryptocurrencies introduces at least one decision that protocol creators need to make: either ban or allow ASICs as part of their design. Choosing to avoid ASIC miners in a protocol is interpreted as part of a design that aims to offer better opportunities for regular users mining from unspecialized machines, which can be as important to the system as the blockchain performance.

The enforcement of anonymity is another topic that got blockchain users divided, with some of them considering the possibility of performing public transactions.

Considering that blockchains are increasing in popularity and acceptance, to choose public transactions seems to be the most appropriate strategy for social legitimation and institutional legality. If instead, it's decided to perform completely anonymous transactions, any possible audit will be forbidden,

---

[3] CCN. 2018. *Vitalik Buterin Advises Against Declaring War on Ethash ASIC Miners*. [ONLINE] Available at: https://www.ccn.com/vitalik-advises-against-declaring-war-on-ethash-asic-miners/. [Accessed 10 April 2018].

[4] Ethereum Blog. 2018. *Introducing Casper "the Friendly Ghost" - Ethereum Blog* . [ONLINE] Available at: https://blog.ethereum.org/2015/08/01/introducing-casper-friendly-ghost/. [Accessed 24 April 2018].

[5] GitHub. 2018. *EIP: Modify block mining to be ASIC resistant. · Issue #958 · ethereum/EIPs · GitHub*. [ONLINE] Available at: https://github.com/ethereum/EIPs/issues/958. [Accessed 10 April 2018].

[6] "To compensate the increasing hardware speed and varying interest in running nodes over time, the proof-of-work difficulty is determined by a moving average targeting an average number of blocks per hour. If they're generated too fast, the difficulty increases."Nakamoto, Satoshi (2009). P3

allowing botnets to hide and perform malicious activities that cannot be tracked by governments. Even when crypto anarchists believe blockchain networks to be the antithesis of governments, choosing blockchains over regular institutionalized economies is neither a denial to nation-states legitimacy nor to the civilian duties of their inhabitants.

On the other hand, blockchain users are concerned about the endurability of their efforts, as a consequence of the recent actions of companies like Bitmain, with the production of ASIC machines for Ethereum (which is one of the main platforms currently used for DApps) and the position of some developers responsible for allowing these kind of miners. Ethereum Classic team, which will also be affected by ETH ASICs, hasn't pronounced[7] about these actions, thus reinforcing the worries of the community.

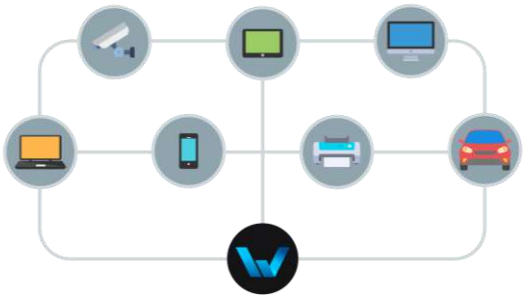
This is the scenario from which Webchain assembles the requirements to be met. The conditions for its deliverance are set next.

Webchain network:

The name is the resulting combination of *web*site and block*chain*, and has been created with a simple and profitable purpose: to secure DApps using regular CPUs and, eventually, mining scripts. In order to succeed at that purpose, *Webchain* applied a modified version of the CryptoNight hashing algorithm and built its own upon the ETC protocol, following ERC20 and ERC223 standards .

Webchain conceives the community of website users as the processing grid for applications. The protocol is constantly being revised in order to avoid exploitation with ASIC, thus keeping well-balanced block difficulty and device performance. There are over 1.5 billion websites, which are delivering millions of services every second; through Webchain each of those sites could be securing DApps.

One of the main limitations for any person willing to mine is to own hardware according to the block difficulty of the blockchain. This usually translates to high-end machines (with cutting edge CPU & memory components) and a stable connection while they work. This approach is limitative both on the usual economic assets of users and the flexibility of connections they have access to.



Webchain doesn't require a particularly good hardware. As long as the device has a processor, it will count on a percentage of unused CPU power and deploy the web miner, which is executed asynchronously. This allows users to mine from a good set of devices like a desktop computer, smartphones, or even those connecting with IoT.

[7] reddit. 2018. *So not a single word about The Bitmain Asics? : EthereumClassic*. [ONLINE] Available at: https://www.reddit.com/r/EthereumClassic/comments/8aswbw/so_not_a_single_word_about_the_bitmain_asics/. [Accessed 13 April 2018].

Besides the possibility of mining coins from almost every internet-connected device, Webchain is botnet unfriendly, as all transactions made on it are public and trackable, a condition that also guarantees that no illicit activities could find a hideout here.

Webchain is a public project managed by a group of developers and admins with the support of its community. The project is available at https://github.com/webchain-network, where people can pull branches and request for merges into the main repository.

The protocol:

Name: *Webchain*
Consensus Mechanism: Modified CryptoNightV7 egalitarian PoW
Base Reward: 50 WEB
Era length: 100 000 blocks (~2 weeks)
Block time: 10 seconds
Smart Contract standard : ERC-20, ERC-223
Locked Premine: 350 000 000 WEB (20%)
Total supply: 1 600 000 000 ~ 1 750 000 000 WEB

CryptoNight[8] is referred to as:

> "a memory-hard hash function. It is designed to be inefficiently computable on GPU, FPGA and ASIC architectures. The CryptoNight algorithm's first step is initializing large scratchpad with pseudo-random data. The next step is numerous read/write operations at pseudo-random addresses contained in the scratchpad. The final step is hashing the entire scratchpad to produce the resulting value." CryptoNight Hash Function (2018). P1

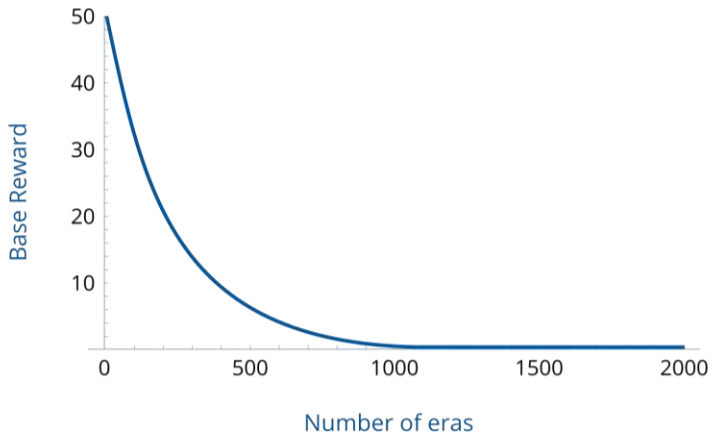
In order to keep an egalitarian distribution of work, *Webchain* will be continuously tweaking the hashing algorithm; preventing exploitation with ASIC machines, as nobody will design an ASIC knowing that it will be useless almost instantly after being implemented.

Blocks are grouped into eras. Each era contains 100 000 blocks, so Era 1 contains blocks 0-99999; Era 2, 100000-199999 and so on. Base reward is reduced every era by 1/250, as described in the following equation:

$$y = 50\left(\frac{249}{250}\right)^{x}$$

Where x represents the number of eras and y the base reward. Better explained, the base reward in Era 1 is 50 WEB, in Era 2 − 49.8 WEB, Era 3 − 49.6008 WEB etc. (see the figure below).

[8] CryptoNight Hash Function. 2018. *CRYPTONOTE STANDARD 008*. [ONLINE] Available at: https://cryptonote.org/cns/cns008.txt [Accessed 17 April 2018].



Webchain: roadmap

This project is thought to be a product under constant development, open to the community and considering both the particular objectives of the project and ETC changes and updates:

2018 - 2nd Quarter:

- GitHub integration
- Social Media campaign
- Announcement Thread on Bitcointalk.org
- Webchain pool development
- Webchain explorer development
- Miner for Webchain
- Webchain network development

2018 -3rd Quarter:

- Include Webchain on JavaScript mining services
- GUI wallet
- Sidechain prototype
- Webchain mobile wallet

2018 - 4th Quarter / 1st Quarter 2019

- Supporting developers to build DApps on top of Webchain
- IPFS
- Compatibility with different blockchains
- Improvements to mitigate differences between local and web mining

More features to come:

- Sharding the Webchain network

References

CCN. 2018. *Japan Wants Cryptocurrency Exchanges to De-List Anonymous Altcoins: Report*. [ONLINE] Available at: https://www.ccn.com/japan-is-pressuring-cryptocurrency-exchanges-to-de-list-anonymous-altcoins-report/. [Accessed 06 May 2018].

CoinDesk. 2018. *Bitmain Confirms Release of First Ethereum ASIC Miners - CoinDesk*. [ONLINE] Available at: https://www.coindesk.com/bitmain-confirms-release-first-ever-ethereum-asic-miners/. [Accessed 10 April 2018].

Cointelegraph. 2018. *Bitmain Announces New Monero-Mining Antminer X3, Crypto'€ ™s Devs Say Will €˜ Not Work€ ™*. [ONLINE] Available at: https://cointelegraph.com/news/bitmain-announces-new-monero-mining-antminer-x3-cryptos-devs-say-will-not-work. [Accessed 10 April 2018].

Cryptocurrency News. 2018. *Coincheck | The Japanese Exchange Drops Monero, Dash, & Zcash*. [ONLINE] Available at: https://cryptocurrencynews.com/daily-news/exchanges/coincheck-drops/. [Accessed 28 April 2018].

CryptoNight Hash Function. 2018. *CRYPTONOTE STANDARD 008*. [ONLINE] Available at: https://cryptonote.org/cns/cns008.txt [Accessed 17 April 2018].

CryptoNote Technology. 2018. *CryptoNote Technology*. [ONLINE] Available at: https://cryptonote.org/inside. [Accessed 26 April 2018].

CRYPTONOTE STANDARD 008 CryptoNote. Available at: https://cryptonote.org/cns/cns008.txt [Accessed April 10, 2018].

Ethereum Blog. 2018. *Introducing Casper "the Friendly Ghost" - Ethereum Blog*. [ONLINE] Available at: https://blog.ethereum.org/2015/08/01/introducing-casper-friendly-ghost/. [Accessed 24 April 2018].

GitHub. 2018. *EIP: Modify block mining to be ASIC resistant. · Issue #958 · ethereum/EIPs · GitHub*. [ONLINE] Available at: https://github.com/ethereum/EIPs/issues/958. [Accessed 10 April 2018].
Kuhn, T.S., 1996. *The Structure of Scientific Revolutions*

Nakamoto, Satoshi (2009), [Bitcoin: A Peer-to-Peer Electronic Cash System. Available at: https://bitcoin.org/bitcoin.pdf [Accessed March 29, 2018].

reddit. 2018. *So not a single word about The Bitmain Asics? : EthereumClassic*. [ONLINE] Available at: https://www.reddit.com/r/EthereumClassic/comments/8aswbw/so_not_a_single_word_about_the_bitmain_asics/. [Accessed 13 April 2018].