Beldex

Private and Decentralized Ecosystem

Version 3.0

July 2nd, 2021

Legal Disclaimer

This document does not constitute or imply a prospectus of any sort. No wording contained herein should be construed as a solicitation for investment. Accordingly, this whitepaper does not pertain in any way to an offering of securities in any jurisdiction worldwide whatsoever. Rather, this whitepaper constitutes a technical description of the functionality of the Beldex Coin and the deployment of a user-friendly platform that will allow users to trade in cryptocurrencies.

The purpose of the document is to present the Beldex exchange project and details about BDX only. There should not be a redistribution of this without further written permission of the BELDEX team or this document and the information contained herein may not be sent or addressed wholly or in part directly or indirectly to any person in countries restricted. Nothing in this white paper shall be deemed to offer a document of any sort of a solicitation for investment or not in any way to offer any securities in any jurisdiction. The project plan was considered carefully before preparing this document. Beldex makes no representations and gives no warranties or guarantees of whatever nature in respect of this document including but not limited to the completeness of any information, facts or opinions contained therein. The founders, advisors, partners, directors, employees, and agents of Beldex and itself cannot be held liable for the use of and reliance on the content in this document.

The information set forth in this White Paper is subject to change. The information set forth below may not be exhaustive of all information that Beldex represents and does not imply any elements of a contractual relationship. This White Paper may be modified to provide more detailed information at any time.

Abstract

A complete privacy-based ecosystem that anonymizes transactions, messages, and your online footprint by incentivizing network validators and creating an economic model that ensures sustainable development of the ecosystem. The private ecosystem consists of the Beldex blockchain, decentralized and anonymous messenger, browser, wallet, a privacy protocol, and the Beldex Bridge connecting to other ecosystems.

This whitepaper provides an overview of the Beldex ecosystem. Any future additions or changes to the ecosystem will be released in subsequent versions of this paper.

1.0 Why Beldex?

Privacy in communication and transactions were often left out as lofty necessities in the past, however, there is a great degree of awareness among individuals about their privacy as global digitization continues to expand. Blockchain is thought to solve this problem. The early adopters of crypto assumed that a blockchain transaction could not be traced back to their origins. However, this false perception was soon debunked when the lot of blockchain analysis firms emerged with solutions for tracing blockchain transactions. This also applies to Bitcoin transactions [1]. Most crypto transactions do not hide the amount of transactions, the sender or receiver addresses and their balances. Coins such as Monero and other private crypto attempted to solve the problem of privacy. Monero, especially, remains an anonymous cryptocurrency with a strong foundation in privacy [2]. But even privacy blockchains were met with issues of scalability in proof-of-work consensus [3]. Moreover, even if a coin does support privacy, it may not support a wallet or an ecosystem. This adds to the deanonymization of transactions. For example, if there are no decentralized wallets, the user of a privacy coin may have to rely on a centralized wallet to store their coins. An institution with sufficient information about the inputs and outputs of a wallet can perform chainalysis to find information pertaining to a transaction, also known as an EABE attack [4]. Beldex proposes a unique, viable solution to the problems of privacy, scalability, and ecosystem.

2.0 Introducing Beldex Blockchain

Beldex is a mined proof-of-work coin with masternodes as a mining opportunity to the community. Originally a fork of Monero, Beldex has integrated PrivateSend privacy protocol from DASH and a few more key privacy features like ViewKey from ZEC to improve the original privacy, as well as its own configurable privacy technology.

BELDEX's core advantages,

- Untraceable Roots - Like Monero which uses RingCT, Beldex too uses RingCT network type but with a higher size of RingCT.

● Conditional Transactions - Transaction will be done only if the specified conditions are met.

● Airdrop - If an individual stakes a certain amount of crypto in the wallet they get a specific number of rewards in terms of the same coins.

● Trustworthy - If the owner reports fraudulence and the suspected receiver is unable to justify the transaction, that particular transaction alone is revertible by the decision of the review tribunal.

2.1 Basic Parameters

Parameters	**Metrics**
Beldex difficulty target(blocktime)	120 Seconds
Difficulty Algorithm	Zawy LWMA
Hashing Algorithm	Cryptonight Conceal
Elliptic curve	Curve25519

2.2 Cryptonote Features

Full node architecture can be implemented with any cryptocurrency, however, Beldex utilizes Monero's source code as its base, since Monero offers greater privacy to transactions using the cryptonote protocol. The CryptoNote protocol proposed a combination of ring signatures, ringCT (confidential transactions), and stealth addresses [5]. Monero's implementation of the protocol offers greater privacy to CryptoNote transactions [6]. When interactions occur across the Beldex independent layers, for example, the second and the first, to reduce the risk due to time-based analysis, an exchange medium that underpins the ecosystem is provided. This means that, when initiating a Flash transaction, users will retain the privacy guarantees offered by the Beldex chain and vice versa.

2.3 Ring Signatures

Ring signatures take many inputs from multiple sources and combine them with the original input from the sender. The original sender's information is concealed with a number of inputs. This masks the true history of outputs from a transaction. Beldex provides mandatory privacy, thus all Beldex transactions will employ Ring signatures and will have a fixed ring size 10 per transaction. For every unique transaction, there are nine other inputs in a ring transaction. Thus, the sender may not have to sign the transaction using their private key, but instead only the ring signature.

2.4 Stealth Addresses

For any crypto transaction, the receiver would have to share their address, either directly to the sender, or on a public forum, thus revealing the details of their transaction. Beldex uses a form of intermediary addresses called stealth addresses to obfuscate the identity of the receiver. Whenever a sender initiates a transaction, the receiver generates a one-time intermediary address and funds are sent to this address. Funds sent to the intermediary address always reflect on the public address. The Diffie-Hellman key exchange enables the receiver to generate a private spend key for their intermediary address. So, they can claim ownership of the funds transferred to this intermediary address [7]. Thus, the receivers in a Beldex transaction are protected by a one-time expendable stealth address.

2.5 RingCT

Protecting transactional privacy doesn't stop with obfuscating the sender and receiver identity. To prevent any time-based analysis of transactions using the amount transferred, Monero Research Labs first proposed Ring Confidential Transactions (RingCT) as a means to obfuscate the amount in a transaction. RingCT uses range proofs which employ Pedersen commitments to ensure that the amount transferred can be verified without knowing the actual value, and this range is between 0 and 2^{64}. If Alice sends an amount x to Bob, she commits a value y and hashes y to the secret x such as $H(x||y)$. Once Bob receives the amount, she can then reveal her secret and Bob can verify that Alice indeed committed the correct outcome y. Thus, with Pedersen commitments, one can ensure that only non-negative values are sent and the actual value is masked. The size of crypto transactions that use traditional range proofs are large, thus, as an alternative, bulletproofs is used to greatly reduce the size of the transaction [8]. Therefore, to improve transaction scalability, Beldex will utilise a form of bulletproofs to reduce the payload that nodes and masternodes are required to store and transmit.

2.6 Masternodes

Beldex improvises on the CryptoNote protocol to provide greater privacy; however, a group of incentivized masternodes determine most of the functionality and scalability in Beldex. These masternodes are full nodes that store the entire copy of the Beldex blockchain. To set up a Beldex masternode, a node operator must lock-in aminimum collateral and possess the required minimum bandwidth and storage capabilities. The collateral ensures that the masternode operators refrain from acting dishonestly, as they have a significant stake in the network. As compensation for their services, masternode operators receive a portion of the block reward. A masternode is continually reviewed and if it is found to act dishonestly or doesn't provide the required bandwidth at any time, then it is penalized and moved to the end of the reward queue. A maximum of three warnings is given to a masternode operator before they are removed from the network.

The network thus formed is resistant to Sybil attacks, in which a single or a group of bad actors work in coalition to undermine the network. The initial setup collateral and the periodical review of masternodes ensure that such attacks are prevented. The maximum amount of stake a single validator can have is limited by supply and demand, preventing one validator to have a disproportionately large stake so as to sabotage the second-layer ecosystem services. Resistance to Sybil attacks can also be acquired through Cryptoeconomics [9]. When a bad actor begins to accumulate Beldex (BDX) in order to obtain a majority stake within the network, the supply in circulation decreases and inturn drives the price up. Acquiring additional Beldex becomes increasingly expensive, thus making the attack economically unfeasible. This disincentivizes the attacker. To ensure that masternode validators obtain sustainable returns for their services, the circulating supply is actively reduced and the emission curves and minimum collateral requirements are designed such that enough circulating supply is locked within the masternodes.

2.7 Block Reward

Block rewards in the Beldex network are currently distributed through proof-of-work consensus. A node or a masternode creates a new block every 10 minutes by collecting the transactions, validating them, including them within the block, and adding the block to the end of the network. To perform this action, they maintain a certain bandwidth and expend power to do so. In return, they collect block rewards as new BDX coins are emitted. The Beldex block reward is set to a constant value of 2 BDX.

Node Reward: In addition to the transaction fees, 10% of the block reward is awarded to the node that constructs the block.

Master Node Reward: 90% of total Beldex rewards go to a Masternode, or two Masternodes if both the masternodes construct the block at the same time. Once the Masternode receives a reward, it assumes the last position in the reward queue. Thus, nodes that recently received rewards are moved to the end of the reward queue while nodes that have been waiting for a longer period are moved to the start of the queue. The very first time a Masternode validator is indexed on the network's distributed decentralized directory, it assumes the last position in

the reward queue. The masternodes that are found to provide optimum services to the network continually move up the queue, if they are not otherwise penalized.

2.8 Authenticated Collateralization

A masternode operator may stake this amount entirely by themselves or stake part of the amount and let other users stake the remaining. In this case, they share the rewards based on their stake within the masternode. To be added to the Beldex distributed directory, each Masternode must prove to the network that they hold the necessary stake, which is 10000 BDX. The innate privacy features of Beldex prevent the masternodes from doing so as public addresses do not reveal the amount of transaction. They also cannot use viewkeys to see transactions going out of the network.

To solve this dilemma of Masternodes, Beldex uses a novel method of time-locking the collateral. The initial collateral by a masternode is locked for a specific block-height, say *X* blocks. Thus, from the time of registration until *X* blocks are created, the masternodes will be unable to spend this collateral. Beldex leverages this method to ensure that a particular masternode holds the required collateral amount.

First time Masternode registrants will time-lock an output for 8640 blocks. The locked output can only be spent after the required number of blocks has been transcended. In the additional field of transaction, the Masternode operator provides the Beldex address to receive rewards. This address is the public key of the Masternode operator. The transactions for the purpose of registration are open transactions, thus they may not be included in a ring transaction as they do not serve to provide anonymity.

The existing Masternodes in the network must verify that the first time Masternode registrants possess the required collateral before they are added to the distributed decentralized directory.

2.9 Flash

Flash instant transactions are a second layer atop the Beldex blockchain that allows for confirmation of transactions before they are included in a block. Blockchain transactions typically take the time required for the transaction to be included in a block and confirmed by the network. A Beldex transaction requires 10 confirmations and the block creation time is 2 minutes. Thus, it may take anywhere between 20-40 minutes for a transaction to be confirmed. But with flash, it only takes a few seconds.

The Beldex second layer architecture (Flash) is similar to Bitcoin’s lightning network in that a shortest possible route is selected between the Flash channels [10]. A channel path reducing algorithm is used to send the outputs to the receiver, where channels from users who’ve made transactions with each other before become relays. If B has sent or received inputs from A and C, then B can act as a relay in transactions between A and C.

Flash instant transactions are feasible through the use of Masternodes that confirm a transaction's authenticity by securing the key images associated with the UTXOs. In a ring signature transaction, the UTXOs are linked to a distinctive key image. Select Masternodes store this key image and hold onto it until the transaction is added to a block on the Beldex network. If the said key image is produced more than once, then that signals a double spending attempt. The corresponding duplicate transaction is rejected.

Similar to Ethereum, Flash will enable a mechanism for competing transactions to pay a higher fee to be completed first. But this is several times faster and will be in the order of a few seconds since it takes place outside the blockchain. Confirmation time on the blockchain is also significantly reduced due to the network transition to a Proof-of-Stake (POS) consensus.

2.10 Coin Burning Mechanism

The Beldex coin burning mechanism is a way to curb inflation and deliver sustainable price discovery. To achieve this, the network fee obtained through Flash transactions is burned.

2.11 Proof-of-Stake (POS) in Beldex Chain

POS is an alternative to POW that is designed to be economical and energy-efficient. At present, most cryptocurrencies run on a POW algorithm that consumes a lot of energy through mining hardware. Newer and powerful hardware is developed to plow through the hashrate. This hardware is often not affordable to everyone, making them less decentralized and they consume several KW of power every day. Bitcoin's annual energy consumption index is an estimated 95.87 TWh, according to Digiconomist [11].

Beldex initially proposes the implementation of the RandomX algorithm to prevent ASIC mining and provide equal opportunity to CPU and GPU miners. However, Beldex will be implementing Proof-of-Stake in its network. Currently, the Beldex POS is in the testnet stage and is being tested for attacks against privacy and security. Later, this will be upgraded to a full POS network. A full POS Beldex network will enable users to stake BDX on nodes. Those with a stake can participate in validating blocks on the network. The higher the stake, the higher the chances for the node to be selected to validate a block, and the lower is the difficulty. POS on Beldex is based on delimited competition of nodes.

Anyone is free to contribute to the Beldex network, given the required collateral staking amount is locked in the node. Dishonest nodes are disincentivized and their collateral is devalued. This prevents the nodes from acting against the network whereas honest nodes are rewarded and appraised. Beldex also provides pool staking via masternodes where the hardware is shared between a few individuals who share the stake amount (10,000 BDX).

3.0 Beldex Services

3.1 Beldex Decentralized Wallets

3.1.1 Decentralized Web Wallets

The decentralized web wallets can be accessed through the websites wallet.beldex.io and walletv2.beldex.io. Both the wallets are a means for BDX users to hold, send, or receive their BDX. Version 2 of the wallet (walletv2.beldex.io) provides additional features such as creating multiple Beldex wallets and adding contacts. As they are decentralized, they can be accessed only with the unique Mnemonic Key. Both wallets offer the privacy of transactions.

3.1.2 Android & iOS Wallet

The Android and iOS wallets come with the same features as the Beldex electron wallet. The mobile wallets provide instant access to the Beldex wallet. Store, send, receive, or stake BDX. You can download the Beldex wallet for Android devices here. The wallet for iOS devices is also under development.

3.1.3 Beldex Electron Desktop Wallet

The Beldex Electron desktop wallet is a downloadable application built for Windows and Linux. The electron desktop wallet is fast, secure, and decentralized. It allows for the storage and transaction of BDX. A unique feature of the Beldex electron wallet is that it also supports pool staking. In pool staking, users can select the node and the amount to stake to validate blocks via masternodes. Later, the electron wallet will also support Mac devices.

3.2 Beldex Bridge

3.2.1 Binance Smart Chain Bridge

Binance Smart Chain is one of the fastest-growing ecosystems. The blockchain allows for interoperability with the Binance Chain and other platforms being built on it. Beldex will be bridging the BDX coin to the Binance Smart Chain without trading off its inherent privacy features. The BDX coin can be swapped for the Wrapped-BDX (wBDX) token on the Binance Smart Chain. Each wBDX token is backed by the BDX coin in a 1:1 ratio. The wBDX privacy token can be utilized on the Binance Smart Chain platforms. Users can also swap back wBDX to BDX using the Beldex-Binance Smart Chain Bridge.

3.2.2 ETH Bridge

The Beldex network is a native chain, and thus, it has to be bridged to the Ethereum chain in order to utilize BDX on the Ethereum platform. The Beldex to Ethereum Bridge will allow

the BDX token to exist as an ERC-20 token on the Ethereum chain in a 1:1 ratio. This will allow Beldex tokens to be utilized on various Ethereum based platforms and wallets. The corresponding ERC-20 tokens can be swapped back to BDX coins on the Ethereum bridge.

3.2.3 DOT Bridge

DOT is an emerging Ethereum competitor. Thus, Beldex will be bridged to the Polkadot chain to improve interoperability between the Beldex-Polka chains. The Beldex to Polkadot Bridge will allow the BDX token to exist as a DOT-based token on the Polkadot chain in a 1:1 ratio. This will allow Beldex tokens to be utilized on various Polkadot based platforms and wallets. The corresponding DOT-based ERC-20 tokens can be swapped back to BDX coins on the Ethereum bridge.

3.3 Beldex Privacy Protocol

The Beldex privacy protocol is cross chain payment privacy and anonymity protocol that anonymizes transactions on the Bitcoin, Ethereum, Polkadot, BSC, and Cosmos chains. To achieve this, Beldex uses a form of the zk-SNARKS algorithm first proposed by ZCash [12] along with the Zether protocol [13] and El Gamal encryption. Bulletproof range proofs are used to reduce the size of the transaction.

The Beldex privacy protocol is deployed on the substrate of the Binance Smart Chain network, essentially a second layer. Let's consider that user A wants to anonymously send Ethereum (ETH) to user B. Beldex provides the perfect platform for this operation.

User A creates an account on the Beldex protocol. They then proceed to burn their Ethereum tokens on the Ethereum chain for equivalent wrapped privacy tokens on a 1:1 ratio on the Beldex chain, say b-ETH. User 'A' then sends an X amount of b-ETH to user 'B' by initiating a transaction via the Beldex privacy protocol. Once the token is received, the user 'B' can then reclaim ETH from b-ETH. User 'B' will however, not know the amount that was locked in the contract by user 'A'.

With the aid of zk-SNARKS, the network can verify that user A has the ownership of the privacy tokens that were transferred. The El Gamal homomorphic encryption ensures the verification of the inputs and outputs, even if the actual values of transactions are not known; whereas to obfuscate sender and receiver identity, a "one-out-of-many" protocol is used. Beldex uses RingCT for this purpose.

3.4 Decentralized Messaging App (B-Chat)

B-Chat is an anonymous messaging application that routes messages using BelNet. With modern day applications such as WhatsApp and Signal, messaging has become end-to-end encrypted. The Signal protocol [14], especially, has proven to offer a greater degree of

privacy than the former. However, end-to-end encryption does not offer complete privacy as the data is ultimately stored on a centralized data centre. Centralized data centres are susceptible to attacks due to their centralized nature. They are also sparsely protected against government policies and intervention. There's no preventing a government or an authority from mandating centralized messaging applications to share user data. This takes away the privacy that is offered by these applications.

B-Chat introduces routing of messages through the BelNet, a decentralized Virtual Private Network (dVPN). The decentralized VPN, the BelNet, ensures that messages are routed to their destination through the shortest possible node distance while encrypting them at each hop. The minimum hop length is set as 3, not counting the origin and destination nodes. This prevents a dishonest node from sabotaging the message as it only receives an encrypted form of the message to begin with.

Messages can be sent by the sender even if the receiver is online or offline, with the help of Beldex Secure Masternodes. When the receiver is online, the message packets get routed through the masternodes. The secure Masternodes act as the routing channel when user A wants to send a message to user B. The Masternode determines the shortest possible distance over which the message can be routed on the routing channel. To do this, the origin node (node where the message originates) gets the destination nodes' information from the distributed decentralized directory stored by the Masternodes. Then, it establishes a safe route while checking for available bandwidth and traffic congestion. It then transmits the message, which gets encrypted at each node hop and a minimum of three node hops are required for each message packed. The message is received by the destination node which in turn relays it to the user B. When the user B is offline, the closest node, or the destination node, stores the message and relays it when they return online.

3.5 BelNet

Virtual Private Networks (VPNs) have enabled people to remain anonymous with their online activity. But today's VPNs aren't completely private since most of them are managed by centralized systems. Existing onion routing protocols such as Tor offer minimum decentralization while their Distributed Hash Tables (DHTs) are managed by a handful of nodes called Directory Authorities [15]. Thus, they offer only rudimentary privacy.

On the other hand, an onion routing protocol on a blockchain network will remain completely decentralized, and therefore offers greater privacy. BelNet is a private decentralized VPN that works based on the Beldex Routing Protocol (BRP). The BRP optimizes the communication between nodes such that the traffic is traversed through the network with minimum load to the secure Masternodes.

The BRP uses the packet switching routing model and supports a wide range of internet protocols. It's Distributed Hash Table that lists the nodes on the network is maintained by Masternodes, based on a node limiting and authorizing mechanism. The governing Masternodes are a set of nodes that get randomly assigned to verify an incoming new node.

A new node must meet the bandwidth and staking requirements to obtain the status of a relay or exit node on the BelNet. The governing nodes are reassigned to each node and at fixed time intervals, they keep verifying if a node has sufficient bandwidth. If any node fails to meet the bandwidth requirements, then they are penalized by the governing nodes and their rewards get cut until they provide the required bandwidth. The significant staking capital also prevents the nodes from acting dishonestly in the network.

3.6 Wallet Browser Extension

The Beldex decentralized wallet will be provided as a downloadable extension on the Chrome and Firefox browsers which can be used to connect the wallet to other platforms.

3.7 Beldex Browser

The online advertising industry thrives out of unwarranted advertising by tracking user activity. User privacy is disregarded day in and day out. In addition, certain applications have the practice of monitoring a users' offline data. In today's advertising industry, however, data processors or middlemen take away a large sum of this ad revenue from content authors. Large players have also monopolized the advertising market [16]. To combat this, Beldex proposes the Beldex browser, a secure and privacy-first browser that adds value to advertisers and content creators while preserving user privacy.

The Beldex browser routes user traffic using BelNet and the Beldex Masternodes, which anonymizes the source and destination of the traffic. Users choose the content they want to pay their attention while content creators and advertisers can target a more specific audience. Donning the peer-to-peer agenda, content authors can publish ad-free content to their audience who may choose to pay creators for their content with BDX.

4.0 Marketing

4.1 Community

Beldex has had a very strong community base since inception. Beldex has various channels for engaging with the community. You can find the full list of announcement boards and social media below.

Telegram Announcements: https://t.me/official_beldex
Telegram Chat: https://t.me/beldexcoin
Twitter: https://twitter.com/BeldexCoin
Discord: https://discord.gg/Hj4MAmA5gs
Facebook: https://www.facebook.com/beldexofficial
Instagram: https://www.instagram.com/beldexcoin/?hl=en
LinkedIn: https://in.linkedin.com/company/beldex-coin

Medium: https://beldexcoin.medium.com/

4.2 Bounty and Airdrop

Tokens reserved for the purpose of bounty and airdrop are 80,000 BDX tokens valued at $10,000 USD. Airdrops will be conducted at regular intervals at the discretion of Beldex.

5.0 Contributions

Beldex contributors are primarily masternode validators who strengthen the network by setting up masternodes and validating blocks. To contribute to the Beldex network, you can either set up a dedicated masternode or stake on platforms that support Beldex masternode staking. Validators can also share the minimum collateral of 10000 BDX to set up a masternode and for this purpose, Beldex will partner with shared masternode pools where they can easily stake a BDX amount of their choosing and receive rewards proportional to their stake.

Independent developers who are interested in contributing may contribute to Beldex on their own volition. Developers can find the open source Beldex source code here. To contribute, leave a message on our discord channel and our team will get back to you.

References

[1] *Bitcoin, https://bitcoin.org/en/protect-your-privacy#*

[2] *Monero, https://getmonero.org*

[3] *P. Monero-Sanchez et al., "DLSAG: Non-Interactive Refund Transactions For Interoperable Payment Channels in Monero," https://eprint.iacr.org/2019/595.pdf*

[4] *Github Comment - EABE/Knacc Attack, https://github.com/monero-project/monero/issues/1673#issuecomment-312968452*

[5] *N. van Saberhagen,"CryptoNote v 2.0," https://web.archive.org/web/20201028121818/https://cryptonote.org/whitepaper.pdf*

[6] *K. M. Alonso, J. H. Joancomarti, "Monero Privacy In The Blockchain," https://eprint.iacr.org/2018/535.pdf*

[7] *W. Diffie, M. E. Hellman, "New Directions in Cryptography," https://ee.stanford.edu/~hellman/publications/24.pdf*

[8] *B. Bünz, J. Bootle, et al.,* "*Bulletproofs: Short Proofs for Confidential Transactions and More," https://eprint.iacr.org/2017/1066.pdf*

[9] *M. Quintyne-Collins, "Short Paper: Towards Characterizing Sybil Attacks in Cryptocurrency Mixers," https://eprint.iacr.org/2019/1111.pdf*

[10] *J. Poon, T. Dryja, "The Bitcoin Lightning Network: Scalable Off-Chain Instant Payments," https://lightning.network/lightning-network-paper.pdf*

[11] *Bitcoin Energy Consumption, https://digiconomist.net/bitcoin-energy-consumption/*

[12] *E. Ben Sasson et al., "Zerocash: Decentralized Anonymous Payments from Bitcoin," 2014 IEEE Symposium on Security and Privacy, https://ieeexplore.ieee.org/document/6956581 2014, pp. 459-474, doi: 10.1109/SP.2014.36.*

[13] *Zether protocol, https://eprint.iacr.org/2019/191.pdf*

[14] *K. Cohn-Gordon, C. Cremers, et al., "A Formal Security Analysis of the Signal Messaging Protocol," https://eprint.iacr.org/2016/1013.pdf*

[15] *How China Blocks the Tor Anonymity Network, https://www.technologyreview.com/2012/04/04/186902/how-china-blocks-the-tor-anonymity-network/*

[16] *How Google and Facebook Have Taken Over the Digital Ad Industry, Fortune, http://fortune.com/2017/01/04/google-facebook-ad-industry/*