Xolentum

Sayan Bhattacharyya, Ngeo Jia Jun

Version 1

January 1st, 2021

1. Introduction

Privacy is a key factor, when it comes to digital transactions and exchange of data. At present, a majority of the existing digital currencies have a public ledger, which means the activity, transactions and balances of a user are open to the world. This is a ridiculous level of transparency as it completely eliminates the basic privacy rights of a user.

Xolentum is a decentralized, peer-to-peer and open-source digital currency. Our base is off Monero, a cryptocurrency that has established itself as one of the most secure and private transaction networks to date [1]. However, we've improved upon our parent codebase with some significant changes. (See 6 and 8.4)

At Xolentum, a user's privacy rights are placed above all else. Not only is the network private, but also fast and secure.

2. Why Xolentum?

- *Xolentum is fast*

  Xolentum has a 60-second block time, which means transactions are processed in a span of just a minute.

- *Xolentum is secure*

  Xolentum is a decentralized network and hence operated by a network of users. Transactions are confirmed by distributed consensus and then immutably recorded on the blockchain.

- *Xolentum is untraceable*

  Transactions on the Xolentum blockchain cannot be tracked as the origin, destination and transacted amounts are obfuscated by default.

3. Xolentum for all

One of the primary goals behind sticking with *RandomX* for the hashing algorithm is to make sure that everyone is able to mine Xolentum, regardless of the hardware they use. Xolentum is ASIC-resistant, optimized for CPU. GPUs are able to mine Xolentum, however at 1:1 with CPUs, there is no additional GPU advantage.

4. Basic Parameters

Xolentum Difficulty Target (Block Time)	60 seconds
Difficulty Algorithm	Zawy LWMA-4 [2]
Hashing Algorithm	RandomX [3]
Elliptic Curve	Curve25519 [4]

5. CryptoNote

Xolentum code is based on the CryptoNote [5], an application layer protocol which was the pioneer in privacy-oriented decentralization, which powers several such currencies at present.

5.1 Ring Signatures

Ring signatures work by constructing a ring of possible signers to a transaction where only one of the signers is the actual sender. Xolentum makes use of ring signatures to obfuscate the true history of transaction outputs. Ring signatures will be mandatory for all Xolentum transactions (excluding block reward transactions), and uniquely, a fixed ring-size of 5 is enforced on the Xolentum blockchain. This means that each input will spend from one of five possible outputs, including the true output.

5.2 Stealth Addresses

Xolentum makes use of stealth addresses to ensure that the true public key of the receiver is never linked to their transaction. Every time a Xolentum transaction is sent, a one-time stealth address is created and the funds are sent to this address. Using a Diffie-Hellman key exchange, the receiver of the transaction is able to calculate a private spend key for this stealth address, thereby taking ownership of the funds without having to reveal their true public address. Stealth addresses provide protection to receivers of transactions and are a core privacy feature in Xolentum.

5.3 RingCT

RingCT was first proposed by the Monero Research Lab as a way to obfuscate transaction amounts [6]. Current deployments of RingCT use range proofs, which leverage Pedersen commitments to prove that the amount of a transaction being sent is between 0 and 264. This range ensures that only non-negative amounts of currency are sent, without revealing the actual amount sent in the transaction. Recently a number of cryptocurrencies have proposed implementing bulletproofs as a replacement to traditional range proofs in RingCT because of the significant reduction in transaction size [7].

Bulletproof v1 was MLSAG (Multilayered Linkable Spontaneous Anonymous Group). When Xolentum was incorporated, the idea of CLSAG (Compact Linkable Spontaneous Anonymous Group) was already proposed and mostly implemented in the parent codebase. With an independent development scheme thereon, CLSAG fitted perfectly into our code and when Xolentum launched, CLSAG was already activated.

6. Transaction Proof-of-Work

Transaction PoW has been implemented to introduce a computational barrier for the evil party who attempt to bloat the network chain using tremendous number of transactions [8]. In general, with this barrier enabled, the only way to push a transaction is by having the sender mine it like they are mining the blocks.

6.1 Implementation

Starting with transaction v2, a mandatory field named "nonce" is introduced in the transaction body (not transaction prefix). Before a transaction is considered valid, a difficulty check is done before the input checking is even executed. This helps prevents DDoS by bottlenecking the disk bandwidth required to validate the inputs.

6.2 PoW function

We have made every attempt to make it as memory hard as possible while ensuring normal users could send transactions. After numerous discussions, we decided to go with the CryptoNight algorithm as the PoW function. Due to the fact that pruning will remove some data from transaction body itself, we resorted to run the function on the pruned transaction blob instead of unpruned one. This will allow pruning node to verify the PoW even if the transaction is pruned.

6.3 Integration

v4 - Activation of TX PoW
v5 - Enforcement of TX PoW

7. Block Reward

Distribution of block rewards in Xolentum is conducted through proof-of-work, a robust and well-studied system for the creation of blocks and the ordering of transactions. Miners collect and write transactions into blocks and collect fees for doing so.

The current block reward scheme is 50 XOL till block 42000 (2.1 million emission), 8 XOL thereon. The sudden drop is clearly questionable; however, this is what was decided via a community poll.

At present, 100% of the block reward goes to the PoW mining.

8. CryptoNote Differences

8.1 ASIC Resistance

An application-specific integrated circuit (ASIC) miner is a device that is designed for the sole purpose of mining digital currency. Generally, each ASIC miner is constructed to mine a specific digital currency. There are several benefits of ASICs such as securing the network by increasing the network hash rate, and ensuring miners behave decently due to the huge amount of investment that goes into purchasing of an ASIC. However, they simultaneously pose a risk to decentralization because they outpace all other mining methods, are manufactured by specific companies, have very limited distribution channels due to the specialized nature of the hardware, and they require significant capital costs to develop and operate profitably.

Regardless of the benefits of ASICs mining the network, we believe that Xolentum should be for the common man; hence CPUs should be supported instead of ASICs dominating the network. Hence, we have adopted a proof-of-work (PoW) algorithm that is optimized for general-purpose CPUs – *RandomX.* GPUs are able to mine; however, they are at a disadvantage because the algorithm is optimized for CPUs by design.

8.2 Dynamic Block Size and Fees

Unlike many other CryptoNote coins, Xolentum neither has a static block size nor a static fee. The long-term concern in other cryptocurrencies is that large block sizes burden the nodes that store and verify transactions. As block sizes grow, nodes that run on lower grade hardware are unable to process and propagate new blocks, leading to centralization of the node network among those with a commercial interest in maintaining nodes. This can be concerning because distributing the blockchain across many nodes allows for the state of the chain to be confirmed among many different parties, adding to its validity and censorship resistance.

Although there exists a limit, it is adaptive based on the past 100 blocks. Similarly, fees change based on transaction volume. As more transactions are processed on the Xolentum network, the block size limit slowly increases and the fees slowly decrease. The opposite effect holds

true.

8.3 Ring Signature Size

Ring signatures are used to hide real outputs amongst others in any given transaction. The size of a ring signature refers to how many mixins are used to construct the ring.

Unlike a few other CryptoNote coins, Xolentum does not have a dynamic ring signature size, wherein only a minimum is enforced. Xolentum has a static ring size of five. Statically setting the maximum ring-size protects users who construct rings with more than four mixins and setting the ring-size minimum to five more effectively prevents an attacker who owns a large number of outputs from discerning the true outputs spent in a ring signature. Larger ring-sizes also increase the default churning effectiveness non-linearly, becoming more effective as ring-sizes grow.

8.4 Configurable Block Reward System

We have decided to go a different way than both BitCoin and Monero protocol. Tail emission is an unproven system, and so is fees-only. The way block rewards and emission is calculated has been changed in the implementation. Instead of tail emission, we have opted for a configurable block rewards system. This gives us greater control of the emission and can be reduced or increased as needed.

9. Funding

Xolentum is a community sponsored project, with no pre-mine or initial coin offering. Donation addresses can be found on our community funding page. View keys for the private blockchains, that is, Monero and Xolentum have been provided to maintain transparency.

Besides, a few companies have stepped forward to back our project, sponsoring us with various products such as servers for our operation.

10. Conclusion

Xolentum aims to provide a fast, secure, and economical means of digital transactions, powered by the CryptoNote protocol which has revolutionized privacy in blockchains.

References

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

[2] *LWMA Difficulty Algorithm*, https://github.com/zawy12/difficulty-algorithms/issues/3

[3] *RandomX*, https://github.com/tevador/RandomX

[4] *Curve25519*, https://www.intechopen.com/books/theorizing-stem-education-in-the-21st-century/implementation-of-elliptic-curve25519-in-cryptography

[5] *CryptoNote, Nicolas van Saberhagen, CryptoNote v 2.0 (2013)* https://bytecoin.org/old/whitepaper.pdf

[6] *Shen Noether, Adam Mackenzie, and Monero Core Team, Ring Confidential Transactions (2016)*, https://www.getmonero.org/resources/research-lab/pubs/MRL-0005.pdf

[7] *Bulletproofs: Short Proofs for Confidential Transactions and More (2017)*, https://eprint.iacr.org/2017/1066.pdf

[8] *Transaction Proof-Of-Work*, https://forum.nkn.org/t/nkp-0014-use-pow-to-prevent-generate-id-txn-spam/1668