# DigitalNote XDN

http://digitalnote.biz

Revised 30 August, 2018


**Abstract**

*In this whitepaper we present DigitalNote XDN, a brand new technology for securely transferring money and messages between anonymous peers. The new version of the XDN protocol also provides staking with a reward rate. Our solution is based on the CryptoNote code base and keys/addresses system including multi-signatures outputs and ring signatures. [1] [2]*


## 1 Introduction - Launch story.

DigitalNote XDN was originally launched and announced as "duckNote" cryptocurrency on May 30, 2014. It's aim was to introduce a new coin with new and unique features based on the anonymous CryptoNote technology to the cryptocurrency community. A libertarian economy with an original supply curve, proven fair decentralization with CPU-efficient ASIC-resistant mining process, brilliantly scaled network specifications, user friendly cross platform GUI wallet and numerous network improvements were introduced DigitalNote XDN in its duckNote appearance. [3]

In mid-September, 2014 XDN took the next step and duckNote was rebranded as DarkNote, incorporating many new unique features such as untraceable encrypted messages, transfer aggregation, core code and network improvements.

## 2 DigitalNote features:

- Unlinkable transactions (Appendix A)
- Untraceable payments (Appendix B)
- Blockchain analysis resistance (Appendix C)
- CPU-efficient ASIC resistant Proof-of-work (Appendix D)
- Adaptive and scalable (Appendix E)
- Untraceable encrypted messages (3)
- Multi-signature support (4)
- Staking based on blockchain technology (5)

In the next sections we will present DigitalNote XDN's unique features.

# 3 Encrypted messages

## 3.1 Motivation

DigitalNote XDN has made an encrypted untraceable messaging platform where only the recipient can decrypt his message and the message can be stored on a blockchain.

Cryptocurrency is about digital money and the money flow between parties. However bare transfers are inconvenient and are just transfers. In most commercial applications, the payee needs additional information from the payer. For example, an on-line store supports a "money-back feature" and its customer should be able to attach his refund address to his transaction. Alternatively, when you make a donation you may want to specify how your funds should be distributed between all possible charities (just like Humble Bundle allows you to divide your purchase between games' developers). The use of the message facility is able to address this.

The urgency of introducing this feature is supported by the fact that some of the top cryptocurrencies had already implemented it: Bitcoin [4], Florin [5], Cosmoscoin [6] etc. Their developers, however did not attend to convenience of private communication. Whilst there is no problem with attaching a plain-text message, it is tricky to provide an easy-to-use way of handling of secret data.

Both parties can share some *symmetric private key* and use it for encrypting and decrypting messages. But this method is only suitable for continuous and long term communication and/or repeated transactions. Another way: they can use a *public key encryption scheme*, but such algorithms are less effective in case of arbitrary-length messages (when compared with symmetric crypto). We propose a protocol for transferring encrypted messages within transactions, which does not require any preliminary data exchange and it is based on the modern symmetric stream cipher — ChaCha20 [7] — with excellent performance criteria.

## 3.2 The protocol

Here is an example of how the protocol is used in encrypting and decrypting a message. The message is being sent from Alice to Bob:

1. Alice generates a common secret via Diffie-Hellman key exchange protocol at the same CryptoNote one-time keys are generated.
2. She encrypts her message under this key and sends the transaction.
3. Bob re-generates the common secret, just like he recovers CryptoNote outputs private keys.
4. He tries to decrypt all available messages in the transaction and determines (via a checksum) those which were sent to him.

### Encryption

Let $(A, B)$ be Bob's CryptoNote address and H() to be cryptographic hash function Keccak. Alice generates a random value $r$ and computes the common secret $x = H(r \cdot B)$. Additionally she stores $R = r \cdot G$.

Alice takes the plaintext message M and adds four zero bytes to the end. The motivation behind this step will be shown later. After that she uses x as a key for stream cipher ChaCha20 and gets a pseudo-random bit sequence, S.

The resulting encrypted message is $E = M \oplus S$. It is stored together with R on the transaction.

**Decryption**

Bob receives the transaction and re-generates the common secret as $x = H(b \cdot R)$. With $x$ he recovers the same sequence $S$.

Then for every encrypted message $E_i$ he computes $M_i = E_i \oplus S$. $M_i$ which has the last four bytes zeroed indicated they were sent to him, i.e. decrypted correctly. The others may belong to other recipients of the transaction or even be Alice's comments for herself.

### 3.3 Separate messages

Our solution does not rely on an output properties: payee, amount, any other content. That means that transaction comments may be used separately with money transfer, i.e. like just private messages (without payments). Alice can send many messages to different addresses in a single transaction which sends some funds to herself. Due to CryptoNote's unlinkabile onetime keys, no one can prove that there was any money transfer at all: i.e. private message via transaction is indistinguishable from ordinary transactions.

DigitalNote XDN can serve as a service of private encrypted communication, as well as secure money transfers.

### 3.4 Other applications

- **Greetings** A digital postcard with personal "X-mas greetings" and some present inside.
- **Moneyback** A customer can specify his public address (with occasional purchases as he may not have a permanent account on a site), so that only the merchant can see it.
- **Payment ID** The use of a Payment ID allows the merchant to use one address in their wallet to trace multiple customer transactions.
- **Donations** A donator can specify (in a public or private manner) how to distribute his/her pledge.

## 4 DigitalNote Multi-signatures

A multi-signature address is an address that is associated with more than one ECDSA private key. The simplest type is an m-of-n address - it is associated with n private keys, and sending bitcoins from this address requires signatures from at least m keys. A multi- signature transaction is one that sends funds from a multi-signature address. There are several Multi-signatures use cases. One is to greatly increase the difficulty of stealing the users XDN. With a 2-of-2 address, you can keep the two keys on separate machines, and then any theft will require someone having to compromise both, which is very difficult. (e.g., one pc and one dedicated device, or two hosted machines with a different host and OS). It can also be used for more advanced scenarios such as an address shared by multiple people, where a majority vote is required to use the funds. It can also be used for redundancy to protect against loss - with a 2-of-3 address, not only does theft require obtaining 2 different keys, but you can still use the coins if you forget any single key. This allows for more flexible options than just backups.[8]

# 5 Staking with award rate based on XDN blockchain

You can safely stake your DigitalNote on the blockchain for reward. In June 2015 DigitalNote XDN introduced a new blockchain feature: time-locked staking with a variable annual rewards. It allows users to “lock” some of their XDN for a given number of blocks in return for a reward.

Staking is implemented via new types of transaction output/outputs. It includes the staked amount, destination key (or keys) and staking duration which is expressed in blocks to lock the funds for. The transaction itself contains the field unlock time but output-specific parameters are much more convenient, because a user may want not want to lock up all of their funds. The new staking transaction is then included on the blockchain and the counter starts.

When the lock expires, the user can spend this output as usual including the staking reward. Staking acts as a new source of emission.

DigitalNote XDN **multi-signature** core feature enables a common ownership for any DigitalNote XDN units and staking in particular. A family can store their DigitalNote XDN savings in N-of-N staking, which means that only all members together can withdraw the money. Company can keep its capital in M-of-N address, which is redeemable only by at least M members out of N.

Reward rates depends on the staking time and varies from 11000 to 999999 blocks. The longer the period of staking, the higher the reward. The relation takes form of hyperbolic function, as shown below.

# 6 Future Features

Security is the highest priority of any money-related system. DigitalNote XDN will investigate implementing new and improved methods of securing the network, including new Algorithms that retain our ASIC resistance status.

[1]Duckoshi is the smallest XDN unit

# 7 Other DigitalNote specific features

## 7.1 Block time, transaction processing and orphans

DigitalNote has a 2-minute block interval. In general, it is 5x times faster than Bitcoin. It provides almost a negligible quantity of orphan blocks compared with other CryptoNote currencies. Less orphans lead to more profitable mining to secure the network.

## 7.2 Emission process

The total number of XDN is 8589869056, which is a 6th perfect number [9]. Whilst it may look weird in a decimal numeration, it's binary form looks great: $11111111111111110000000000000000_2$.

## 7.3 DigitalNote emission

DigitalNote XDN has 2 sources of main emission:

1. Main source of DigitalNote XDN supply is a CPU-efficient ASIC-resistant Proof-of-Work mining with a constant base block reward = 150 XDN
2. Additional source of emission is DigitalNote XDN staking with an annual reward rate that may act as a Proof-of-activity element in future.

## 7.4 duckNote and DarkNote emission

Initial base block reward is 320000 XDN. Every 11000 blocks (approx. 1 month) it halves until reaching 150 XDN. It will occur in roughly one year after first block. That means that 80% of ever made coins will be available for free market use after just one year of fair Proof-of-Work mining.

After 132000 block, base block reward remains 150 coins until the max number of coin will be reached. It implies that the emission process will last about 77 years, supporting mining incentive and increasing money supply.

## 7.5 Block rewards

Every block reward is a round number: 320k, 160k, . . . , 150 notes. Round numbers are more convenient for human beings: they are easy to remember and easy to deal with. One can accurately predict his mathematical expectation of his mining revenue for arbitrary period of time and therefore his profits.

As a result, there is no dust (millicents) in the mining transaction, and this fact has two benefits:

- **Reducing the size** of blocks and transactions (and the whole blockchain).
- **Increasing privacy**, because dust is hard to use in ring signature (one needs to find outputs with the same amount), so you must spend it not anonymously.

## 7.6 "Spacious" blocks

All CryptoNote-based currencies has smart and neat mechanism of limiting the size of blocks, deterring transaction flood attack. If the current block is greater that median value of last

*N* blocks, it's reward is decreasing with exponential speed. The default CryptoNote "free block size" (maximum size of block which is not affected by the rule above) is 10 KB.

We increased this value up to 32 KB, which allows more transactions to fit into a block "for free".

## 8 Conclusion

In this whitepaper we have presented DigitalNote XDN as a tried and tested cryptocurrency. We have taken many of the good features from CryptoNote (untraceability, unlinkability, egalitarianism and multi-signatures) and added several unique blockchain features to DigitalNote XDN.

We believe DigitalNote XDN has the potential for mass adoption in the crypto economy with its unique and stable platform.

## References


[1] https://cryptonote.org

[2] http://en.wikipedia.org/wiki/Ring_signature

[3] http://en.wikipedia.org/wiki/Economic_liberalism

[4] https://github.com/bitcoin/bitcoin/pull/2738

[5] https://bitcointalk.org/index.php?topic=236742.0

[6] https://bitcointalk.org/index.php?topic=245938.0

[7] http://cr.yp.to/chacha.html

[8] http://bitcoin.stackexchange.com/questions/3718/what-are-multi-signature-transactions

[9] https://en.wikipedia.org/wiki/Perfect_number

[10] Iddo Bentov, Charles Lee, Alex Mizrahi, and Meni Rosenfeld, "Proof of Activity: Extending Bitcoin's Proof of Work via Proof of Stake", 2014, https://eprint.iacr.org/2014/452

[11] https://cryptonote.org/cns/cns008.txt