NANO

What is Nano?

- Nano is a trustless, low-latency cryptocurrency that utilizes a novel block-lattice architecture, where each account has its own blockchain and achieves consensus via delegated Proof of Stake voting.

- Offers feeless, instantaneous transactions, as well as unlimited scalability, making Nano ideal for peer-to-peer transactions.

- The network requires minimal resources, no high-power mining hardware, and can process high transaction throughput.

- To date, the network has processed over four million transactions with an unpruned ledger size of only 1.7GB.

- For a more in-depth look at Nano, please read our whitepaper

How does Nano work?

- Unlike conventional blockchains used in many other cryptocurrencies, Nano uses a block-lattice structure. Each account has its own blockchain (account-chain), equivalent to the account's transaction/balance history. Each account-chain can only be updated by the account's owner; this allows each account-chain to be updated immediately and asynchronously to the rest of the block-lattice, resulting in quick transactions. Since blocks can only be added by each account-chain's owner, transferring funds from one account to another requires two transactions: a send transaction deducting the amount from the sender's balance and a receive transaction adding the amount to the receiving account's balance. The receive transaction can be performed at any time; the recipient does not need to be online during the send transaction.

- Refer to sections three and four of the whitepaper for a more thorough look at how Nano works.

What are the advantages of Nano?

- Zero Fees
  Because the protocol is incredibly lightweight and running a node costs next to nothing, Nano transactions are processed with no fees. One transaction fits within a single UDP packet, and transactions are handled independently, eliminating any block size issue.

- Instantaneous Transaction Speed

Wallets pre-cache the anti-spam Proof of Work for the next transaction once a transaction is sent, making transactions instantaneous, as both sides have the proof of work ready to go. For ongoing transactions there may be delays, but this is intentional to prevent transaction spam.

- Scalability

  Transaction lookups scale with the logarithm of the data set size $\log_N O$ with a tree-like structure or O_1 if they are based on a hash table. To get an idea of how this scales, if it was a simple binary tree with 1,000 entries it would take 10 lookups. With 1,000,000 entries it takes 20 and 1 billion would take 30. Pruned nodes only need to keep the latest block of each account-chain, even further reducing lookup time and system resources.

Who is the team behind Nano?

- Developers
  - Colin LeMahieu- Core Wallet Developer, Creator of Nano
  - Mica Busch- Web & Mobile Developer
  - Sergsw/byte16 - Core Wallet Contributor
  - James Coxon - Services & Integration Developer
  - Zack Shapiro- iOS Mobile Developer
  - Chris Mair - Website Design & Branding Lead
  - Troy Reltzer - Public relations and communications.
  - Russel Waters - Core Code Contributor
  - Devin Torres - Core Wallet Contributor
  - Brian Pugh - Non-protocol Developer
  - Tito Vecchione - Media Deisgns

- Community Managers
  - Louis Nobleman - English, Spanish
  - Jesus Moreno - English, Spanish
  - Kedrin Welodon - English, Russian
  - Gotowerdown - English, Indonesian
  - Flomess - English, Italian
  - Jasper- English, Dutch

Can I mine Nano?

- Nano is non-mineable and has reached its maximum supply of 133,248,290 Nano. Funds were initially distributed via a captcha-faucet distribution system that ended in October 2017. Websites claiming to mine Nano are actually mining other cryptocurrencies, such as Monero, to trade for Nano on an exchange, and then paying out miners in Nano, leveraging Nano' feeless transactions.

Where is the Nano community located?

- Discord: chat.nano.org
- Reddit: /r/nanocurrency
- Twitter: @nanocurrency

Where can I find the Nano wallet?

- Nano currently supports both a desktop and online wallet, with plans to release a mobile wallet and light wallet in the near future.
- The desktop wallet can be downloaded from the Nano website, Nano.co
- Instructions on setting up the desktop wallet can be found on YouTube.
- An open source, online wallet is located at www.Nanowallet.com
- An integrated wallet within Telegram app is available here https://t.me/NanoWalletBot

What are Nano' Units?

- Currently the Nano ticker represents 1 million Nano (MNano), which is 10^30 raw, the smallest unit of Nano (equivalent to a satoshi in bitcoin)
- Nano' smallest unit is 1 raw, while 1 GNano is the largest. 1 Nano is 10^24 raw.
- Nano is the ticker used on exchanges/software to trade MNano.
- 1 Nano does not equal 1 Nano. 1 Nano currently equals 1MNano.
- Name dividers have been put in place to notate the factor of raw units in SI notation:

1 Raw						1 uNano	1 mNano	1 Nano	1 kNano	1 MNano	1 GNano
10^0	10^3	10^6	10^9	10^{12}	10^{15}	10^{18}	10^{21}	10^{24}	10^{27}	10^{30}	10^{33}

How does Nano achieve consensus?

- The voting process is balance-weighted. Every account selects a wallet address of a representative node. This is just a node that is configured to stay online and be ready to vote. When an account selects their representative, the vote weight of that account is increased by the balance of the source account.

- Votes are weighted by account balances. Those who have more funds in the system are inherently incentivized to keep the system honest; a dishonest system would make their investment worthless.
- Additional transactions don't contribute to securing the network; transactions settle individually within a few seconds regardless of other network activity. Because of this there's no reason to incentivize generating activity.

- A list of current representatives, sorted by voting power, can be found here. Any wallet, regardless of balance, can be a representative. A good representative is always online to vote.

Is Nano vulnerable to attacks?

- Nano, like all decentralized cryptocurrencies, may be attacked by malicious parties for attempted financial gain or system demise.

- In section five of the Whitepaper, we outline multiple attack scenarios, the consequences of such an attack, and Nano' protocol for dealing with each attack.

It's been a crazy past couple days leading up to the switch to Nano and the team couldn't be happier. There were a few minor things we missed and are still working to finalize but overall the day couldn't have gone any better.

Also, we are excited to be listed on OK Exchange tomorrow. Our team has been in contact with them for a number of weeks now and they decided to add us to coincide with the Nano rebrand. OK Exchange will be the largest volume exchange that Nano is listed on and is something we have been looking forward to.

Finally, there has been a ton of response to the meet and greet in Austin next week on February 8th. We originally figured 20 to 30 people would attend, however over 150 have signed up. Because of this we will have some additional Core team members present at the event to meet and mingle with all of you. More information will be released on this as we get closer to the event.

Once again I want to personally thank each and every one of you for your support and being such a wonderful community.

What are some of the long-term goals for Nano?

- To see the protocol itself set up as an internet standard that's infrequently touched and managed by a diverse group of people from different geopolitical areas and more specifically it's not controlled by

me or any small group of people. Any such group should not add configurable network parameters to avoid political issues like the block size debate.

- Add IPv6 multicast to transaction broadcasting: announcing a transaction to everyone in the world who wants it.

- Have existing payment-providers accept Nano much like they accept fiat currency today.

- To give the large group of people who do not have access to banks the assurance that payments they accept are secure at the point of exchange.

Additional Questions

- **Does the receiver account have to be online when I create my send transaction?**

    - No, whenever the send transaction goes out, the funds are "not pocketed" by the receiver. The funds are as good as the receivers and cannot be revoked by the sender. "Not pocketed" funds do NOT expire.

- **What are "not pocketed" funds?**

    - A transaction consists of a "send" and a "receive" transaction. During the period where a "send" doesn't have its partnering "receive" transaction, the funds are considered "not pocketed" by the recipient. "Not pocketed" funds are securely the receiver's funds. Once the receiver's wallet comes online, is fully synced, and unlocked, the funds will automatically be signed into their account chain.

- **What are the requirements to run a node?**

    - Currently the only real recommendation is to have a fast storage medium, such as an SSD instead of HDD. This is because currently the full node software does a lot of disk I/O for rapidly processing transactions. This may change with future full node versions that better utilize available system RAM and relax disk I/O.

- **Whats the incentive to run a node?**

    - The incentive to run a node is that it allows you to view and process transactions. A P2P currency will have many services utilizing the network and they obviously need payment data. Their only way around not running a node is pulling data from a possible remote node or creating a custom read-only node. The first requires trust which is likely not acceptable if you are using a cryptocurrency and the second makes very little sense as the additional cost to being a useful node is negligible. There is a self-serving interest for services that benefit from the network to ensure the maintenance of it.

- **How can I run a full node?**
    - The desktop wallet is already a full node! Just by running it you are helping.
- **Whats a representatives?**
    - Most transactions simply go through, but a malicious attacker may try and trick people on the network in an attempt to double spend. During these attacks, consensus must be achieve by voting. Voting requires a computer to be online; for many users this is impractical. Because of this, Nano allows you to assign a representative on your behalf. By default the desktop wallet selects one of the developers' representatives. These representative nodes are not special in any way compared to a normal full node; it's just that representative owners typically make a larger effort to keep their node online 24/7. The representative will vote on your behalf on which block it wants to keep in the block lattice for fork-inducing blocks.
- **Can I send funds to my wallet before it is synced?**
    - Yes. Funds can be sent to any "XRB_" address, even if they were created in an offline environment. Nano is exactly the same as ethereum or bitcoin in this sense. The funds will show up when the wallet is fully synced with the network.
- **How do I backup my wallet?**
    - Just write down your seed and keep it in a safe place. All accounts generated from that seed will be generated again (in order) when you restore that seed.
- **Can I reuse an address?**
    - Yes, unlike IOTA you can reuse addresses like in Bitcoin and Ethereum. Please understand the reasoning for this; IOTA does this because it is a drawback to the quantum-proof digital signature algorithm they use. Nano' current digital signature algorithm is not quantum proof, but the devs have expressed interest in changing to a quantum-proof algorithm as the field matures and quantum computers become a more significant threat to the network.
- **Can someone access my funds even if I use a password? (desktop wallet)**
    - Yes. The password feature of the desktop wallet just encrypts the seed locally on your computer. If anyone gets access to your plaintext (unencrypted seed, the thing we tell you to backup) they have access to your funds. The benefit of the password is that if someone has access to your computer, they don't immediately have access to your Nano.
- **What's a seed? What's a private key? Whats a public key?**
    - Any time you set up a Nano address (such as creating a new wallet) , you will be provided with a "Seed" which is 64 characters of text that is unique to your wallet. Do not store your seed online (e.g do not screenshot, email or save it in a file) because anyone with the seed can access all accounts on it and take all of your Nano! The reason why it is provided is so

that if for any reason you need to recover your account(s) you can do so without the original wallet you created the account on, so keep it safe! All private keys (which are used for signing transactions) are derived from your seed, and all public keys are derived from their partnering private key.