RaiBlocks FAQ

What is RaiBlocks?

- RaiBlocks 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 RaiBlocks ideal for peer-to-peer transactions.

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

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

How does RaiBlocks work?

- Unlike conventional blockchains used in many other cryptocurrencies, RaiBlocks 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 RaiBlocks works.

What are the advantages of RaiBlocks?

- ### Zero Fees
  Because the protocol is incredibly lightweight and running a node costs next to nothing, RaiBlocks 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 RaiBlocks?

- Developers
  - Colin LeMahieu- Core Wallet Developer, Creator of RaiBlocks
  - Mica Busch- Web & Mobile Developer
  - Sergsw/byte16 - Core Wallet Contributor
  - James Coxon - Services & Integration Developer
  - Zack Shapiro- iOS Mobile Developer

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

Can I mine RaiBlocks?

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

Where is the RaiBlocks community located?

- Discord: https://chat.raiblocks.net/
- Reddit: www.reddit.com/r/raiblocks
- Twitter: @raiblocks
- Forum: https://forum.raiblocks.net/

Where is RaiBlocks traded?

- RaiBlocks is currently traded on three exchanges under the ticker symbol $XRB

- Mercatox.com
- Bitgrail.com
- BitFlip

➢ The development team is actively working to add RaiBlocks to additional exchanges, with the goal of Raiblocks ultimately trading on every major exchange. Unfortunately, the RaiBlocks team is not permitted to discuss potential listings on additional exchanges until RaiBlocks is officially listed. The RaiBlocks team will announce each new exchange listing as soon as they are available.

Where can I find the RaiBlocks wallet?

➢ RaiBlocks currently supports both a desktop and online wallet, with plans to release a mobile wallet and light wallet in the near future.

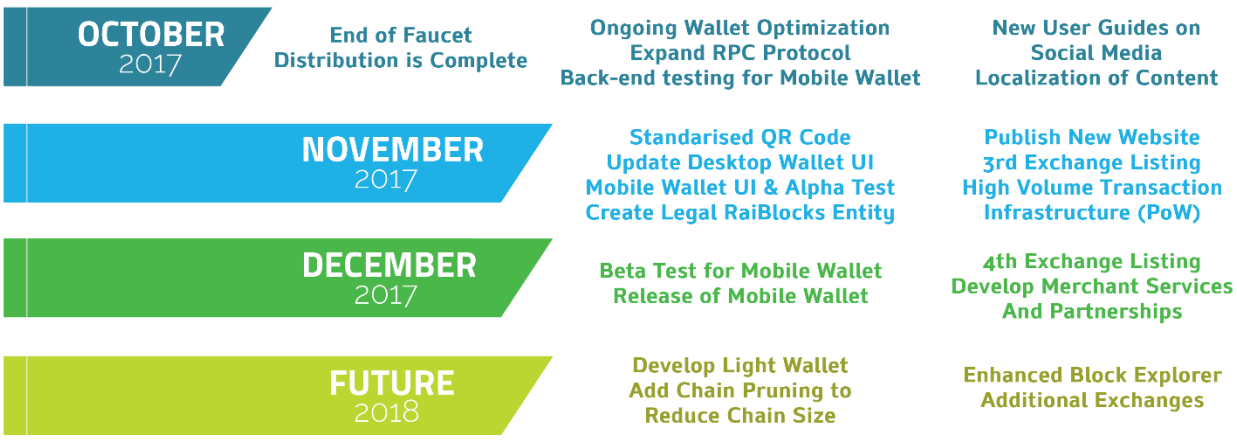
➢ The desktop wallet can be downloaded from the RaiBlocks website, https://raiblocks.net/.

➢ Instructions on setting up the desktop wallet can be found on YouTube.

➢ An open source, online wallet is located at www.raiwallet.com

➢ An integrated wallet within Telegram app is available here https://t.me/RaiWalletBot

What upcoming milestones does RaiBlocks hope to achieve?



What are RaiBlocks' Units?

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

1 Raw						1 uxrb	1 mxrb	1 xrb	1 kxrb	1 Mxrb	1 Gxrb
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 RaiBlocks 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 RaiBlocks vulnerable to attacks?

- RaiBlocks, 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 RaiBlocks' protocol for dealing with each attack.

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

- 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 XRB 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.

How does RaiBlocks compare to other cryptocurrencies?

- **Differences between Bitcoin and RaiBlocks**

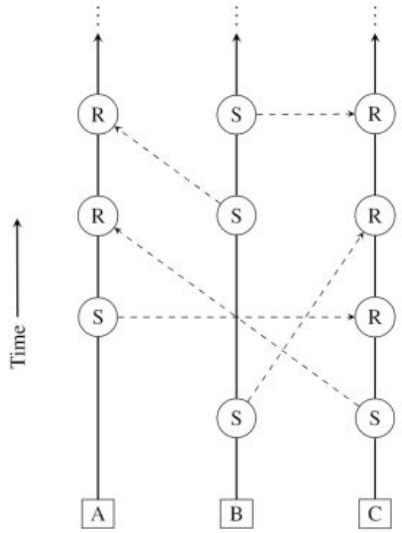
    - Bitcoin organizes transactions into blocks with an average processing time of 10 minutes per block. For a transaction to go through, it must be included in a block, and that block must be mined. To be safe, transactions are usually not considered complete until a few additional blocks are added to the blockchain. Because of this, Bitcoin transactions typically process on the order of hours. With RaiBlocks, each individual transaction is a block, and each block is able to be processed instantly by the network. The limit to the speed of the transactions is primarily network-bound; transactions are processed as fast as they can be propagated throughout the RaiBlocks network.

    - Bitcoin's security is derived from hundreds of terawatts of computing power computing hashes. In order to perform malicious actions, such as a double spend, on the Bitcoin blockchain, an attacker would have to accrue at least half of the network's computation power, which is both financially and practically infeasible.
      RaiBlocks secures its ledger via delegated proof of stake (dPoS). In order to perform malicious actions on the RaiBlocks block-lattice, an attacker would have to posses >50% of the online voting power. Such an attack would spoil their large financial investment, and as such is not an attractive option. The dPoS of RaiBlocks consumes minimal energy, allowing full-nodes to run on inexpensive, low-power hardware.

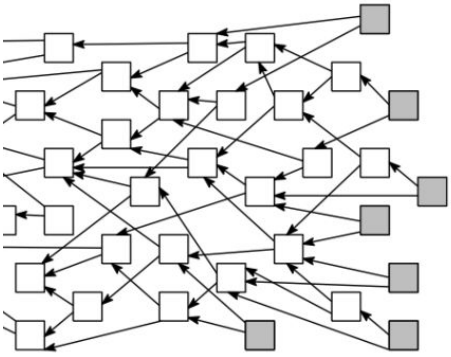
- **Differences between IOTA and RaiBlocks**

    - IOTA's consensus is decided by Proof of Work (PoW) stacking of consecutive transactions, while RaiBlocks' is achieved by voting on conflicting transactions. PoW stacking requires maximizing the continuous network hash rate which is an expense that is inherently paid in electricity by users of the network. Because RaiBlocks doesn't rely on high network PoW to maintain security, the operating cost of RaiBlocks nodes and RaiBlocks users are much lower.

- While IOTA's Tangle and RaiBlocks' block-lattice are both DAG data-structures, offering instantaneous and feeless transactions, the way they operate are significantly different. With IOTA, two "tip" transaction must first be discovered via a probabilistic algorithm, such as a Monte Carlo Random Walk; a good tip is a recent transaction and expands the tangle in a "forward" moving direction. The idea is that if everyone uses similar tip selection algorithms, recent valid transactions will be approved by newer, valid transactions. Once a transaction is sufficiently deep in the Tangle, it is considered confirmed. RaiBlocks' block-lattice is an organized structure that doesn't require "tip" discovery. The last block on each account-chain is easily found/cached, and account transactions can only be appended, like a conventional blockchain. For typical transactions, this transaction is instantaneous and doesn't require any additional blocks for a transaction to be considered confirmed.



Visualization of RaiBlocks' block-lattice. Every transfer of funds requires a send block (S) and a receive block (R), each signed by their account-chain's owner (A, B, C)



IOTA's Tangle and its typical tip sets (shaded). Each transaction approves two previous transactions. Once a transaction is sufficiently deep, it is considered confirmed.

- IOTA's vision is machine-to-machine communication, commerce, data storage and to become the premier protocol of IoT devices. RaiBlocks' focus is on reliable, quick peer-to-peer payments and rapid exchange transfers for arbitrage.

➢ **Differences between Ethereum and RaiBlocks**

- Ethereum is an alternative or separate technology from RaiBlocks. The entire concept of programs executing on top of the Ethereum Virtual Machine is something RaiBlocks doesn't attempt to replicate. The part we focus on is an efficient transfer of value i.e. purely a currency, so while Ethereum requires miners and electricity input which is paid for by devaluing the currency, RaiBlocks has no fees and no devaluing while operating.