What is Randao?

Quanta

The **Random Number Generator** (RNG) is a core part of any lottery system. Creating a secure and unpredictable RNG on the Ethereum blockchain was one of the lagest technical challenges for the Quanta project.

As a result of our research, the Quanta project selected a Randao algorithm as the RNG method for the Quanta lottery. The Randao algorithm is a decentralized and immutable RNG algorithm that operates on the Ethereum blockchain.

A complete Randao process consists of two rounds - a '**Commit**' round and a '**Reveal**' round. A certain number of participants are required for each round. Players are required to submit a deposit before the first round begins. After both the commit and reveal rounds have been completed, each player who participated in both will receive an attractive incentive. Any players who participated in the first commit round, but not the second reveal round will forfeit his or her Randao deposit.

1

1st Round -Commit

Participants who wish to take part in Randao must place a deposit while doing first round (Commit). Appropriate funds will be required in the Quanta Game Wallet to be used for the deposit.

The partcipant must generate a random number within the alotted time and commmit that encrypted number. After Randao deposit and the encrypted number are sent, the partcipant is now committed to Randao participation.

2

2nd Round - Reveal

Once the required number of encrypted random numbers have been commited,

each participant's Quanta Game Wallet will automatically reveal the random number when the 2nd Round starts. Once Randao has completed, participants will receive their Randao honorarium and have their Randao deposit returned.

*Note: Participants will need to remain online until the Reveal process has completed, or risk losing their Randao deposit

What do I need to participate in Randao?

Quanta

Randao Wallet

Quanta Game Wallet is a wallet which supports Ethereum (ETH) for players to play Randao and Lottery.

Quanta Game Wallet is available for download at:

https://www.myquanta.im/randao

*Note: ETH address from Quanta Game Wallet will be required for your Quanta ID registration.

+

Quanta ID

Following information requried to register Quanta ID:

- Username
- Email
- Password
- First name
- Last name
- Date of birth (must be over 18)
- Residential address
- ETH address (Quanta Game Wallet) - Color scan of passport
- Photo of individual holding passport
- Proof of residential address

*Note: May take more than 24hrs to process account registration.

1. Quanta Game Wallet

To participate in Randao, participants should install the Quanta Game Wallet. Quanta Game Wallet is available at:
https://www.quanta.im

1.1 Install Randao Wallet

Follow the Quanta Game Wallet application installation guide for help.

1.2 Create new ETH address or restore existing ETH address on Randao Wallet

The ETH address on Quanta Game Wallet will be required when registering a Quanta ID account. Create a new ETH address, or restore an ETH address from an existing ETH wallet by utilizing a 12-word passphrase.

1.3 Ensure that your Randao Wallet has funds, and set your send password

If you have restored the wallet from an existing ETH address, you may already have fund available in your wallet. If a new ETH address has been generated, ensure that you have fund sent to your new Quanta Game Wallet, as a deposit is required to participate in Randao. Also set a send password to protect your Quanta Game Wallet, from unauthorized sending of your funds.

2. Quanta ID

To participate in Randao, participants must register for a Quanta ID account and also have their Quanta ID details verified by Quanta (Quanta verified account KYC3). Registration for Quanta ID can be performed at:

https://kyc.quanta.im/signup

2.1 Create Quanta ID account

If you do not have a Quanta ID account, select Register to create an account. The following information is required:

- **Display Name:** Name you can use like an ID, must be unique.
- **Email:** must be unique
- **Password:** Will act as your login password.

Select Create Account to submit your information. You will receive an email to verify your email address. Note that the email verification / account activation link will expire after 24 hours.

2.2 Activate account (verify your email)

Open your email inbox, open email from Quanta, and select the "**activation link**" to complete the process of creating your account. You will be taken back to Quanta website. Select "**I'm ready to register**" and complete the following formsto register your Quanta ID.

2.3 Quanta ID - Email verified account (KYC level 1)

The following information is required to complete your email verified account:

- First name
- Last name
- Date of birth (participants must be 18 years old or older)
- Residential address
- ETH address (must be a valid ETH address and same ETH address Randao wallet [1.2])

Submit your information. Once successful, you will arrive at a screen with the button "**I'm Ready to Play**" and "**I want to claim all my winnings**". Select "**I want to claim all my winnings**" and continue on with registration.

2.4 Quanta ID - Quanta verified account (KYC level 3)

Provide the following 3 images (must be legible):

- Color scan of your passport ID page (information from above much match passport)
- Photo of yourself holding passport, with passport ID page open
- Proof of residency (acceptable documentation including: bank statement, credit card statement or utility bill. Documentation must be in English. Physical address must match above registration info)

2.5 Confirmation email

Processing your Quanta verified account (KYC level 3) may take more than 24 hours.Once your registration has been accepted and verified by Quanta, you will receive a confirmation email. Once you receive this email, you are now qualified and verified to participate in Randao.

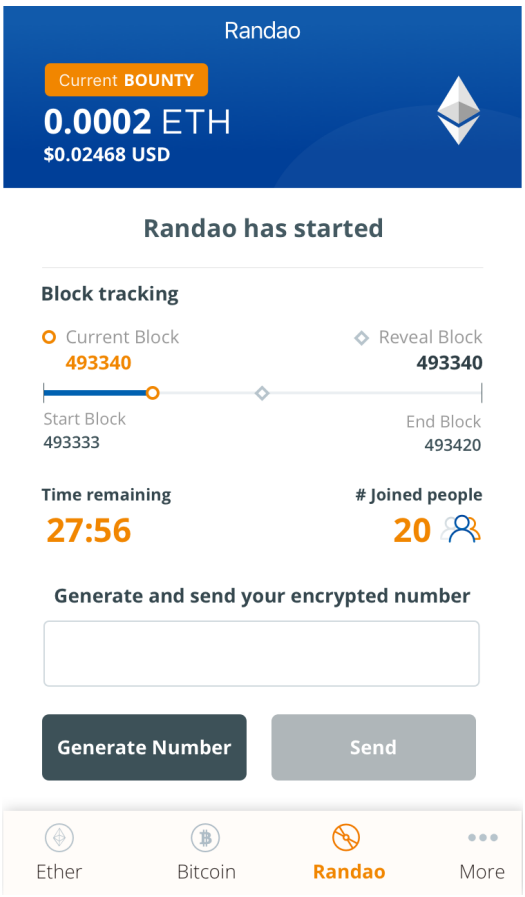
3. Commit Round

Once you have your Quanta verified account (KYC level 3), you are now ready to participate in Randao.

The first round of Randao is the Commit round. Randao will normally commence XXXXXX after ticket sales for the Quanta lottery have closed. In this commit round, participants will need to submit an encrypted random number with a deposit.

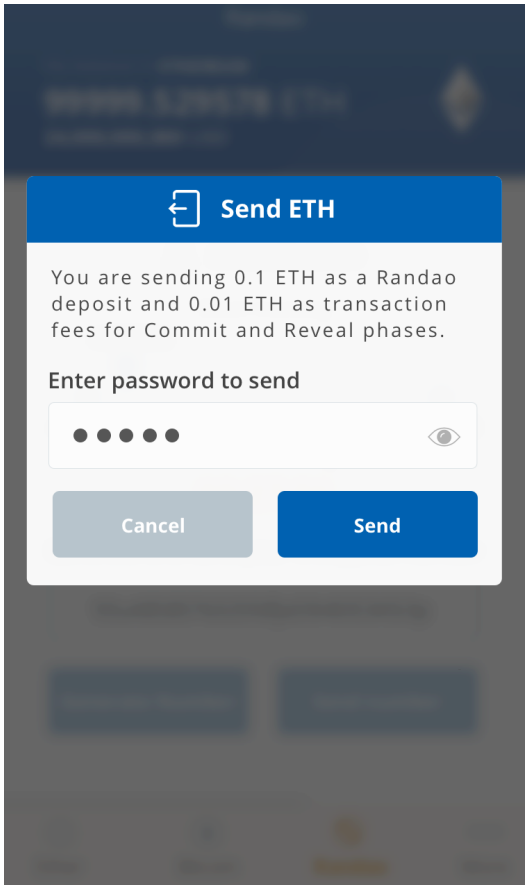
3.1 Generate random number

Launch Quanta Game Wallet to participate. If a Randao session is currently operating and in the Commit round, you will have the opportunity join. A "**Generate Number**" button will be available, and by selecting this, a random number will be generated.



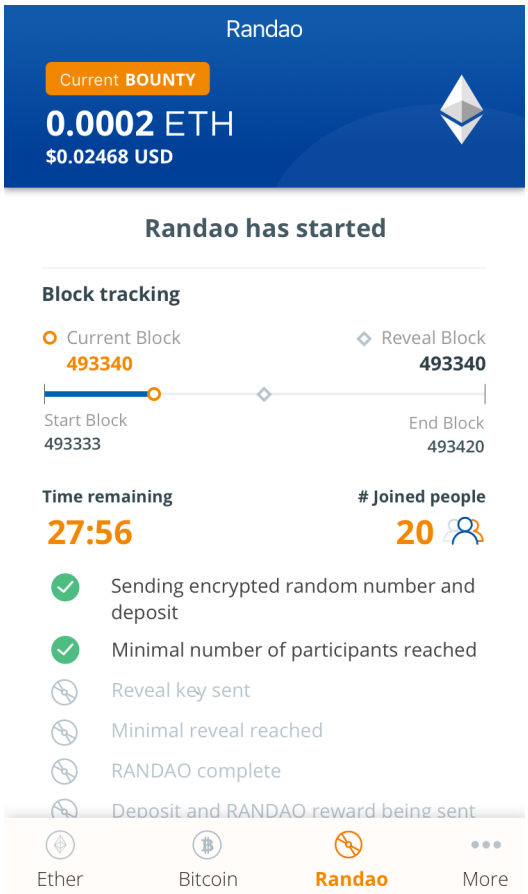
3.2 Commit your number

Before the Commit round ends, select “Send Number” to send/commit your encrypted randomly generated number. At the same time, a deposit payment will be required. Enter your wallet password, and your deposit payment will be sent along with your encrypted randomly generated number.



3.2 Commit your number

After a successful commitment, you will arrive at the following screen. Note that you will need to remain online and keep the Quanta Game Wallet open until you have successfully completed the reveal round, or risk losing your deposit



4. Reveal Round

The next round of Randao is the Reveal round. To move on to the Reveal round, a minimum number of participants is required in the Commit round. The **start block** begins the Commit round, and as long as the required minimum number of participants is reached within the Commit phase, the Reveal round can commence.

Participants can confirm the **Current block**, **Start block** and **End block** from their Quanta Game Wallet. If there are not enough participants, participants will have their deposits returned, and Randao will start again. If the Commit round finishes successfully, the Reveal round will begin. Participants will need to remain online and keep Randao operating. Quanta Game Wallet support participants doing the Reveal Round by sending random number (which was generated in the previous round) to Randao System. Note: participants need to keep the application open to make sure Reveal round be successful.

5. Player Incentive

All players that have successfully completed both rounds of Randao (Commit and Reveal) are eligible for an incentive regardless of whether Randao succeeds or not. This incentive will vary, based on the number of participants and the state of Randao. The Quanta-held bounty will be divided equally to participants upon Randao's successful completion.

5.1 Randao not successful

Any dishonorable player who fails to submit their unencrypted random number (loses internet connection, quits application, etc) will lose their deposit. This lost deposit amount will be divided and sent to other players with who have successfully completed their Randao commit and reveal rounds.

5.1 Randao not successful

Any dishonorable player who fails to submit their unencrypted random number (loses internet connection, quits application, etc) will lose their deposit. This lost deposit amount will be divided and sent to other players with who have successfully completed their Randao commit and reveal rounds.

5.2 Randao successful

All players will receive an incentive, where the amount of the incentive is based on the amount of the bounty + deposit of dishonorable players, divided equally by the number of honorable players, along with their initial deposit.

$$\text{Financial Incentive} = \frac{\text{Bounty + Deposit of dishonorable players}}{\text{Number of honorable players}}$$

5.3 Deposit returned with Incentive

Your deposit and incentives will be automatically sent to you. You can observe the transaction in your Quanta Game Wallet.