

Criminal Investigations and Network Analysis (CINA): A DHS Center of Excellence

Cryptocurrency Wallet Seizure Guide

Prepared For: CINA
Prepared By: Hexordia



HEXORDIA

Table of Contents

Table of Contents.....	2
Description.....	3
iOS Cryptocurrency Wallets.....	4
Phantom.....	4
Uniswap.....	5
SafePal.....	7
Exodus.....	9
MetaMask.....	11
Bither.....	13
Coinbase.....	16
Coincola.....	19
eToro.....	21
Guarda.....	23
MoonPay.....	25
Rainbow.....	28
Android Cryptocurrency Wallets.....	31
Unstoppable.....	31
Coinbase.....	33
Zengo.....	36
eToro.....	40
Guarda.....	44
Phantom.....	48
MoonPay.....	52
Rainbow.....	57
MetaMask.....	60
OKX.....	64
Gemini.....	68
Exodus.....	73

Acknowledgment: This material is based upon work supported by the U.S. Department of Homeland Security under Grant Award Number 17STCIN00001-08-00.

Disclaimer: The views and conclusions contained in this document are those of the authors and should not be interpreted as necessarily representing the official policies, either expressed or implied, of the U.S. Department of Homeland Security.

Description

This report provides a guide on seizing cryptocurrency wallets from select mobile devices, using a step-by-step approach illustrated with screenshots. The focus is on documenting the procedures required to send and secure wallet information on iOS and Android devices, ensuring maximum seizure of cryptocurrency assets.

Definition of Seizing Cryptocurrency: Seizing cryptocurrency, in the context of this report, refers to the act of withdrawing all or the maximum possible funds from a suspect's wallet to a law enforcement agency (LEA) -owned wallet. This process is carried out to ensure that the digital assets are securely transferred and preserved as evidence.

By following this guide, investigators will be equipped with the practical knowledge and visual reference needed to successfully seize cryptocurrency wallets, making this a valuable resource for digital forensic professionals handling cryptocurrency-related cases.

Important Note: This report assumes that the LEA involved has an agency-controlled wallet already set up to receive the funds. This could be either a hardware or software wallet that is ready to receive the funds upon seizure of the wallets. It's important to have multiple cryptocurrency addresses set up (ie BitCoin, Ethereum, etc) as it is often unknown what type of cryptocurrency is being used.

iOS	Android
Phantom	Unstoppable
Uniswap	Coinbase
SafePal	Zengo
Exodus	eToro
MetaMask	Guarda
Bither/Bitpie	Phantom
Coinbase	MoonPay
Coin Cola	Rainbow
eToro	MetaMask
Guarda	OKX
MoonPay	Exodus
Rainbow	Gemini

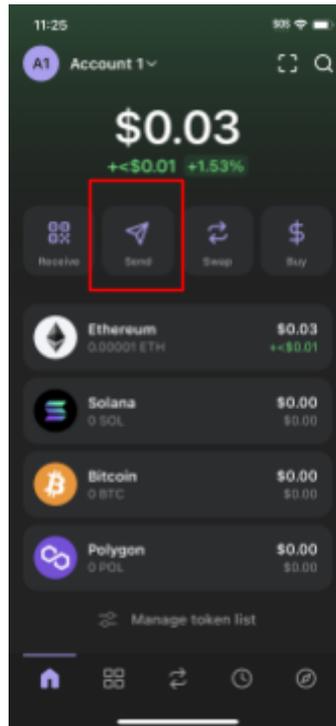
Assumption: This guide assumes that the mobile phone has been seized and the suspect is logged into their cryptocurrency wallet app.

iOS Cryptocurrency Wallets

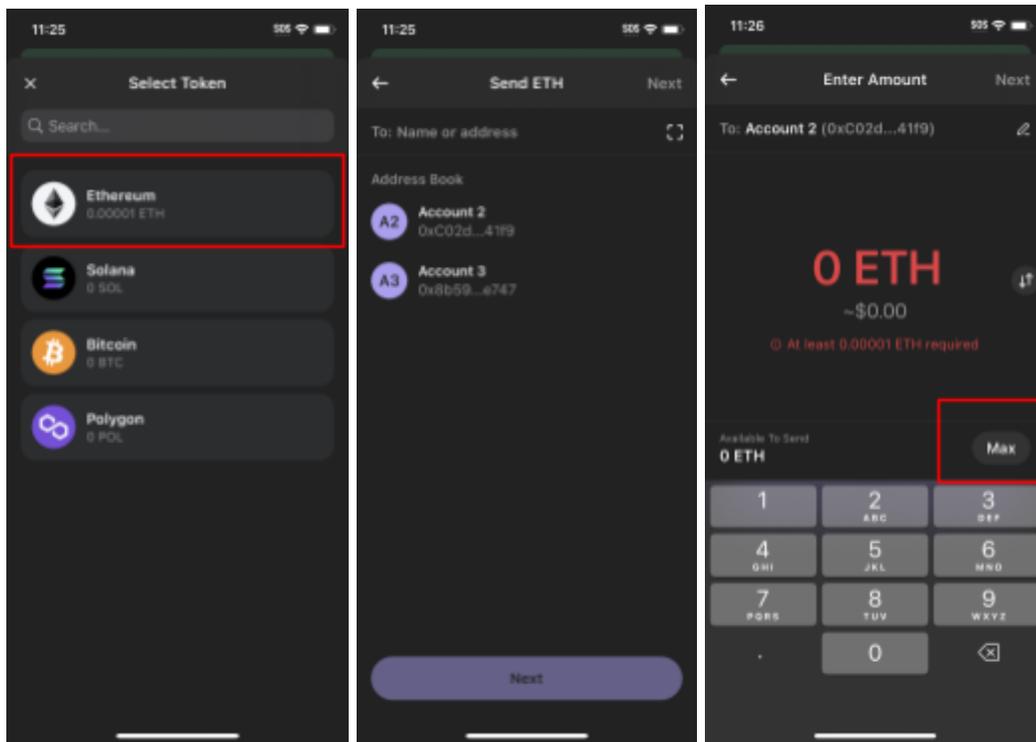
Phantom

To perform a seizure of the wallet the suspect must be signed in to their wallet.

1. Select the “Send” button which is the middle left button with the paper airplane icon.

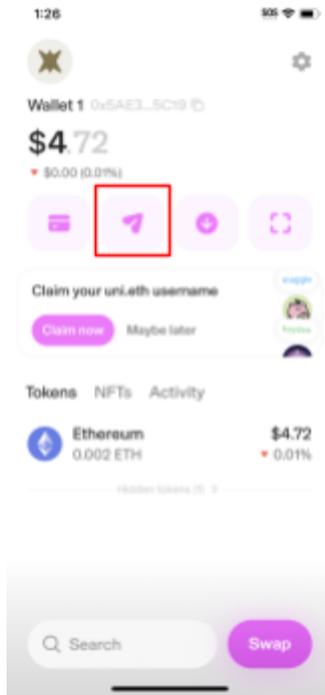


2. After selecting “Send” you will be prompted to select a token in our case we select “Ethereum”. Insert the address to send the funds to. This field needs to be filled with a wallet owned by your organization. After doing so press “Next”. The next screen will allow you to choose the amount of cryptocurrency to send for simplicity press “MAX”. The next screen will display the amount being sent including fees. Finally press “Send”, now the transaction is pushed to the blockchain for confirmation.

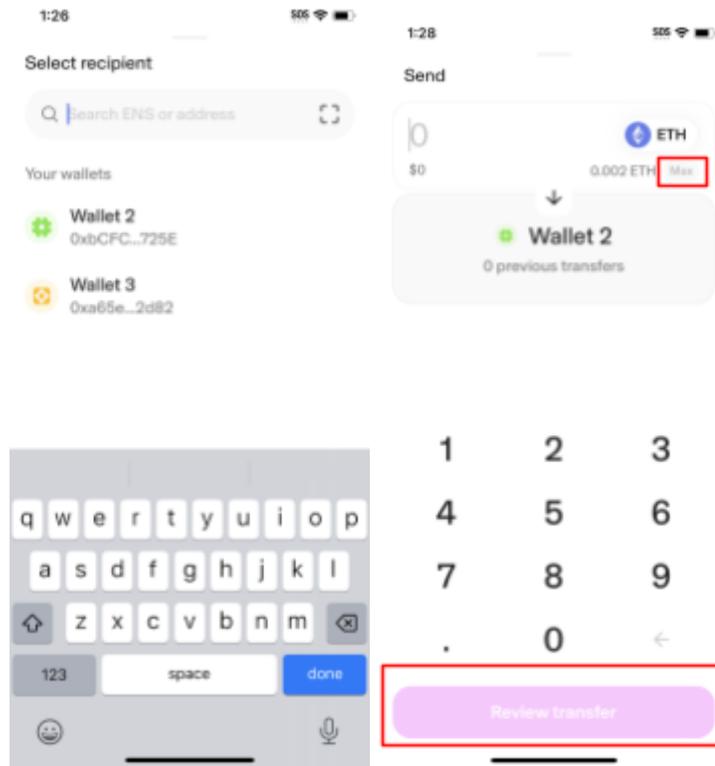


Uniswap

1. On the home screen select the middle left button with the paper airplane icon, this is the send button.



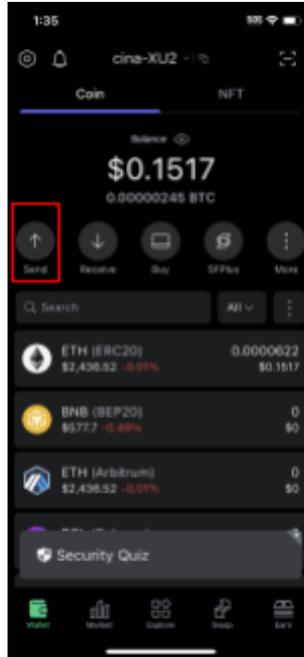
2. To seize the funds it requires a wallet preferably a brand new wallet that was created by your organization for the purpose of receiving the cryptocurrency to be seized.
3. After selecting “Send” you will be prompted to enter a wallet address. The next screen you can select the currency you'd like to use and press the “Max” button to use all funds on this wallet. On the bottom of the screen select “Review Transfer”



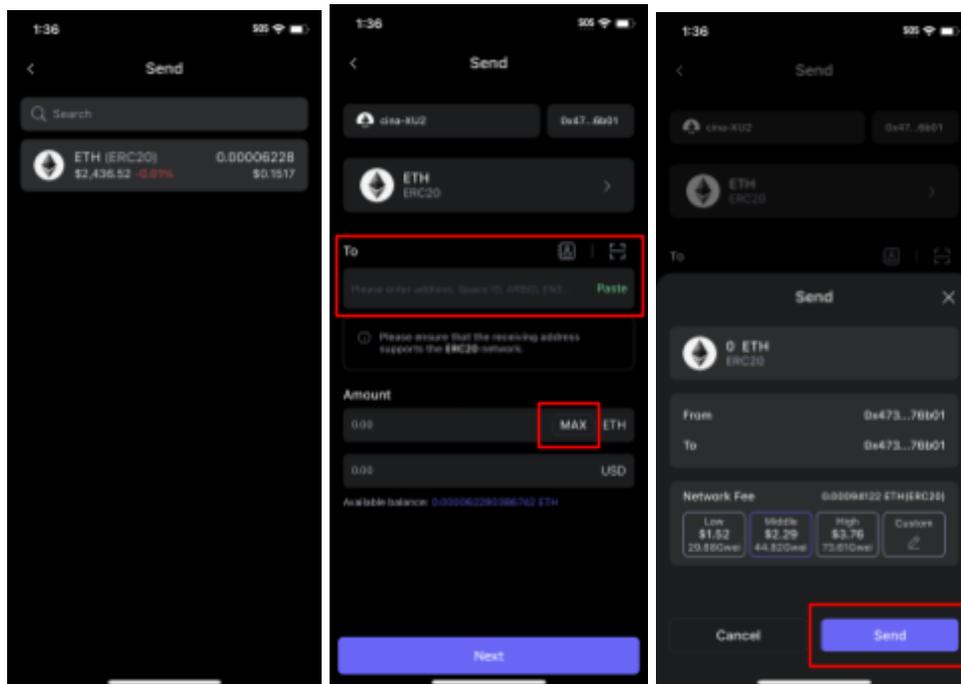
SafePal

Download the SafePal wallet from the app store and open the app, follow the steps below.

1. On the home screen select the “Send” button with the up arrow icon.



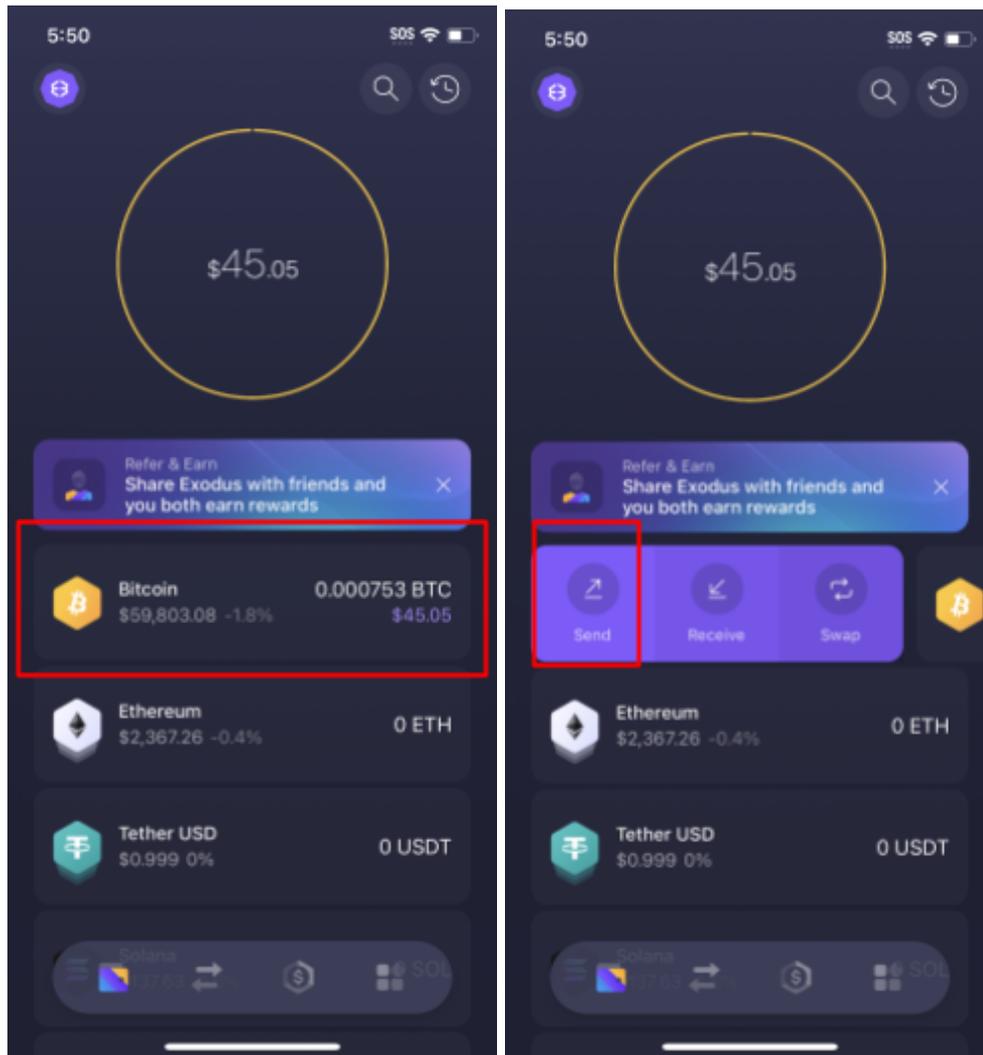
2. To seize the funds it requires a wallet preferably a brand new wallet that was created by your organization for the purpose of receiving the cryptocurrency to be seized.
3. After selecting “Send” you will be prompted to select the wallet you are sending from. The next page you will enter the wallet address and press the “MAX” button, then hit the “Next” button on the bottom of the screen. It will then ask you to review it as well the fees associated with it, press the “Send” button and it will begin the transfer.



Exodus

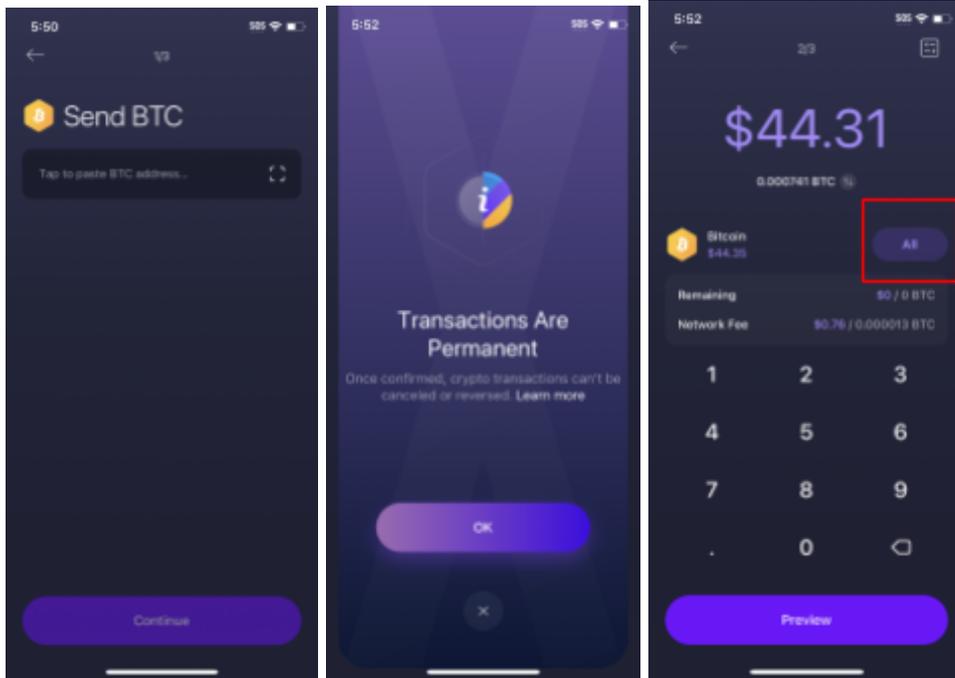
Download the Exodus wallet from the app store and open the app, follow the steps below.

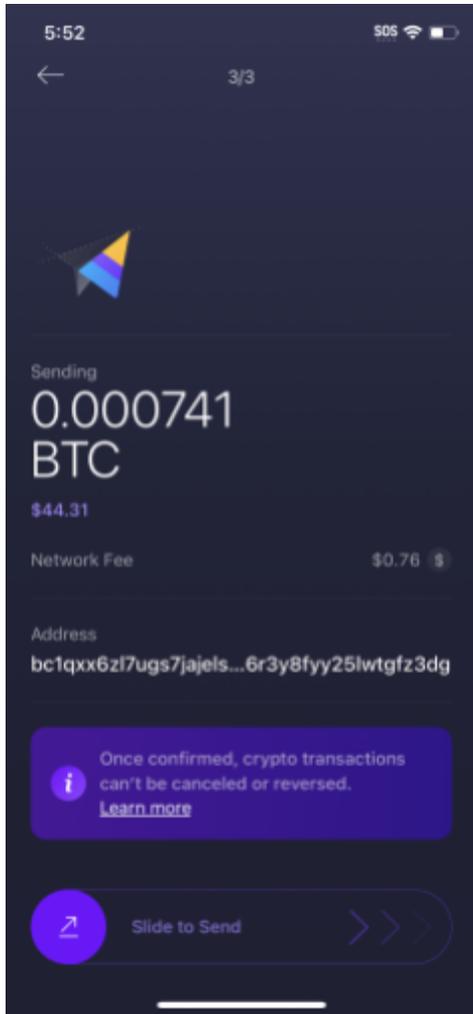
1. On the home screen slide the wallet you want to the right, select “Send”.



2. To seize the funds it requires a wallet preferably a brand new wallet that was created by your organization for the purpose of receiving the cryptocurrency to be seized.
3. After selecting “Send” you will be prompted to insert the address to send the funds to. This field needs to be filled with a wallet owned by your organization. After doing so press “Continue”. A pop up will occur telling you that all transactions are permanent select “Ok”. The next screen will allow you to choose the amount of cryptocurrency to send for simplicity, press “All” and then “Preview”. The next screen will display the amount being sent including fees. Finally slide the arrow icon at the bottom to the left,

now the transaction is pushed to the blockchain for confirmation.



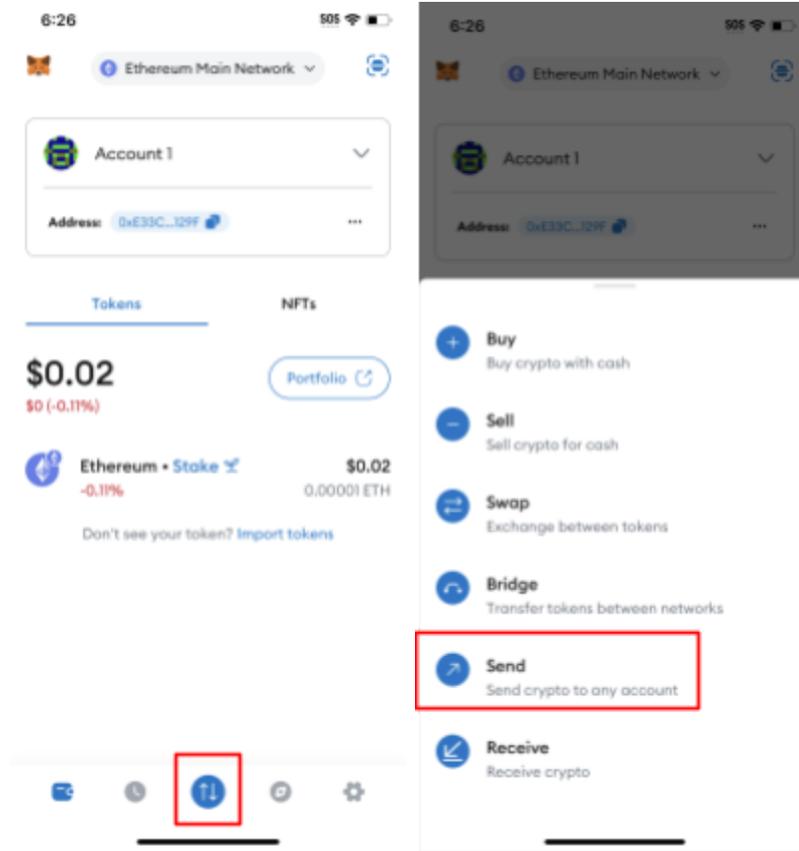


4.

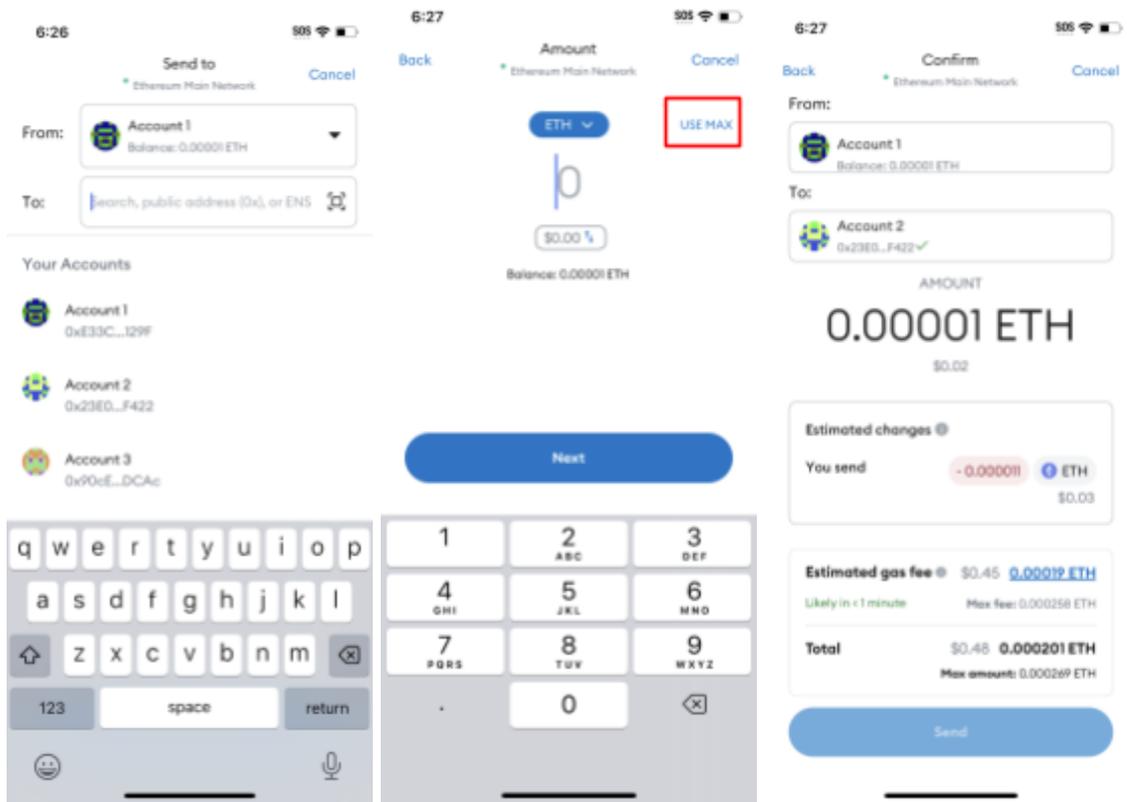
MetaMask

Download the Metamask wallet from the app store and open the app, follow the steps below.

1. On the home page click the middle button at the bottom of Metamask which will open a window with a few options. Choose “Send”.



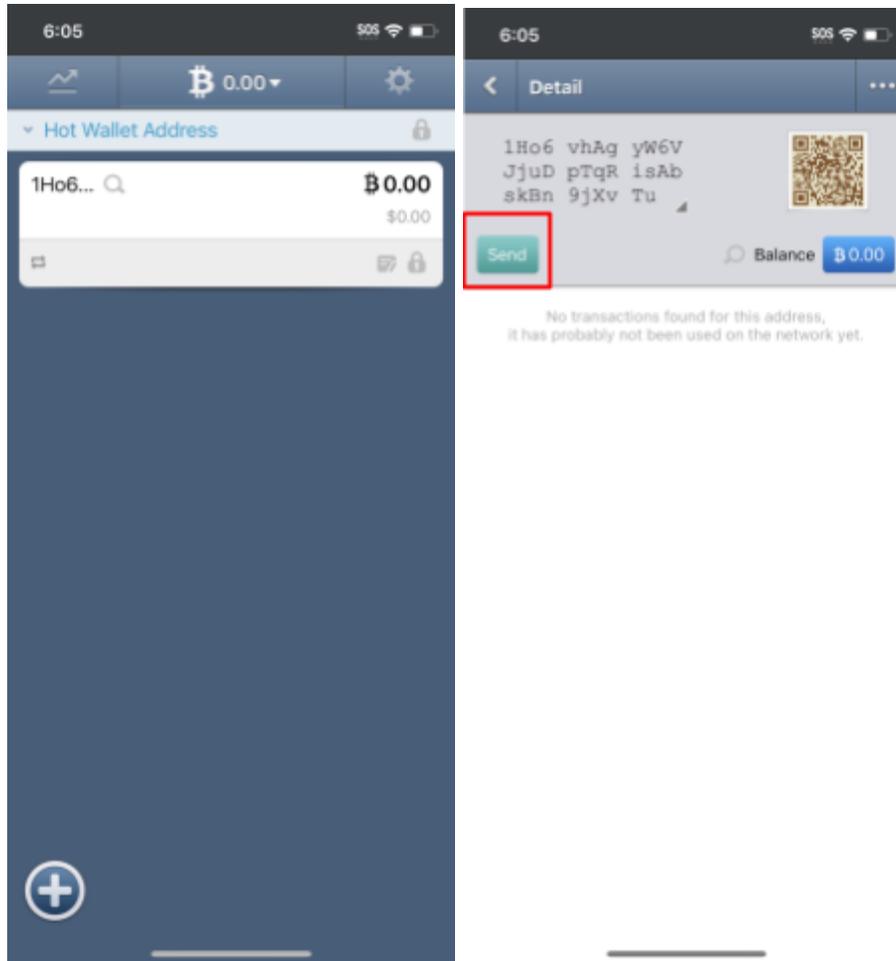
2. To seize the funds it requires a wallet preferably a brand new wallet that was created by your organization for the purpose of receiving the cryptocurrency to be seized.
3. After selecting “Send” you will be prompted to insert the address to send the funds to. This field needs to be filled with a wallet owned by your organization. After doing so press “Continue”. The next screen will allow you to choose the amount of cryptocurrency to send for simplicity press “USE MAX”. The next screen will display the amount being sent including fees. Finally press “Send”, now the transaction is pushed to the blockchain for confirmation.



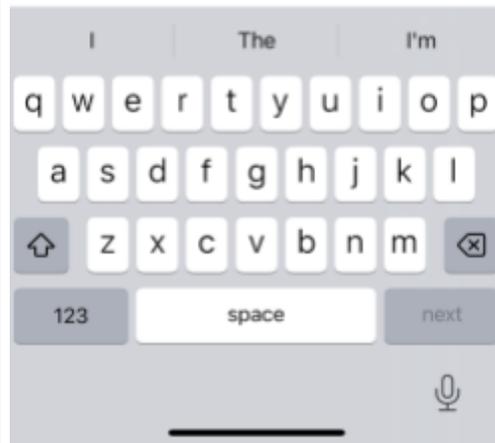
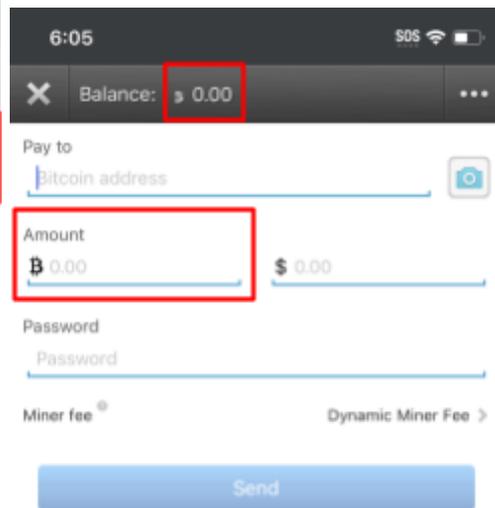
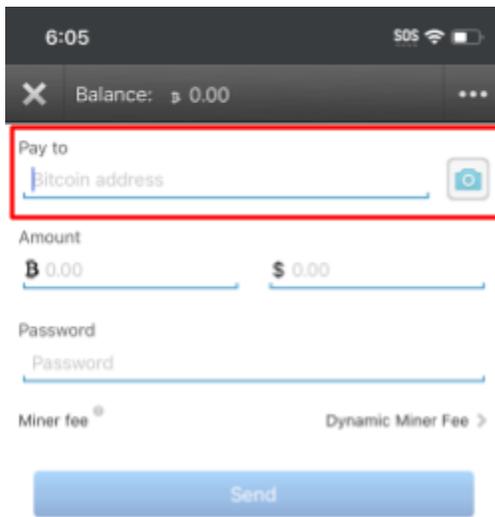
Bither

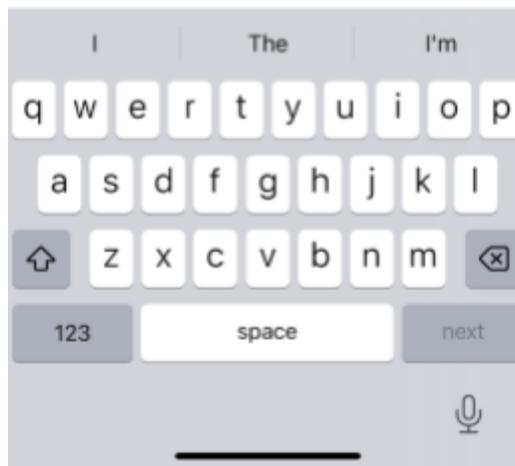
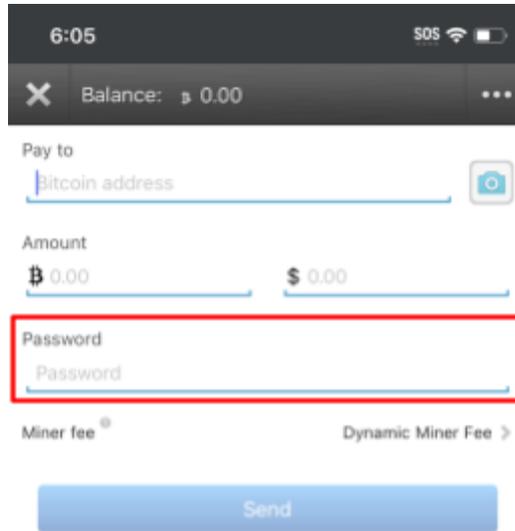
Download the Bither wallet from the app store and open the app, follow the steps below.

1. On the home screen click on the wallet you want to seize. On the next page click the "Send" button.



2. To seize the funds it requires a wallet preferably a brand new wallet that was created by your organization for the purpose of receiving the cryptocurrency to be seized.
3. After selecting “Send” the next page will contain all the next steps. First type in the wallet address you are sending the funds too. Next using the balance given enter that into the “Amount” box as there is no max option. Finally enter the password for the application and press “Send”.

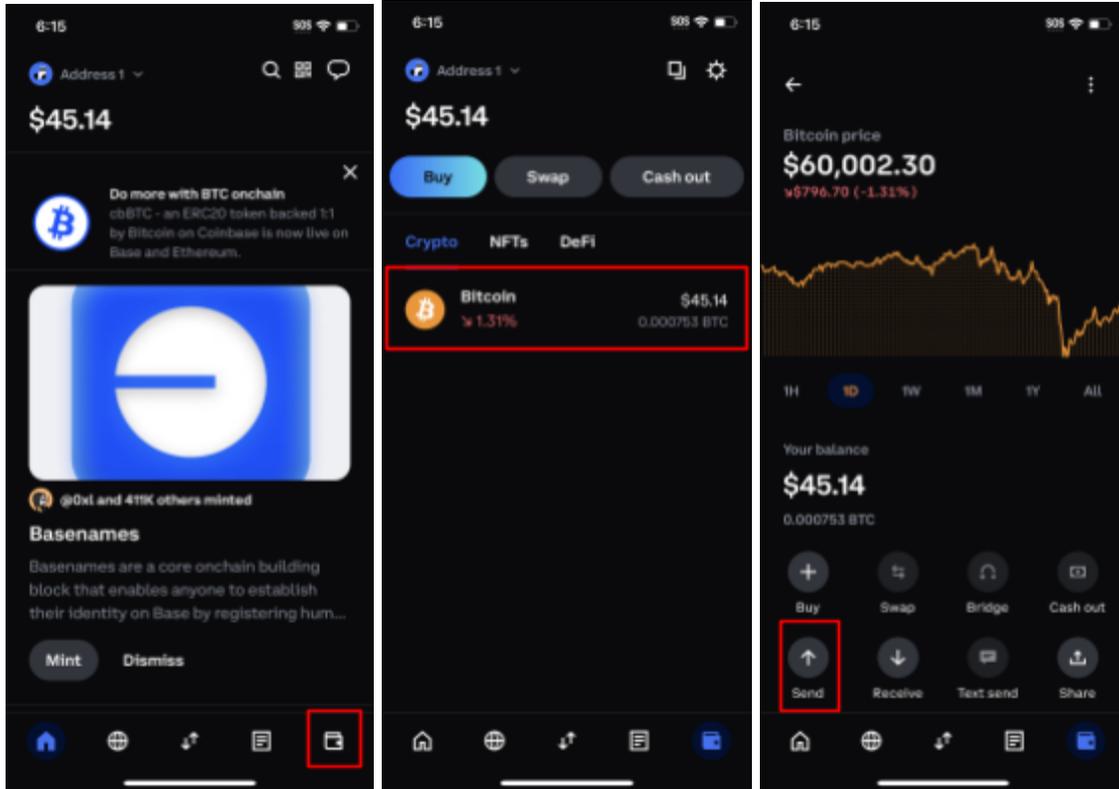




Coinbase

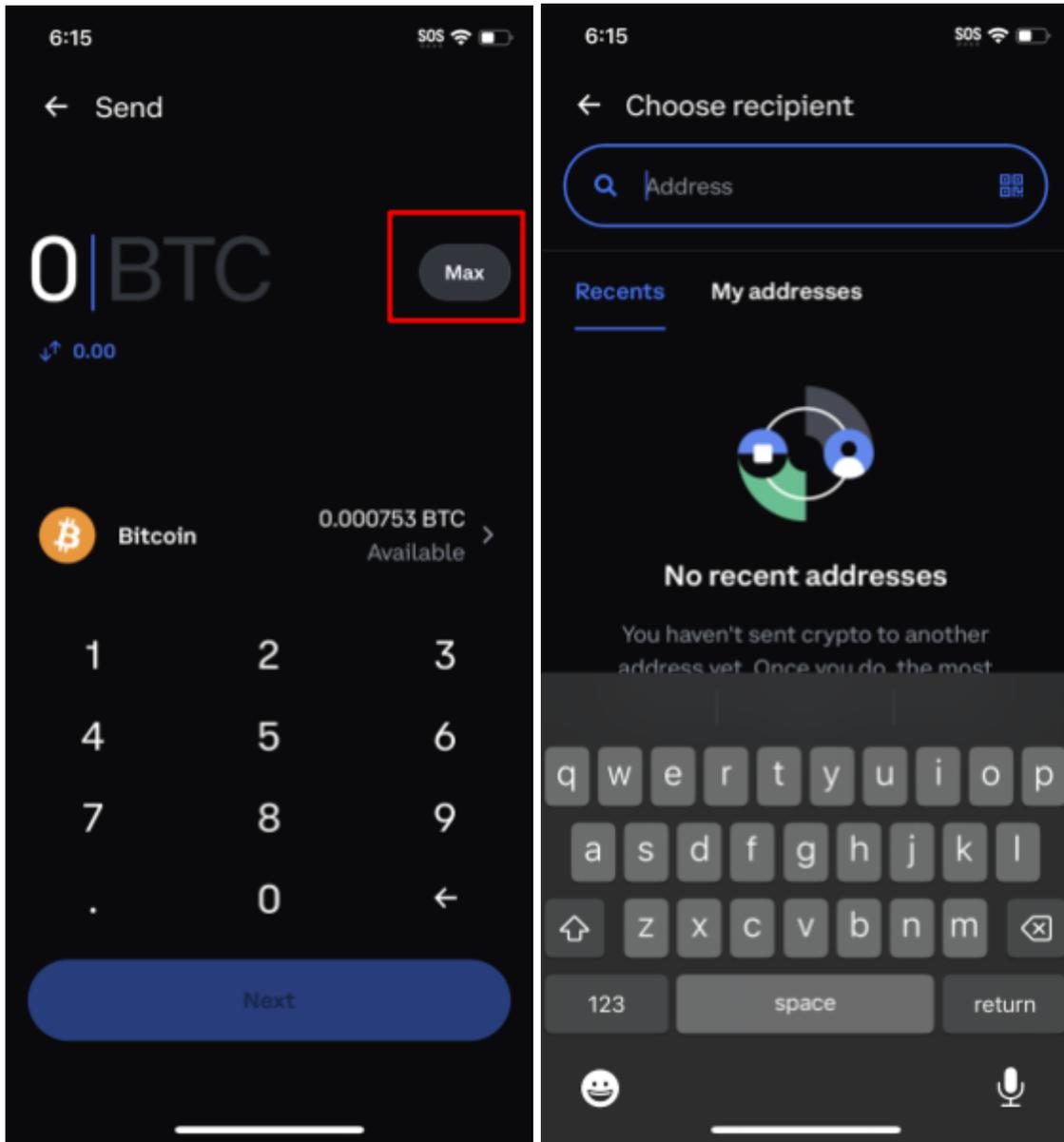
Download the Coinbase wallet from the app store and open the app, follow the steps below.

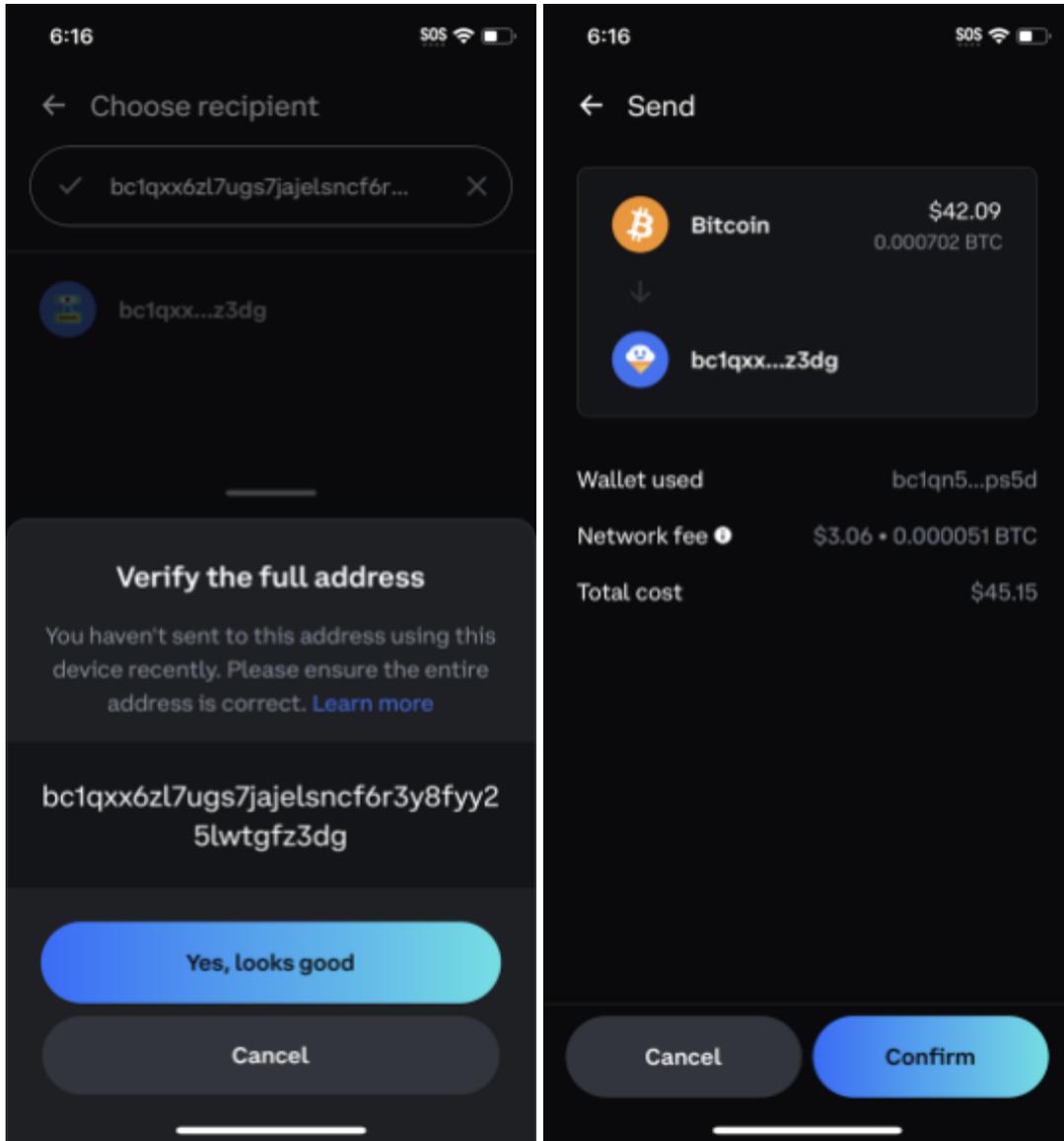
1. On the home page select the wallet icon on the bottom left of the page. Then press on the funds you'd like to use. Finally select the "Send" button on the lower right side of the page, you may need to scroll down to see it.



2. To seize the funds it requires a wallet preferably a brand new wallet that was created by your organization for the purpose of receiving the cryptocurrency to be seized.
3. After selecting “Send” you can enter the amount of funds you want to send, we will select the “Max” button. Next enter the wallet address you are sending to. It may ask to you to verify the wallet address, if it is correct select the “Yes, looks good” button. Finally you can review all the information and select “Confirm” to complete the

transaction.

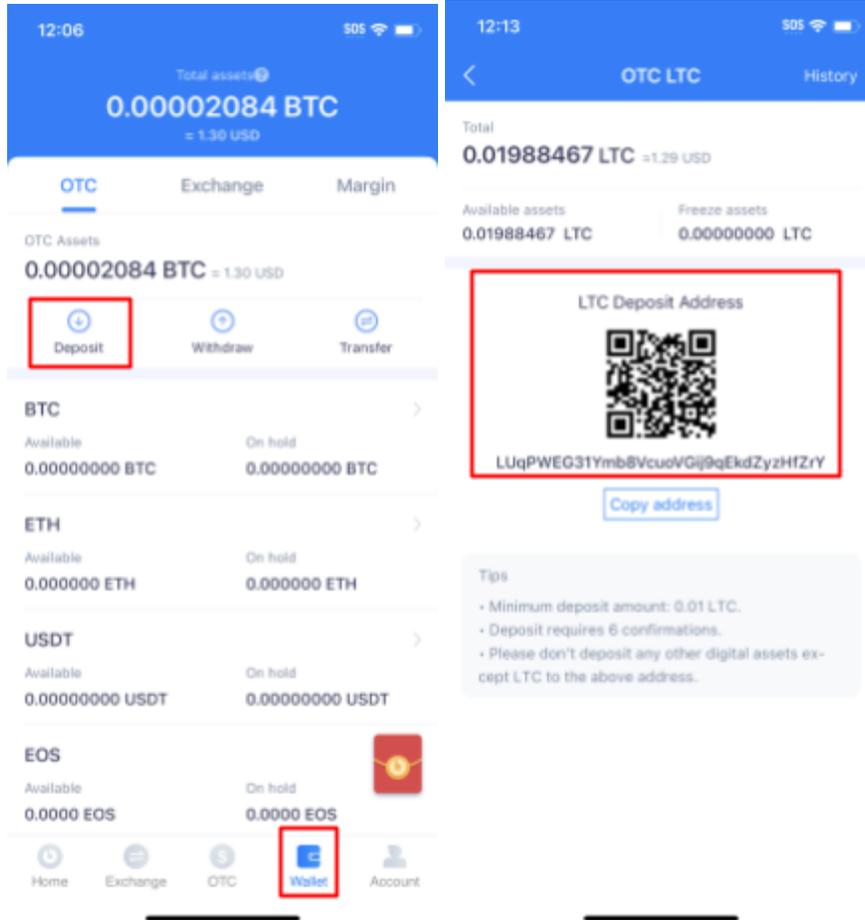




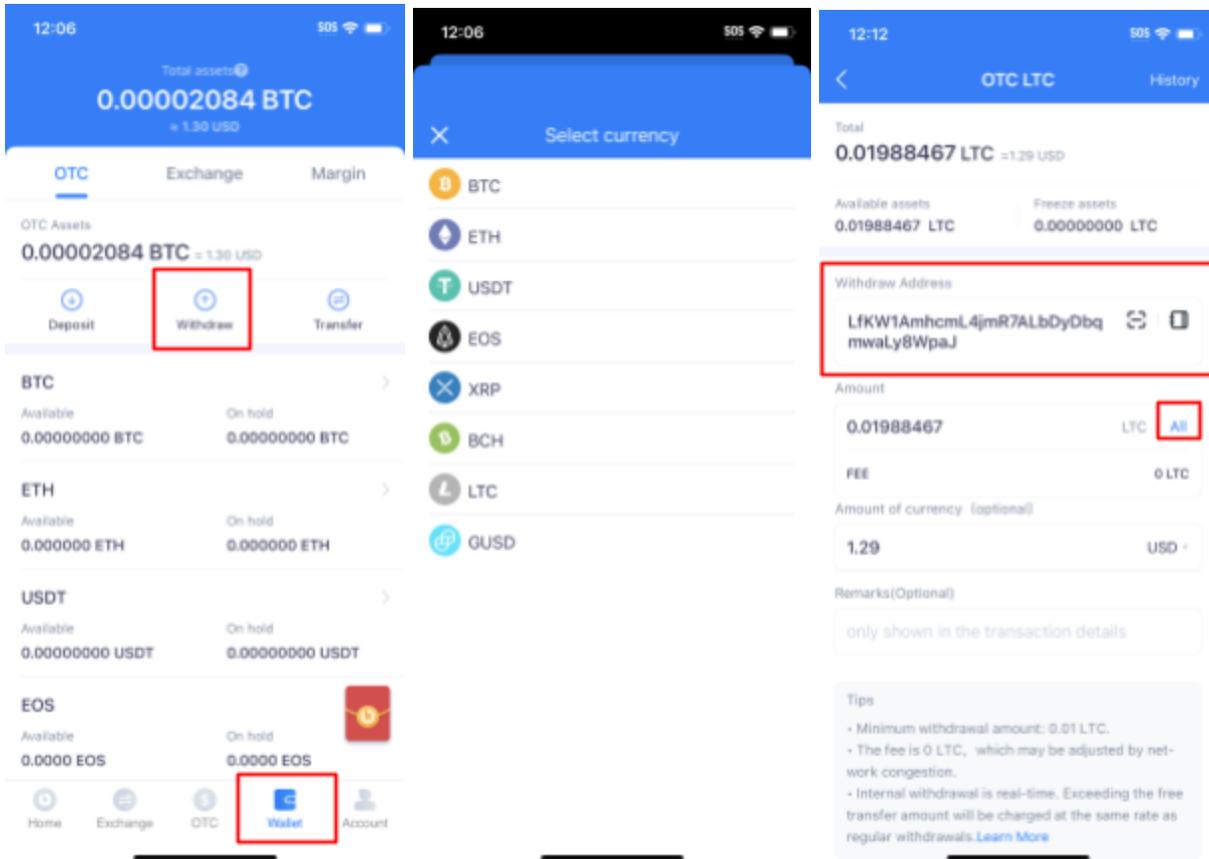
Coincola

Download the Coin Cola wallet from the app store and open the app, follow the steps below.

1. In the wallet screen of Coin Cola first hit "Deposit". On the deposit screen either take note of the wallet address or save the QR code.



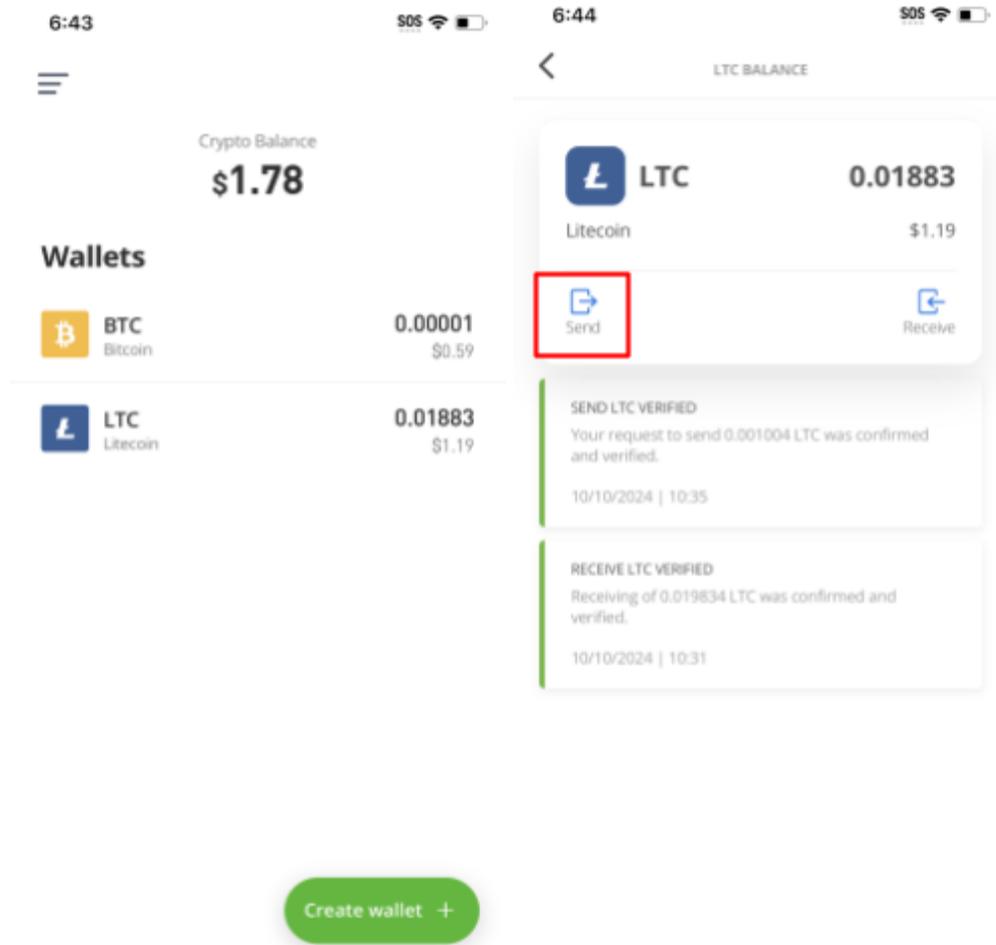
2. To seize the funds it requires a wallet preferably a brand new wallet that was created by your organization for the purpose of receiving the cryptocurrency to be seized.
3. Now on another device that is signed in to the wallet collecting the seizures go to the wallet screen and select the “Withdraw” button. The next page will be selecting the currency, because we have funds in LTC we will select that option. Finally on the last page we will enter the address we noted in the first step and select “All”. At the bottom of the page you will select “Withdraw”



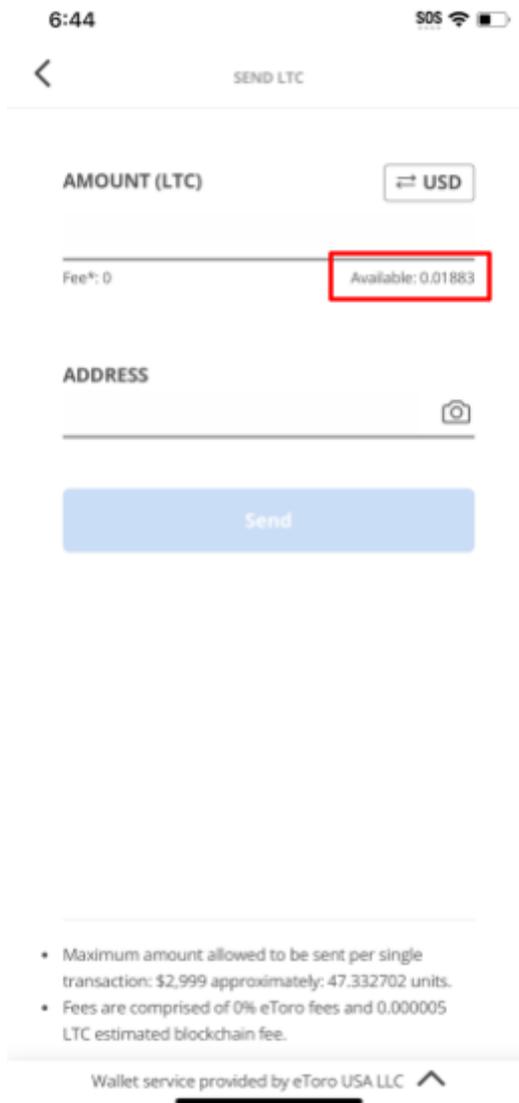
eToro

Download the eToro wallet from the app store and open the app, follow the steps below.

1. On the home screen select the funds you want to send, in our case we selected LTC. On the next page select the “Send” button.



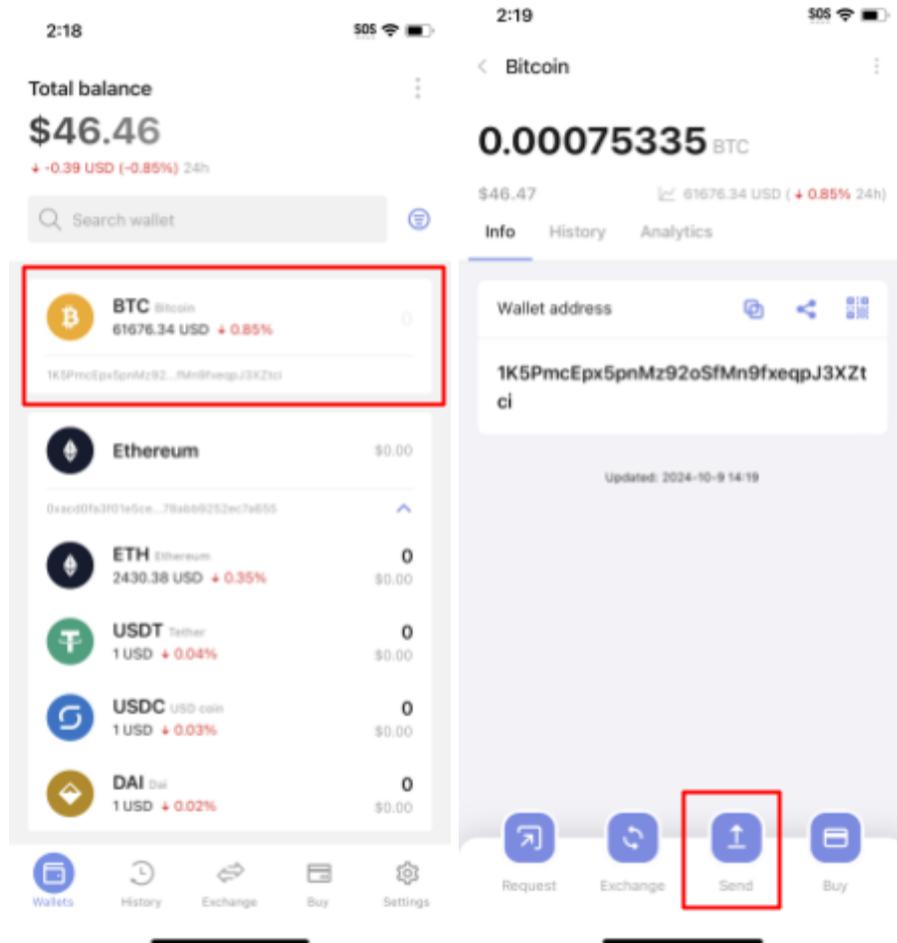
2. To seize the funds it requires a wallet preferably a brand new wallet that was created by your organization for the purpose of receiving the cryptocurrency to be seized.
3. After selecting “Send” the next page will contain all the final steps. Enter the amount to send, there is no max button but the available funds are below the line. Next enter the wallet address you want to send the funds to. Finally press the “Send” button.



Guarda

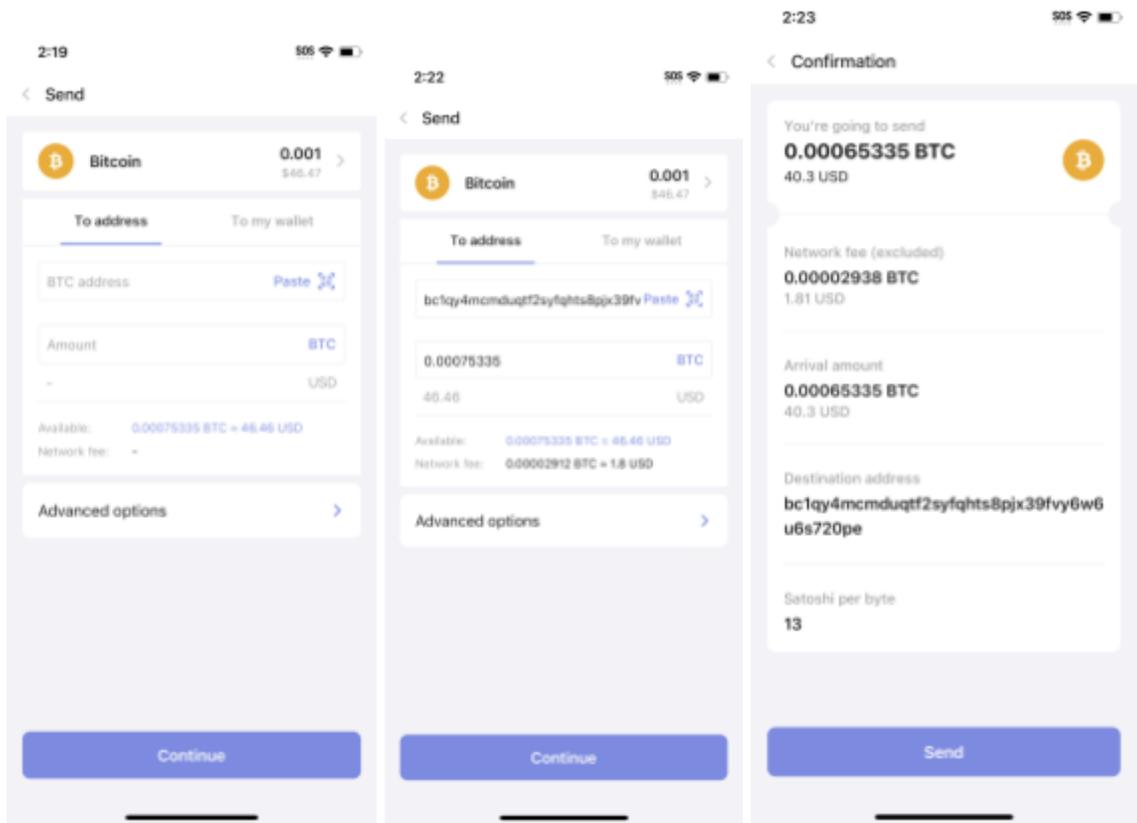
Download the Guarda wallet from the app store and open the app, follow the steps below.

1. On the home screen select the wallet you want to send from. In our case we will select BTC. On the next screen select the “Send” button on the bottom of the page.



2. To seize the funds it requires a wallet preferably a brand new wallet that was created by your organization for the purpose of receiving the cryptocurrency to be seized.
3. After selecting “Send” you will be prompted to enter in the wallet address. There is no max option on Guarda so enter in the total amount available, make to enter in the 0 before the decimal point, then press “Continue”. On the last page you can review all the

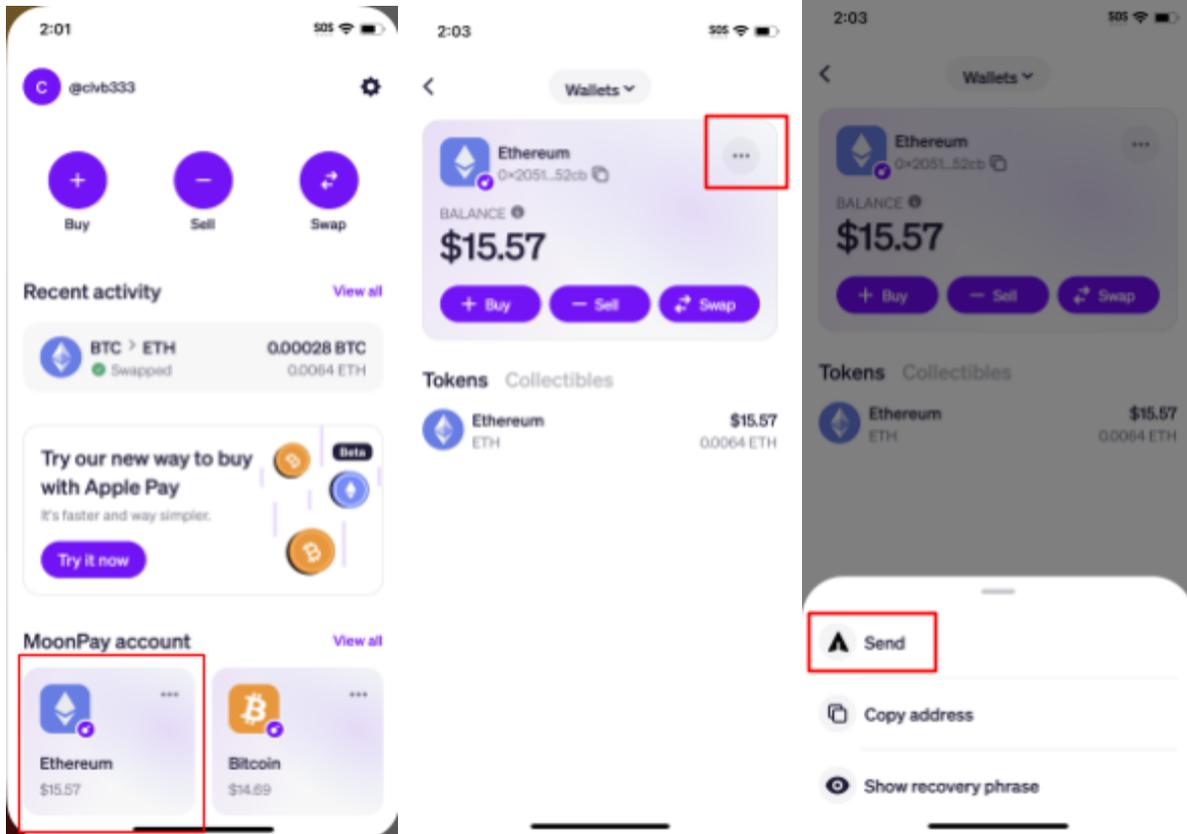
information and select “Send” to begin the transfer.



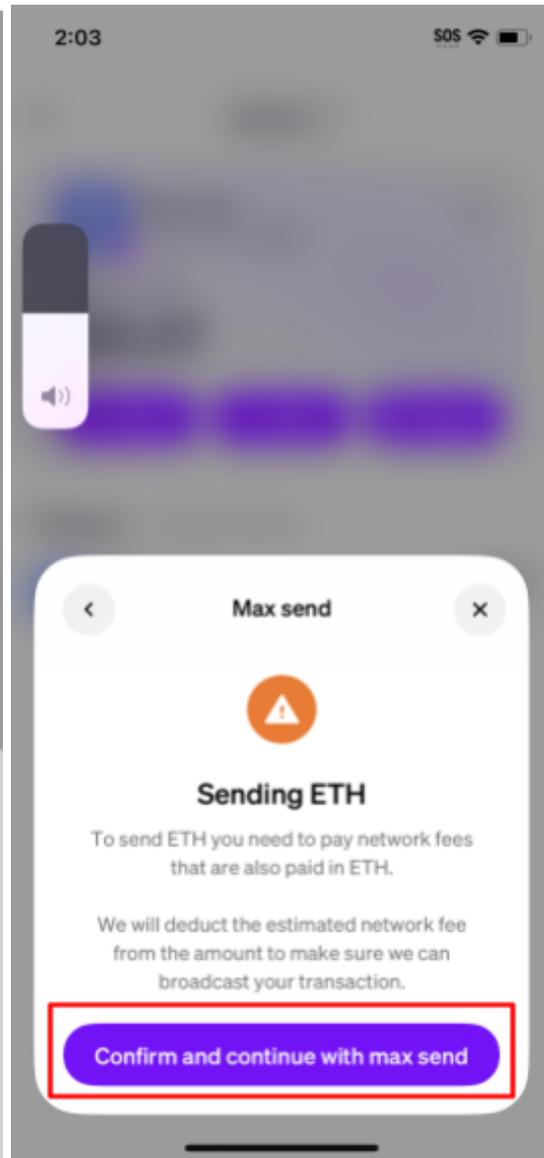
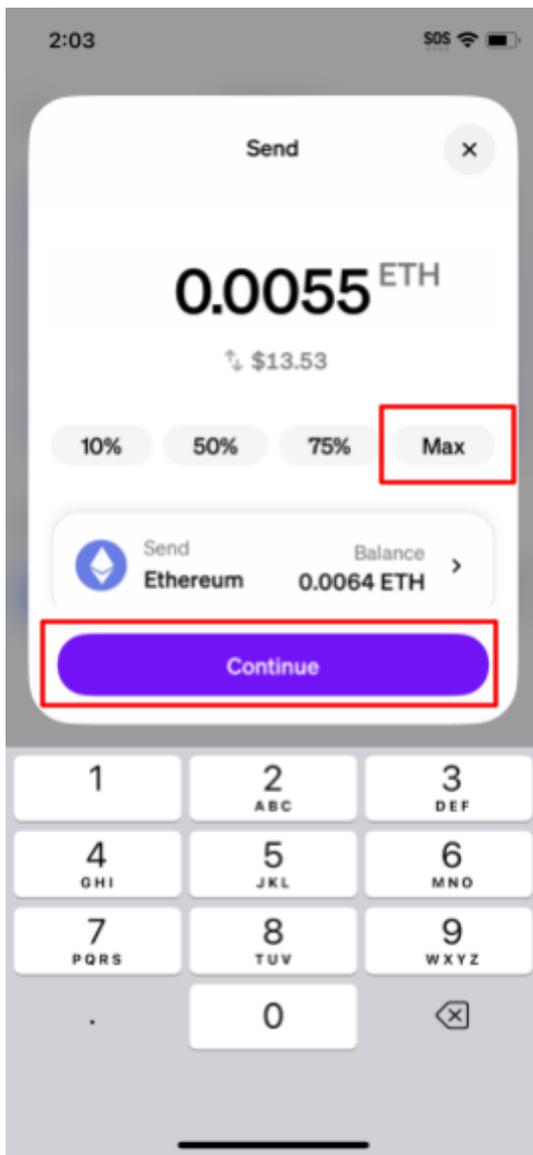
MoonPay

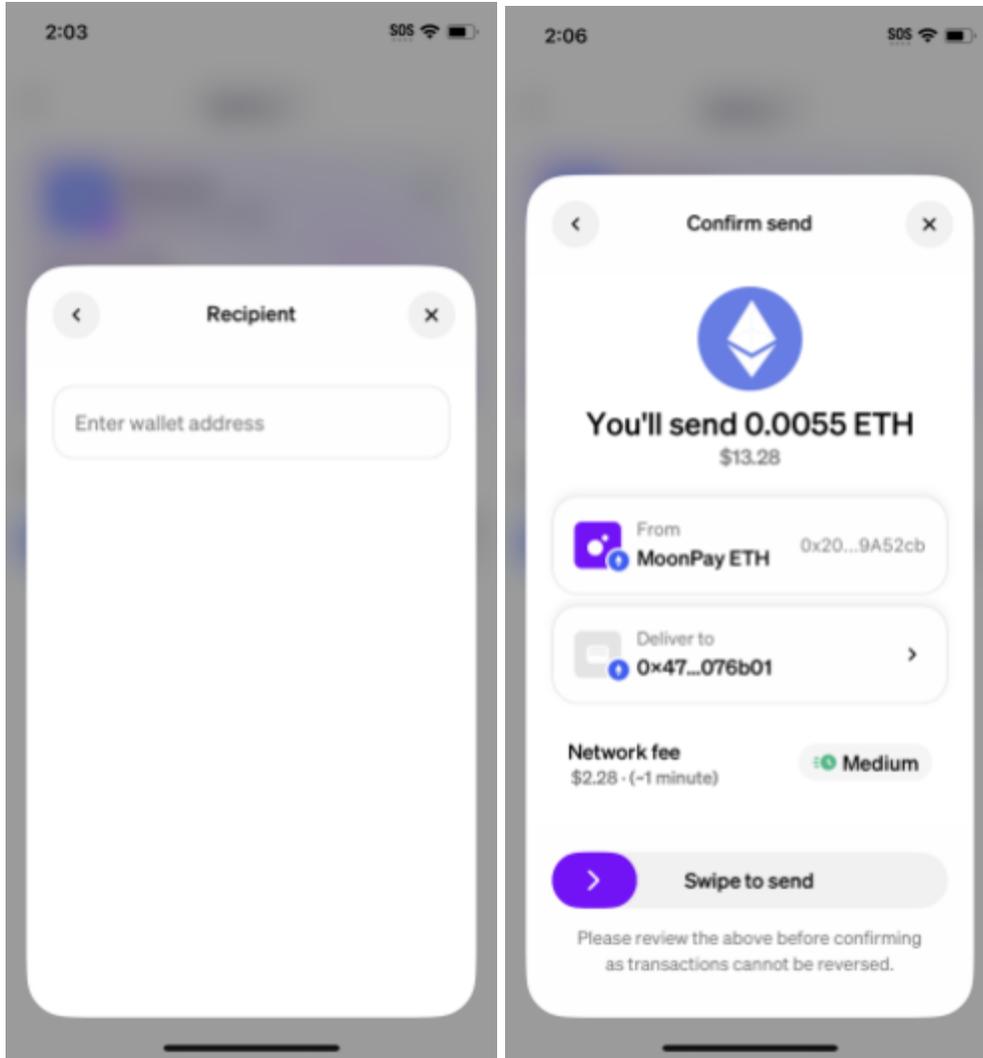
Download the MoonPay wallet from the app store and open the app, follow the steps below.

1. On the home screen select the “MoonPay account” you’d like to send from in this case we will select “Ethereum”. Select the three dots at the top right, and then the “Send” button.



2. To seize the funds it requires a wallet preferably a brand new wallet that was created by your organization for the purpose of receiving the cryptocurrency to be seized.
3. After selecting “Send” select the “Max” button and then click “Continue”. It will then ask to confirm that you want to send the max amount, select the “Confirm and continue with max send” button. On the next page you will enter the wallet address you want to send the funds to. Finally on the last page you can review the transaction and swipe the button at the end to send it.

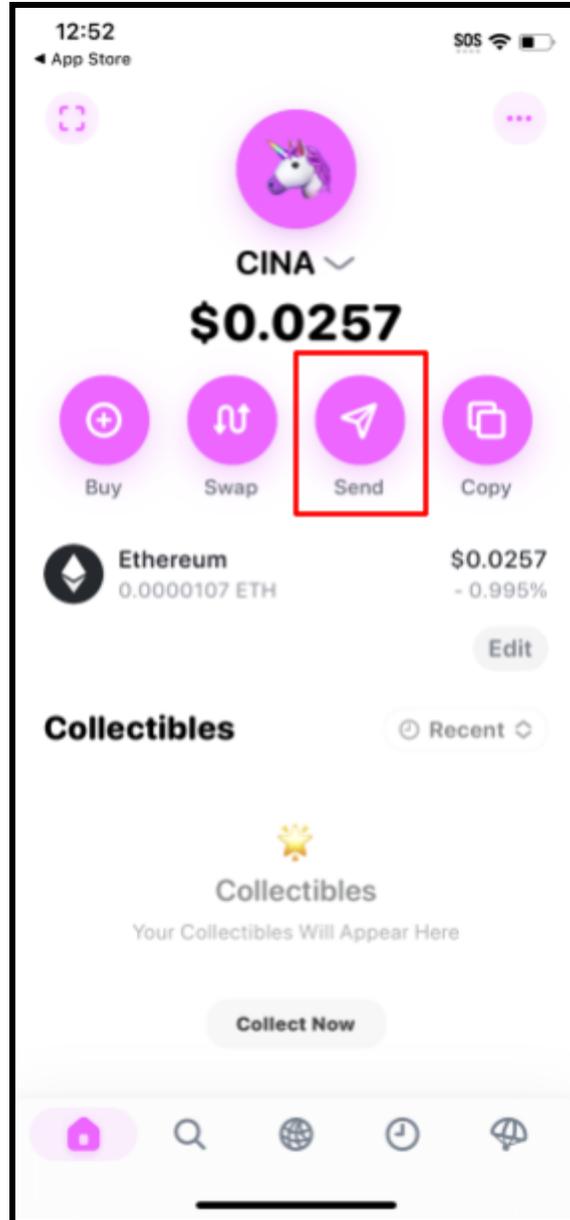




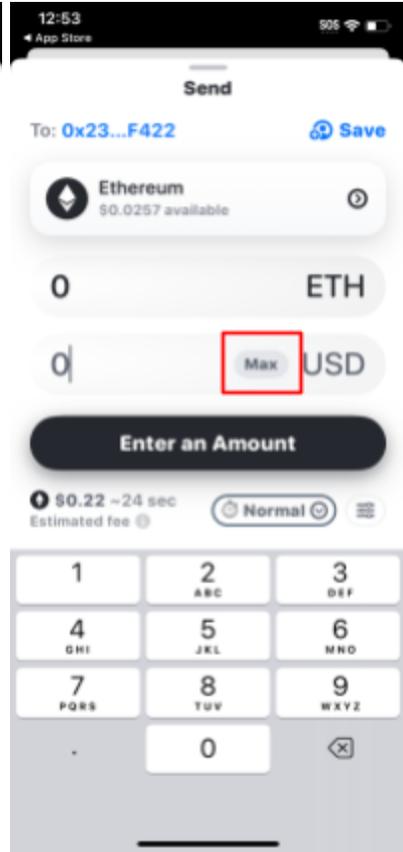
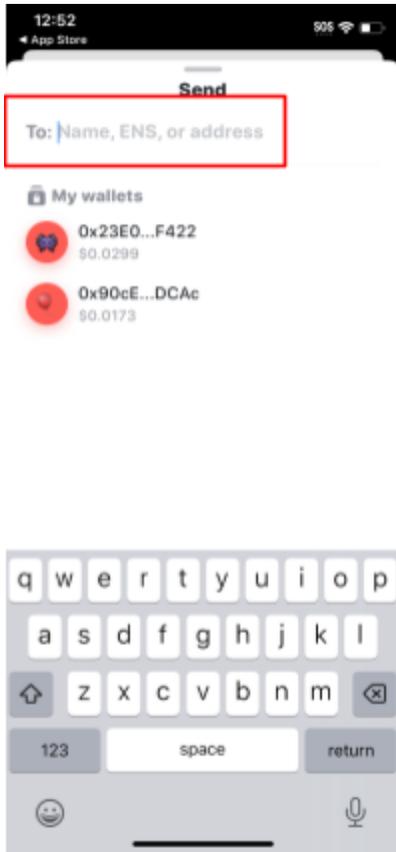
Rainbow

To perform a seizure of the wallet the suspect must be signed in to their wallet. Download the Rainbow wallet from the app store and open the app, follow the steps below.

1. Select the “Send” button which is the third button underneath the wallet balance.



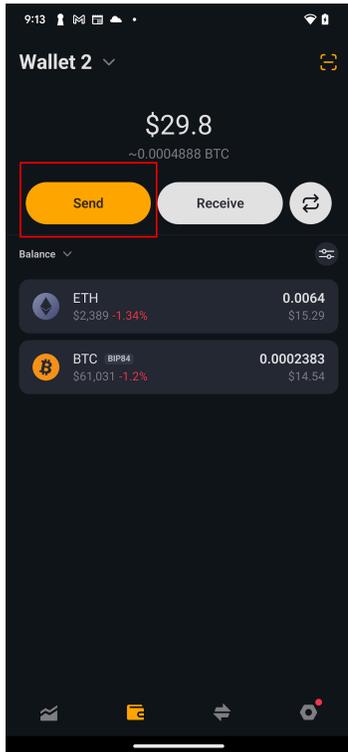
2. To seize the funds it requires a wallet preferably a brand new wallet that was created by your organization for the purpose of receiving the cryptocurrency to be seized.
3. After selecting “Send” you will be prompted to insert the address to send the funds to. This field needs to be filled with a wallet owned by your organization. Next if there are multiple wallets on the phone it will ask which wallet to use. The next screen will allow you to choose the amount of cryptocurrency to send for simplicity press “MAX”.



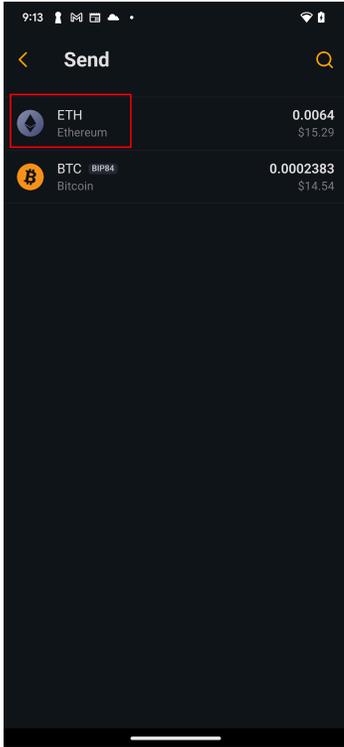
Android Cryptocurrency Wallets

Unstoppable

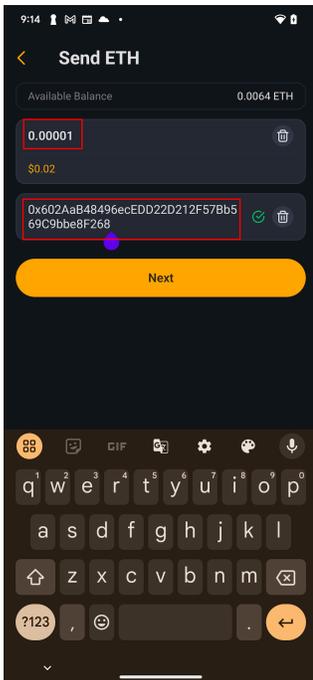
1. Press Send to begin the seizure



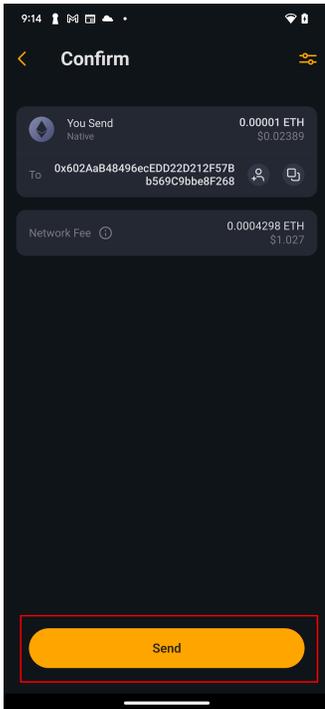
2. Select the currency to seize



3. Specify the amount to seize and the destination address.

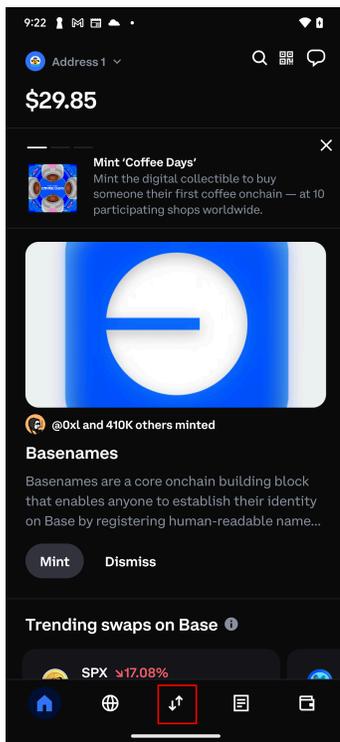


4. Review seizure and press Send to finish.

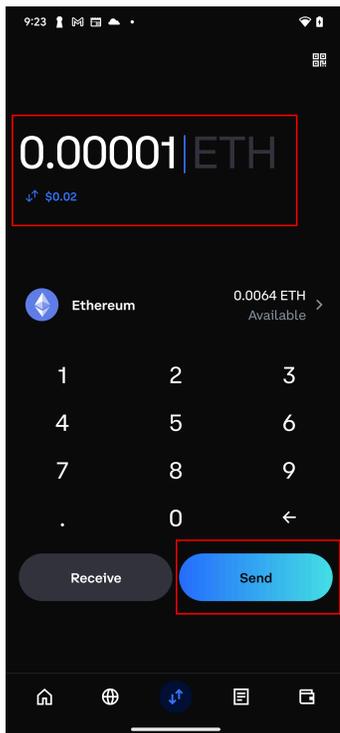


Coinbase

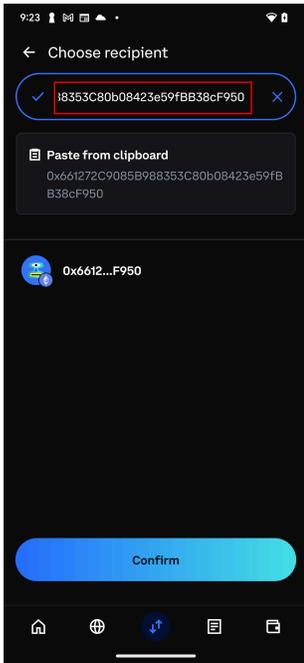
1. Hit the twin arrows button in the bottom-center.



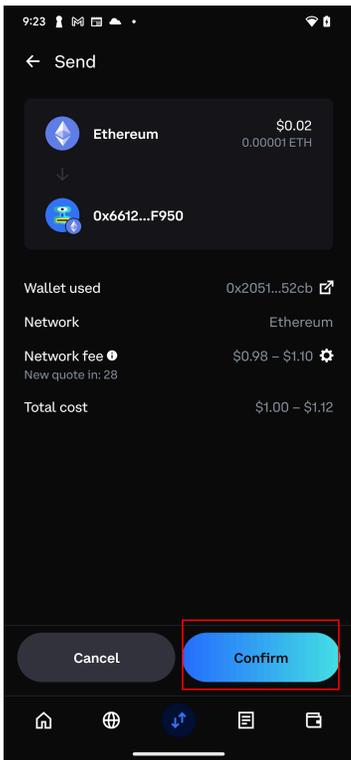
2. Specify the amount. The app will default to the currency with available funds. Hit the Send button.



3. Specify the destination address and hit the Confirm button.

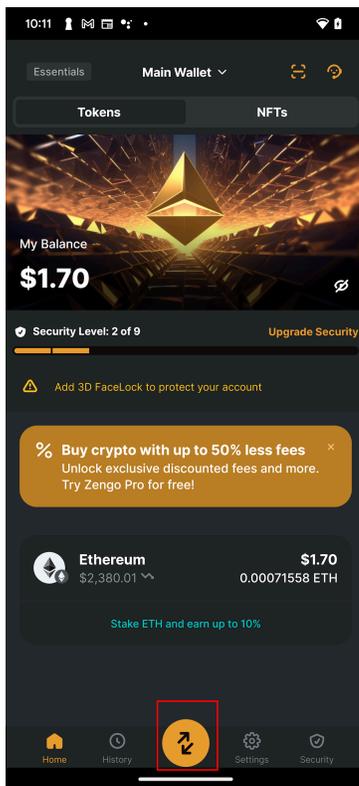


4. Review and hit the Confirm button.

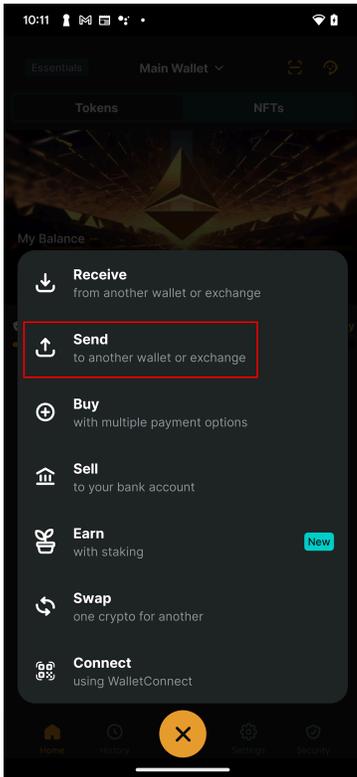


Zengo

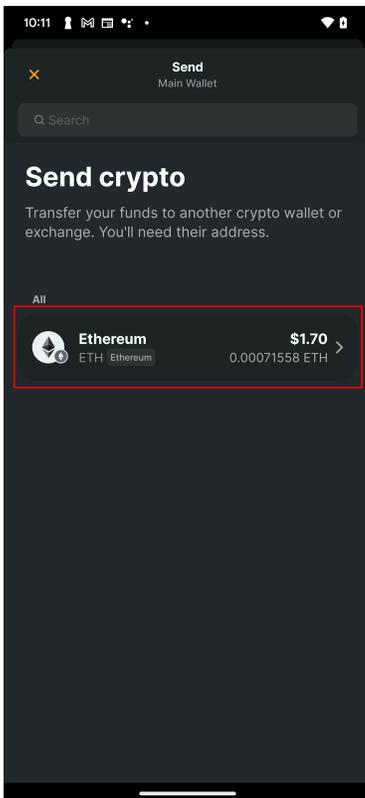
1. Press the twin arrow button at the bottom to begin the seizure.



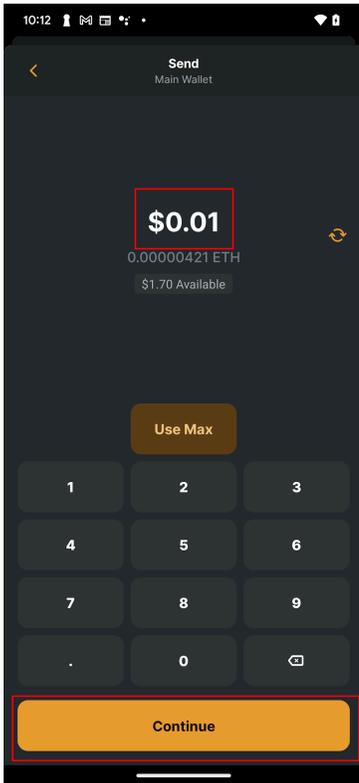
2. Select the Send option



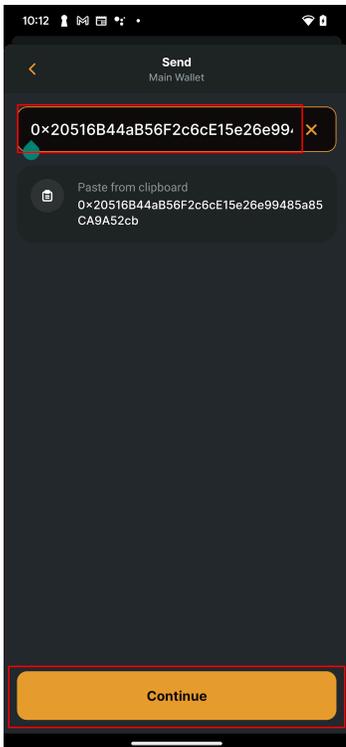
3. Select the currency to seize



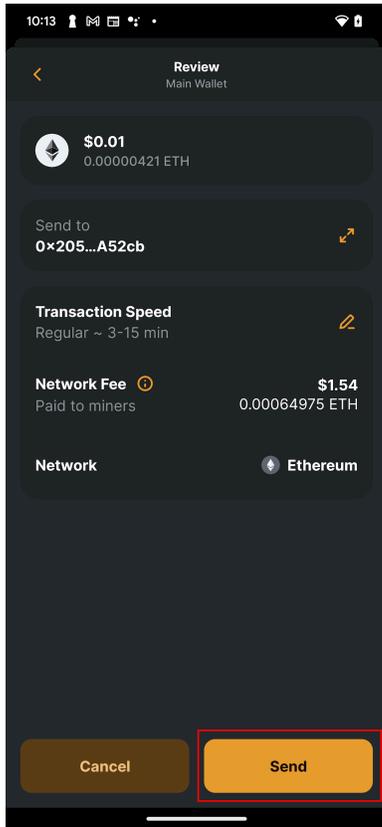
- Specify the amount to send. There is a 'Use Max' button to seize everything.



- Specify the destination address.

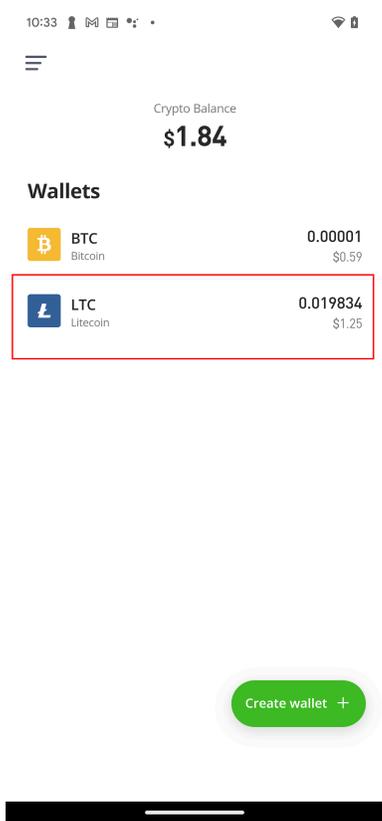


6. Review seizure and press 'Send' to finish.

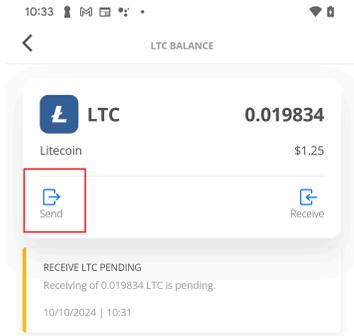


eToro

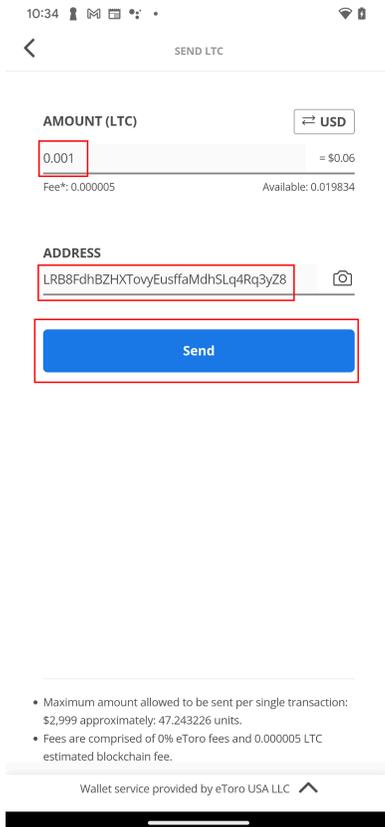
1. Select the currency to seize



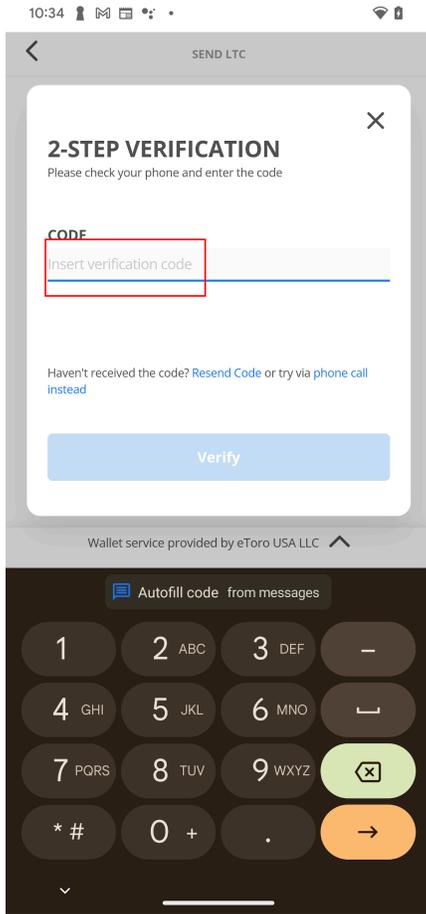
2. Press the send button



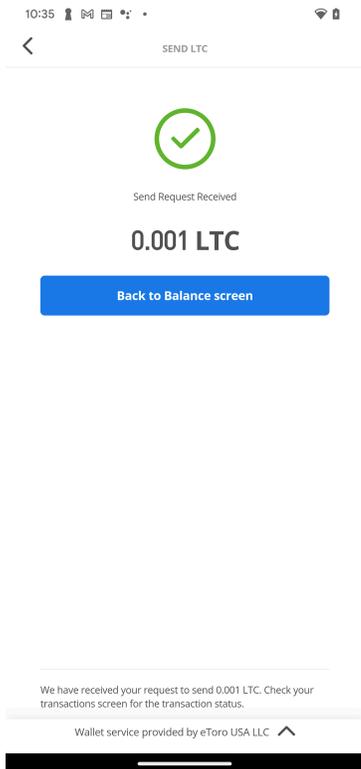
3. Enter the amount and the destination address. Press send.



4. You will need a 2-step verification code. It is sent to the linked phone number over SMS.

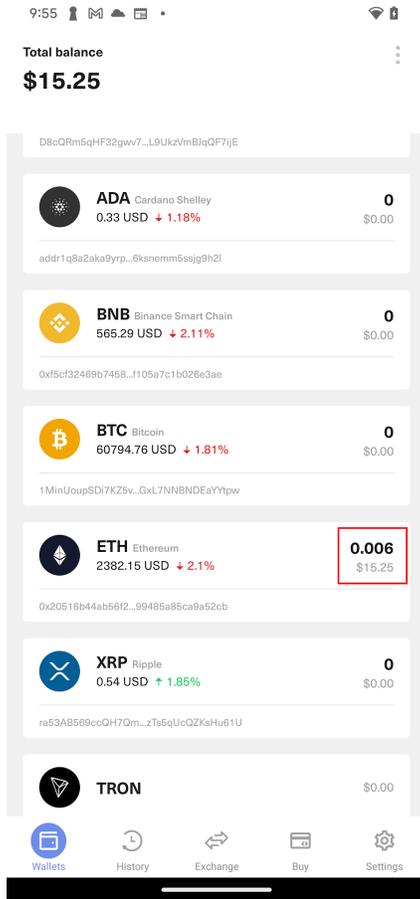


5. Crypto will be sent without further confirmation.

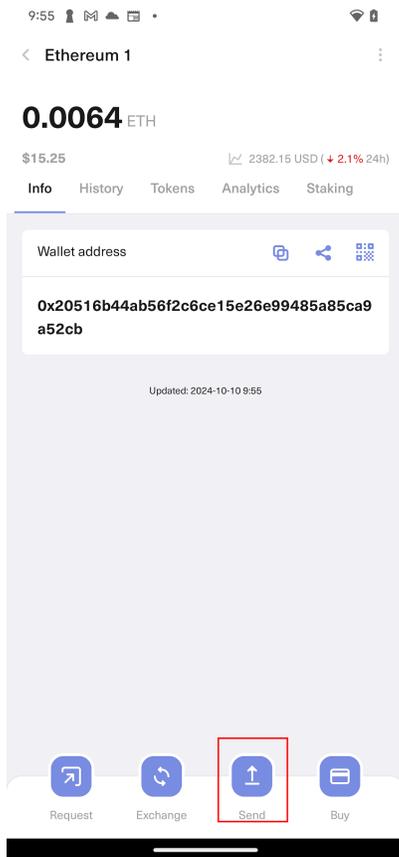


Guarda

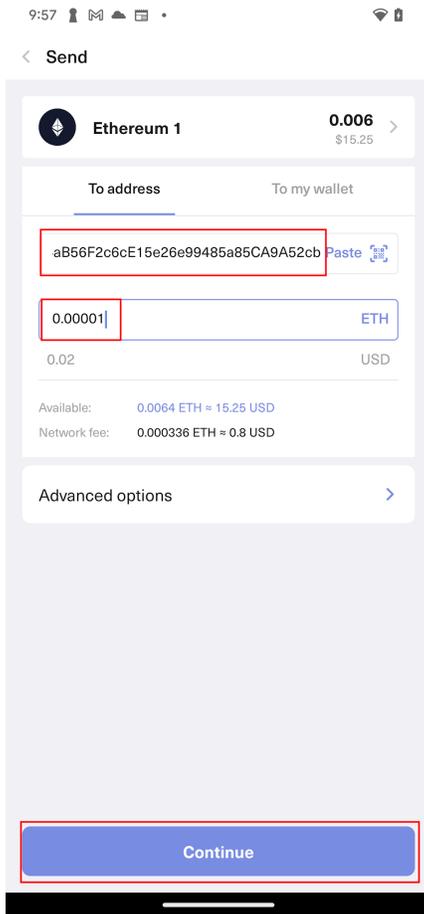
1. Select a wallet with funds to seize



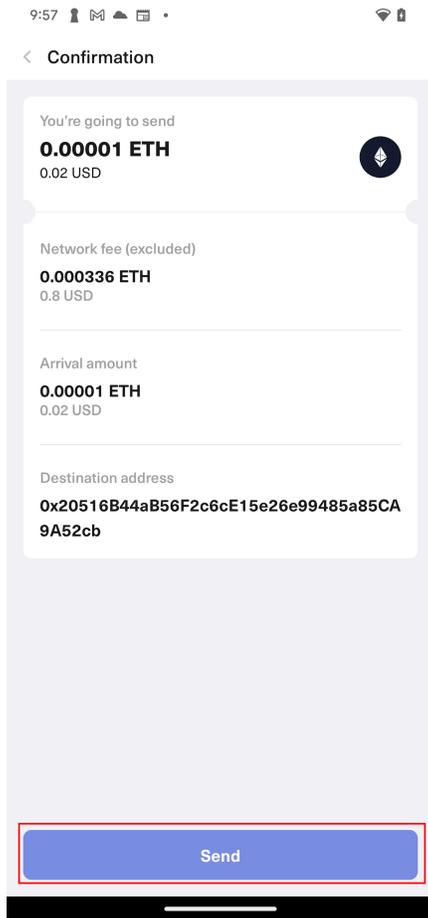
2. Click the Send button at the bottom



3. Specify the destination address and amount and then press Continue

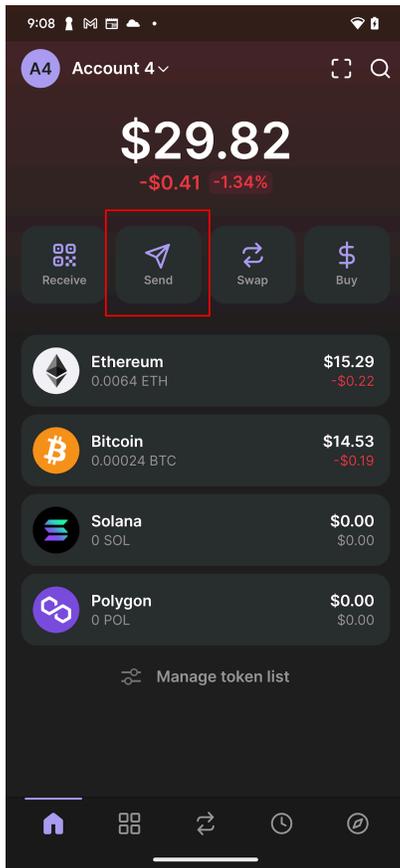


4. Review transaction and then press Send to finish

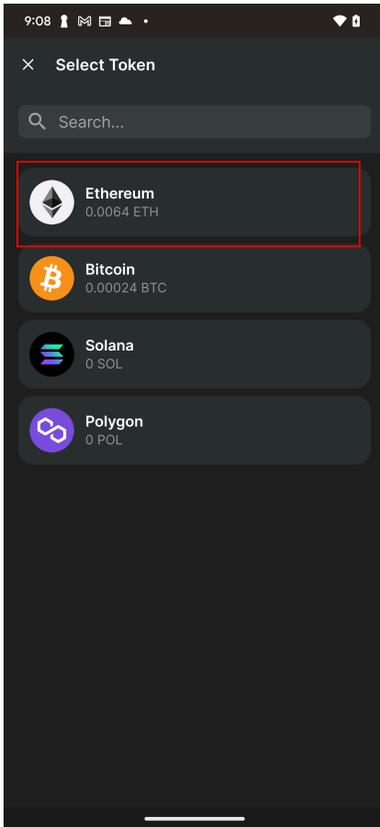


Phantom

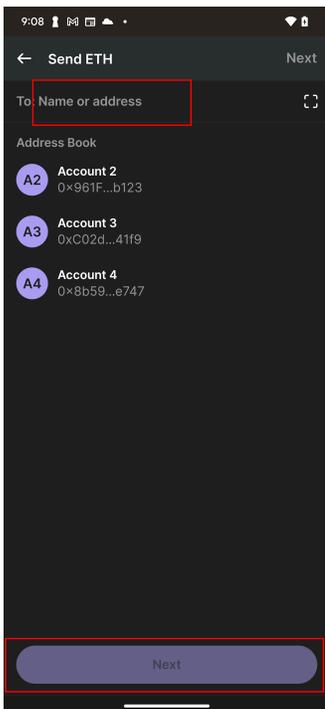
1. Press Send button to start Seizure



2. Select the currency to seize



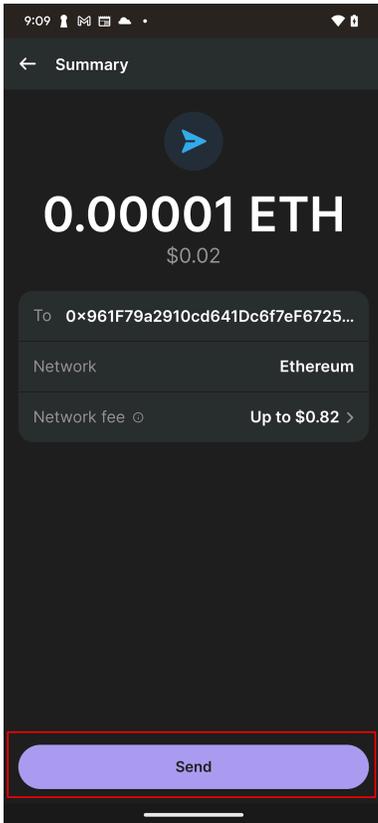
3. Specify the destination address and press Next



4. Specify the amount and press Next. There is a 'Max' button to send everything

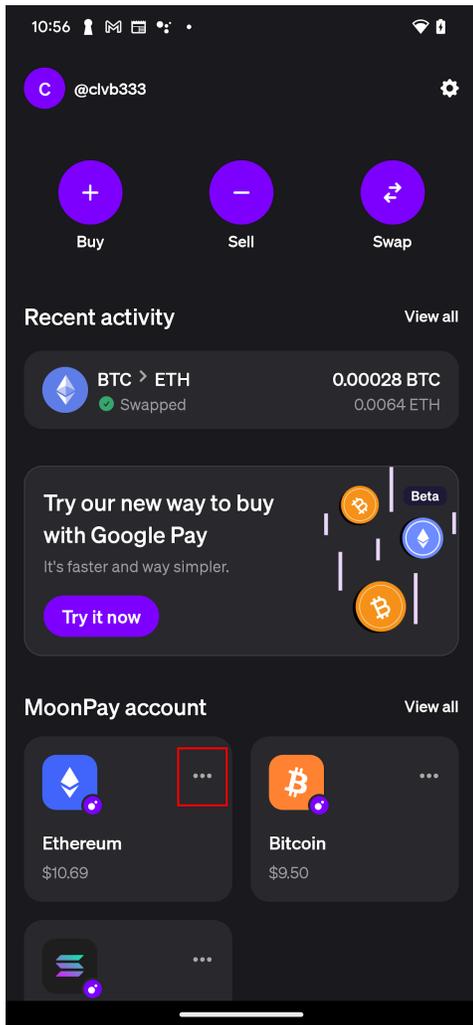


5. Review the seizure and press Send.

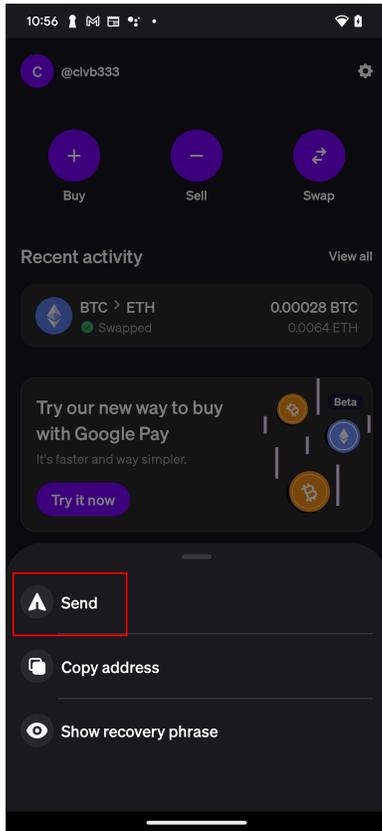


MoonPay

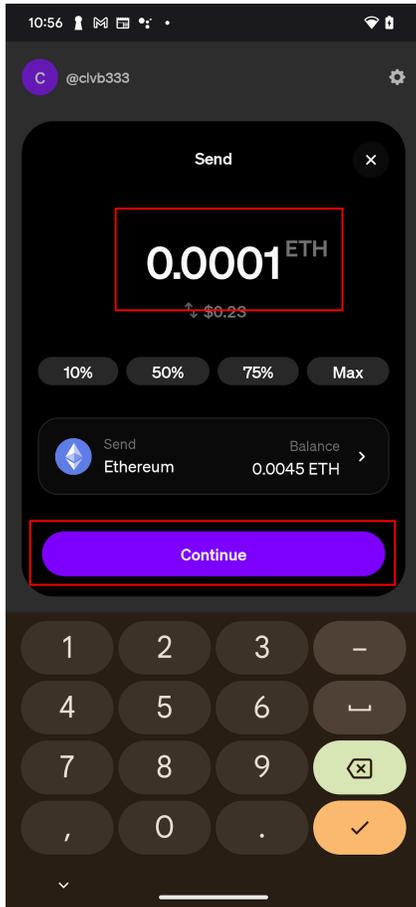
1. Click the three dots on the tile with the desired currency.



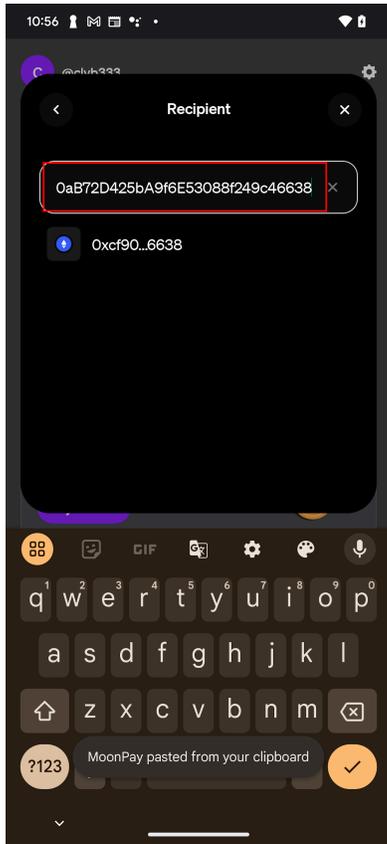
2. Hit the Send button



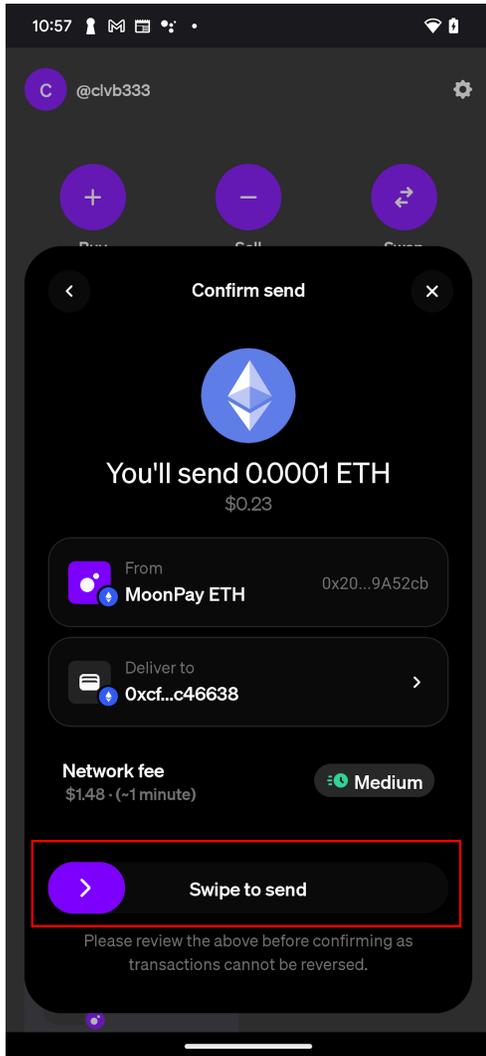
3. Specify the amount and hit Continue. There is a 'MAX' button to seize everything.



4. Specify the destination address

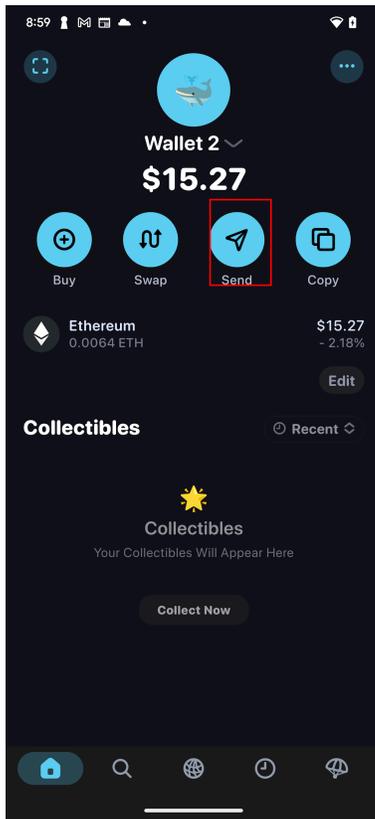


5. Confirm send with swipe



Rainbow

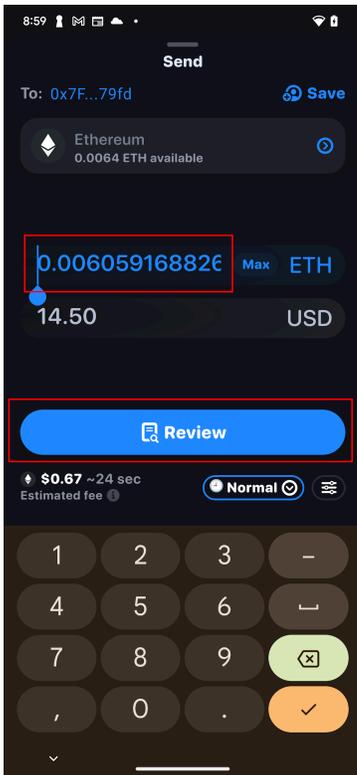
1. Press Send to start seizure



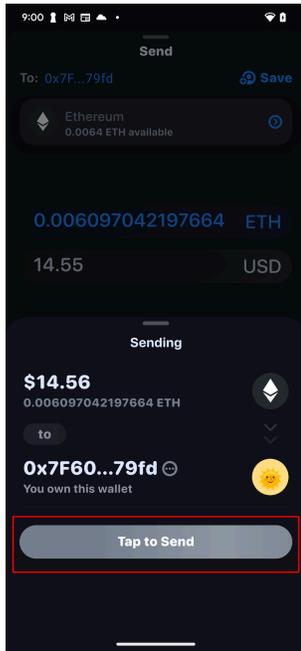
- Specify the destination address and the currency to use.



- Specify the amount to seize. There is a 'Max' button to seize everything.

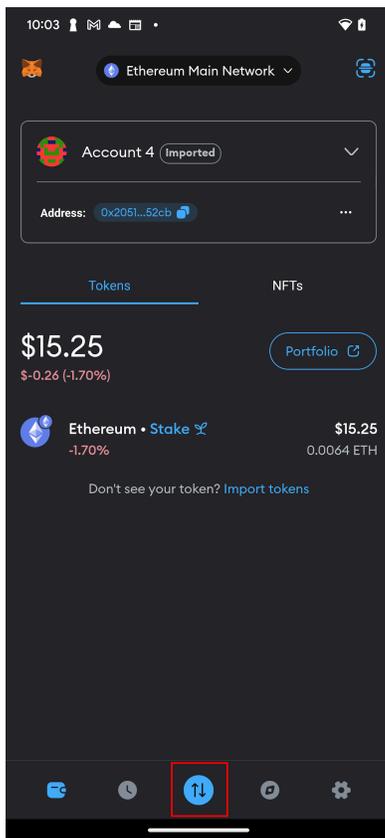


- Review seizure and press 'Tap to Send' to finish

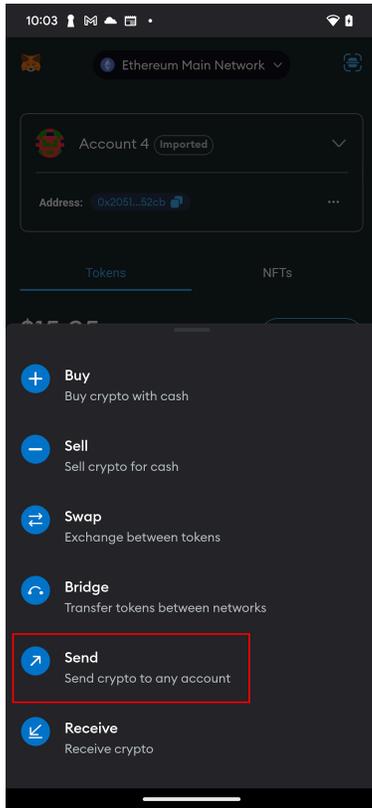


MetaMask

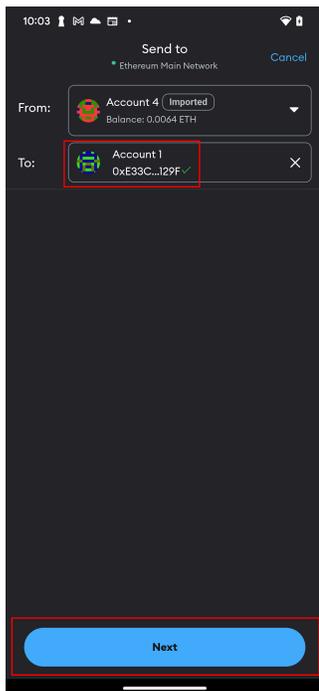
1. Press the twin arrow button at the bottom to pop out the menu



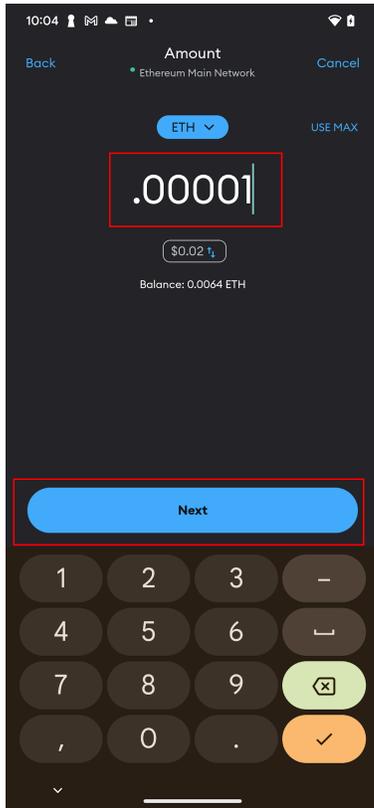
2. Select the Send option



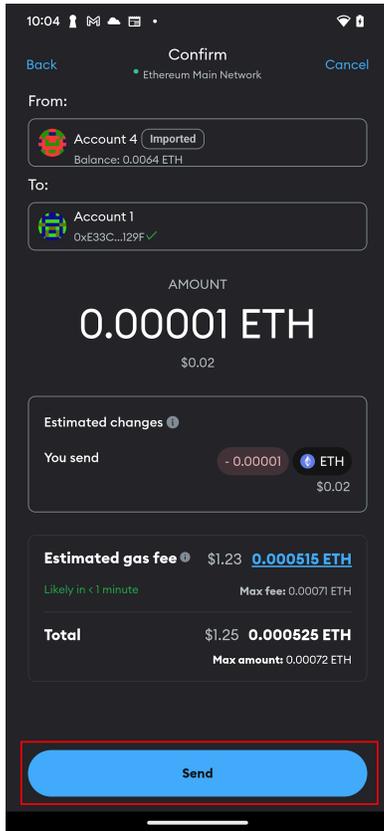
3. Enter the destination address into the second box



4. Enter the amount to seize. There is a USE MAX button to seize everything.



5. Review the transaction and hit Send to confirm.

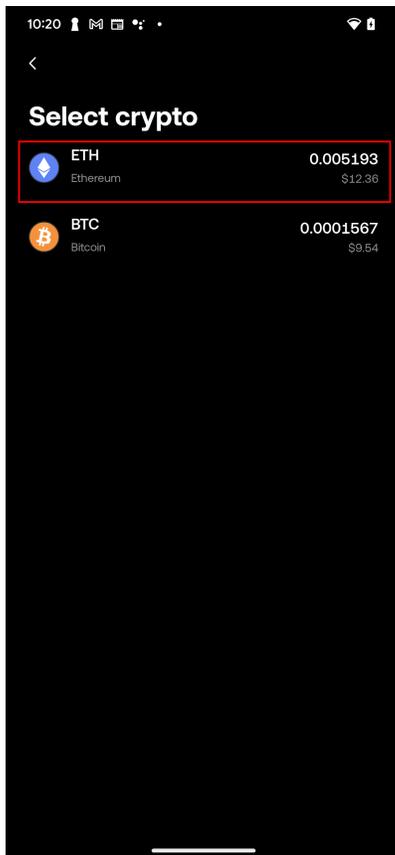


OKX

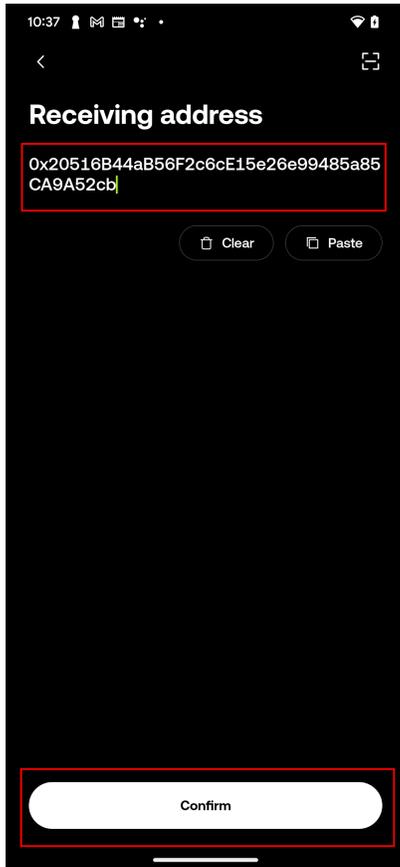
1. Press the send button to begin the seizure



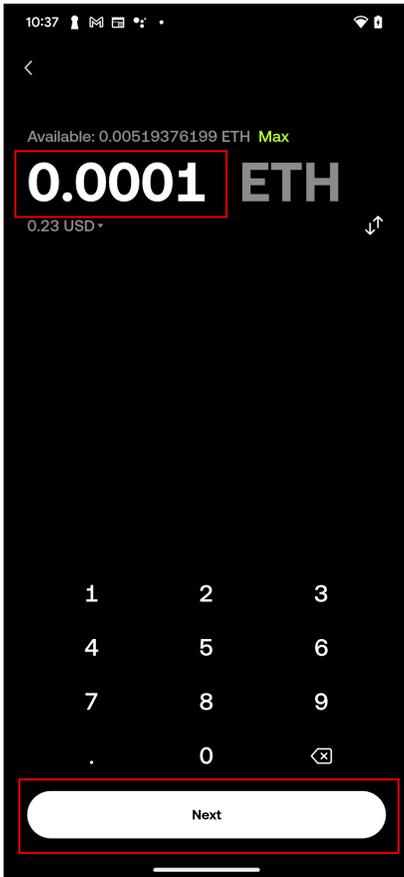
2. Select the currency to Seize



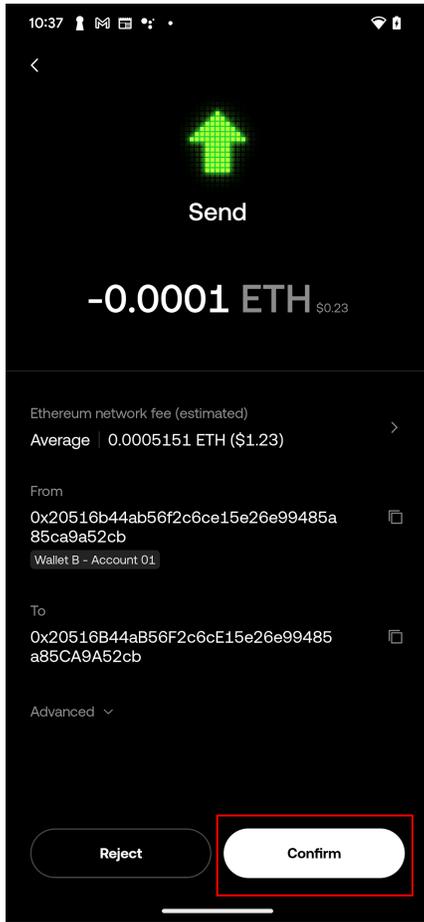
3. Specify the destination address and press Confirm



4. Specify the amount and press Next. There is a 'Max' button to seize everything.

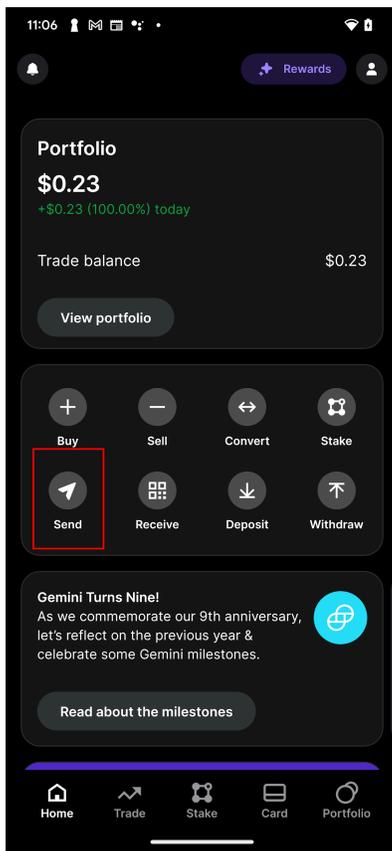


5. Review seizure and press Confirm to finish

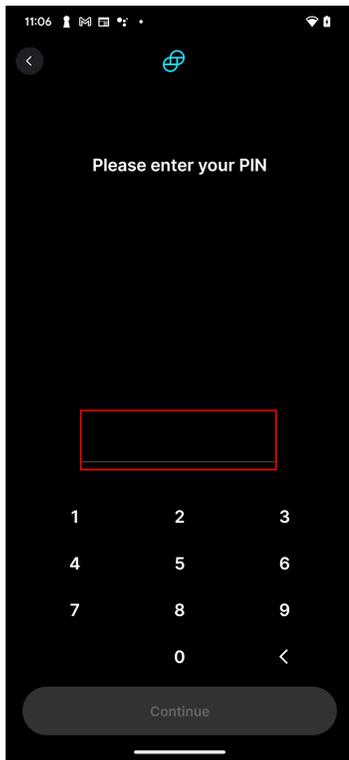


Gemini

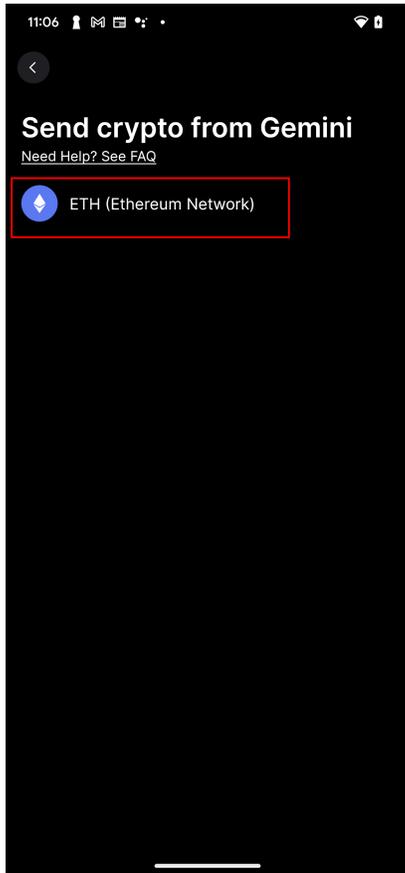
1. Hit the send button



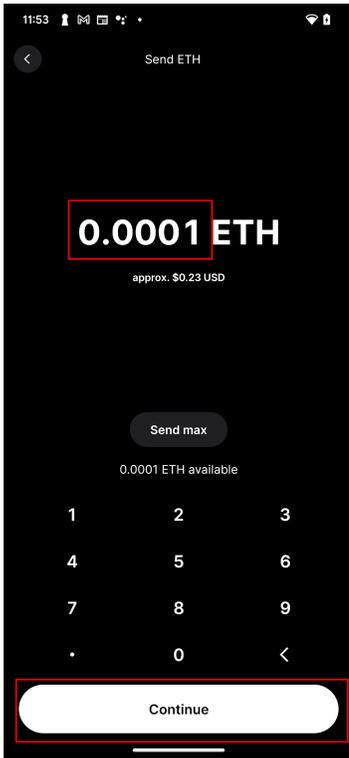
2. It will prompt for the user's PIN. Enter it here to continue



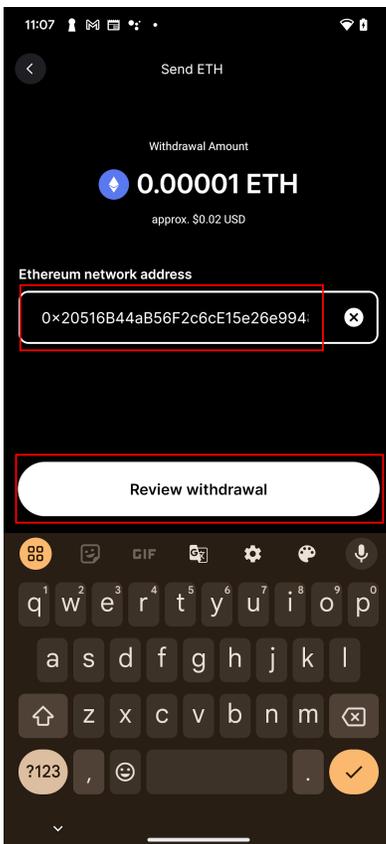
3. Select the currency to seize



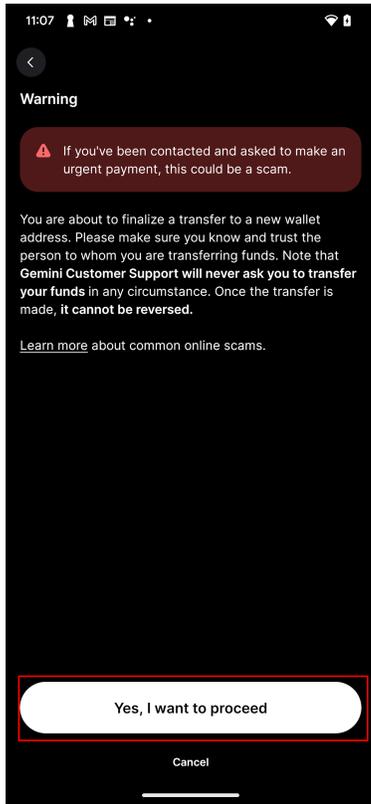
4. Specify the amount and press Continue. There is a 'Send max' button to seize everything.



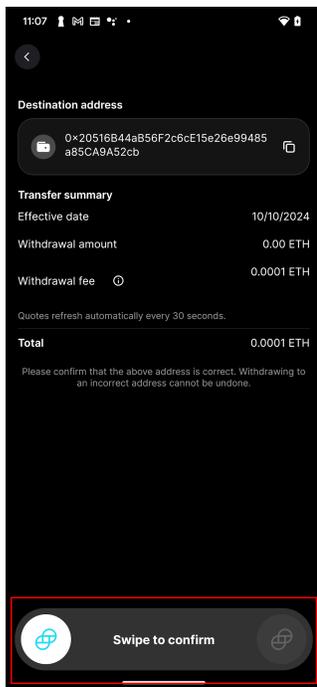
5. Specify the destination address and press Review withdrawal



6. If you are prompted with a warning message click “Yes, I want to proceed”

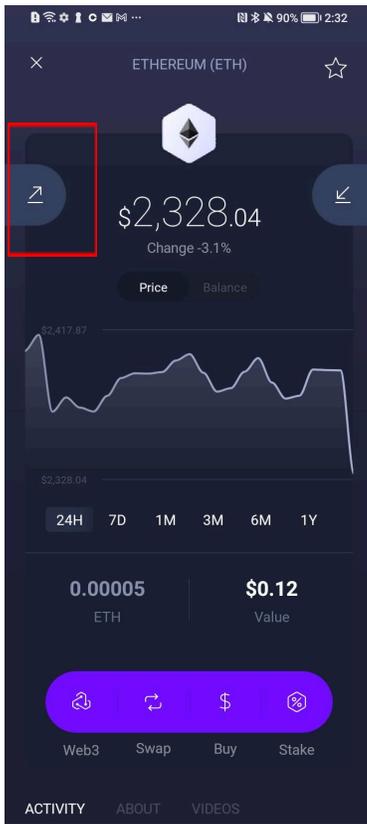


7. Confirm by using the Swipe at the bottom

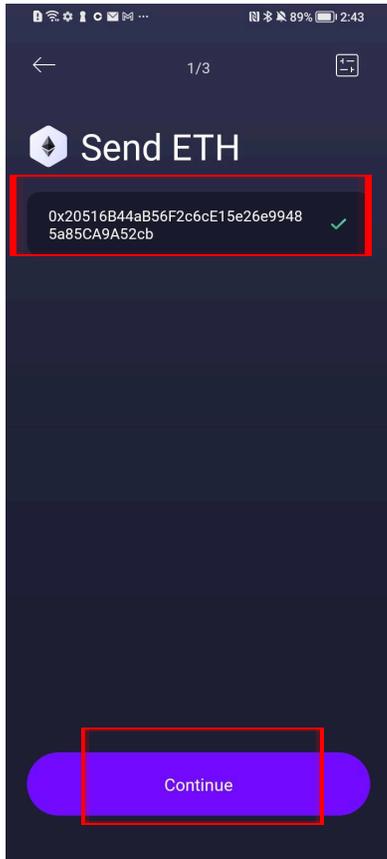


Exodus

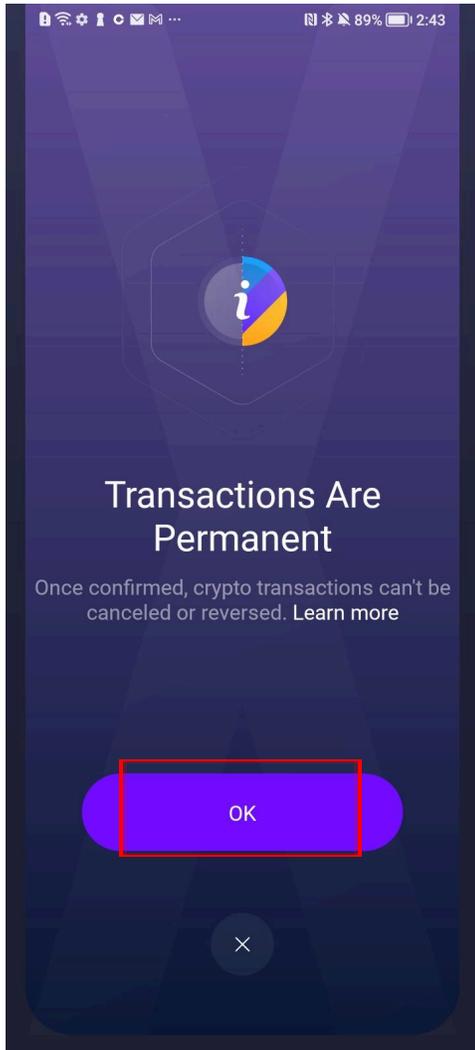
1. Hit the send button



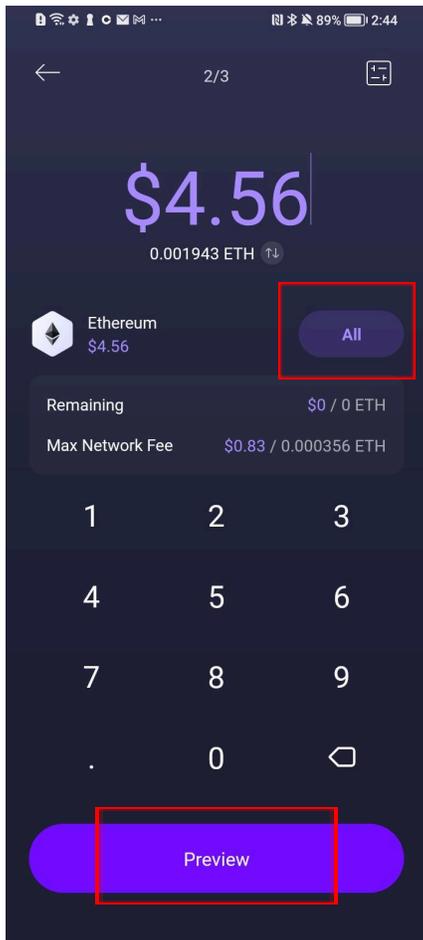
2. Enter in the address of the receiving wallet and press continue.



3. Press OK for the warning



4. Select "All" to transfer out all remaining funds



5. Continue with “Slide to Send”

