A LAWYER'S CRASH COURSE INTO BLOCKCHAIN & CRYPTO

MODULE 1 – CRYPTO WALLET

XIAOLI JIN

HARVARD LAW SCHOOL, JD 2024

Why might a lawyer want to have a crypto wallet, if he/she doesn't trade crypto?

- Regulations on crypto wallets are all over the news

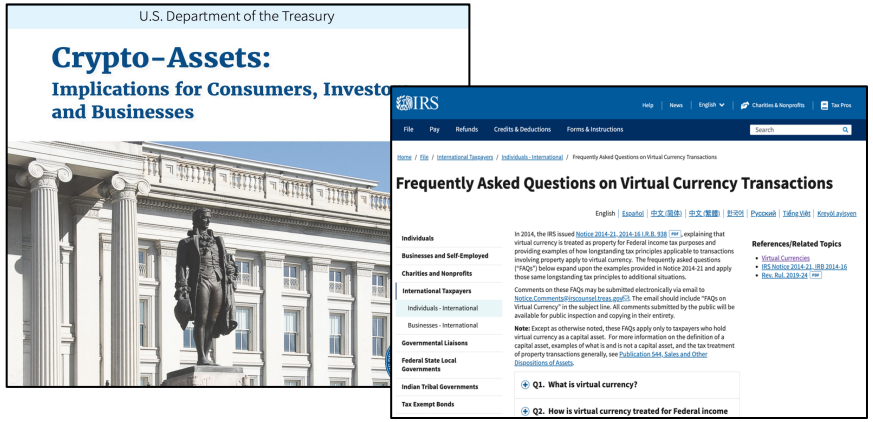
IRS' plans for cracking cryptocurrency wallets

Markets News Report

U.S. Treasury Department on Track to Regulate Unhosted Wallets

Unhosted Crypto Wallet Rules Will Allow Innovation, US Treasury Official Vows

- You can learn by poring over lengthy industry reports…



- But we believe the best way to learn is to set up your own wallet (but please do the readings too ☺)

Moreover, having a crypto wallet is a pre-requisite to exploring many blockchain & crypto use cases.

What you can do after setting up a crypto wallet

If you're interested in technology:

Creating your own **NFT** and transfer it to your wallet, exploring NFT's **copyright** and ownership issues

If you're interested in corporate transactions:

Joining a Decentralized Autonomous Organization (**DAO**), understanding how DAO creates a noval **corporate structure**

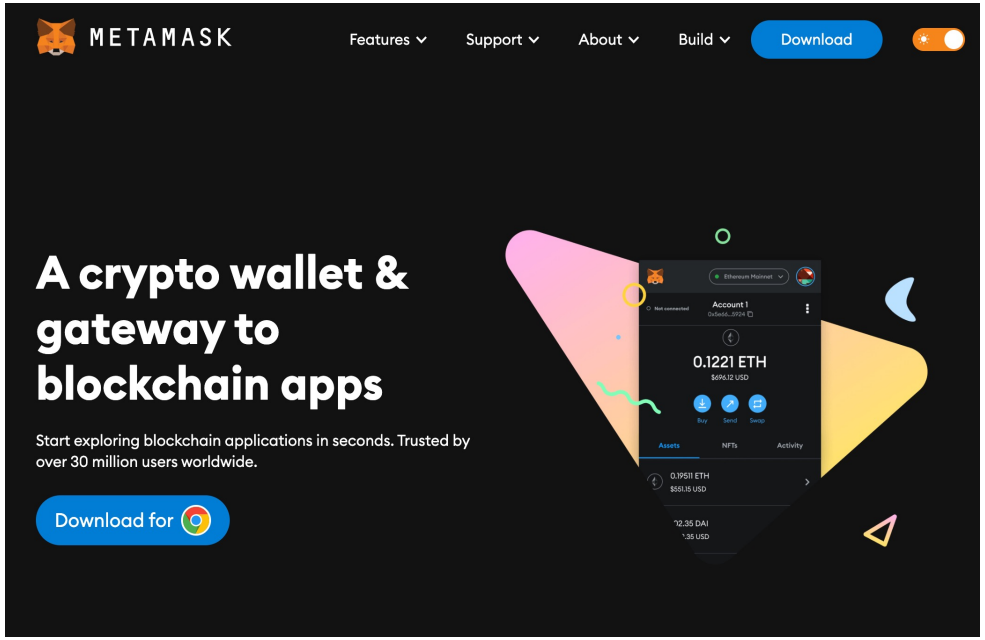
If you're interested in financial regulations:

Exploring **crypto lending** firsthand, observing the challenges of designing a robust regulatory framework

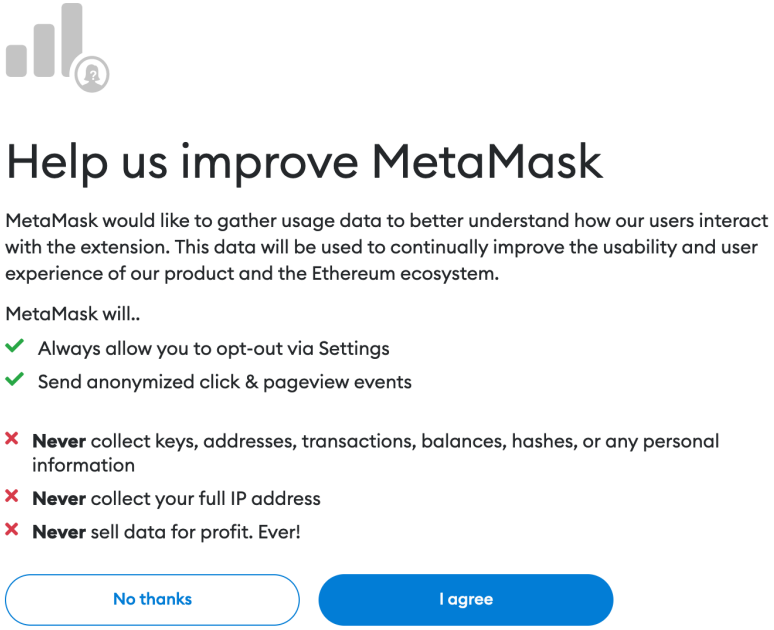
And much more to explore…

Convinced? Let's Get Started!

- Type https://metamask.io in the web browser; download the extension.

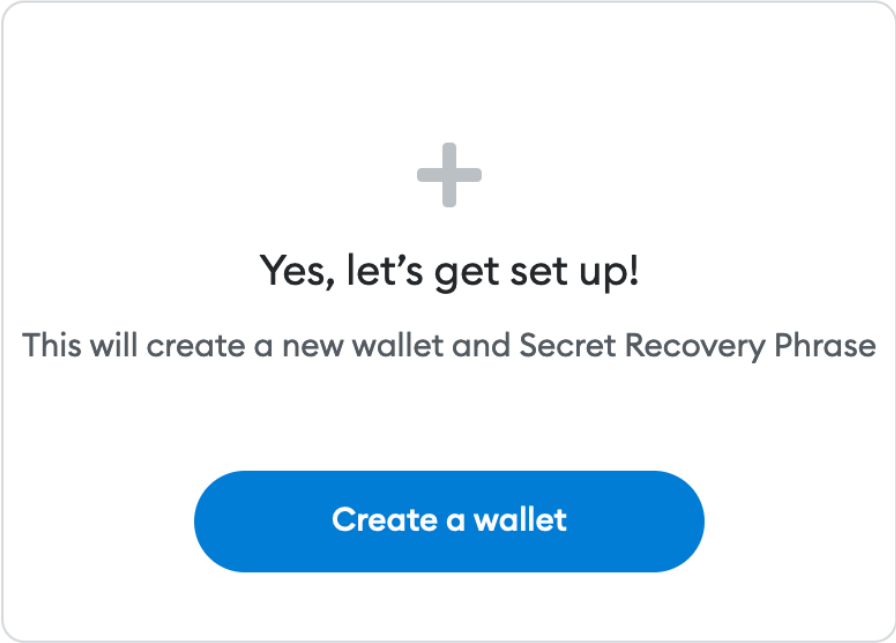


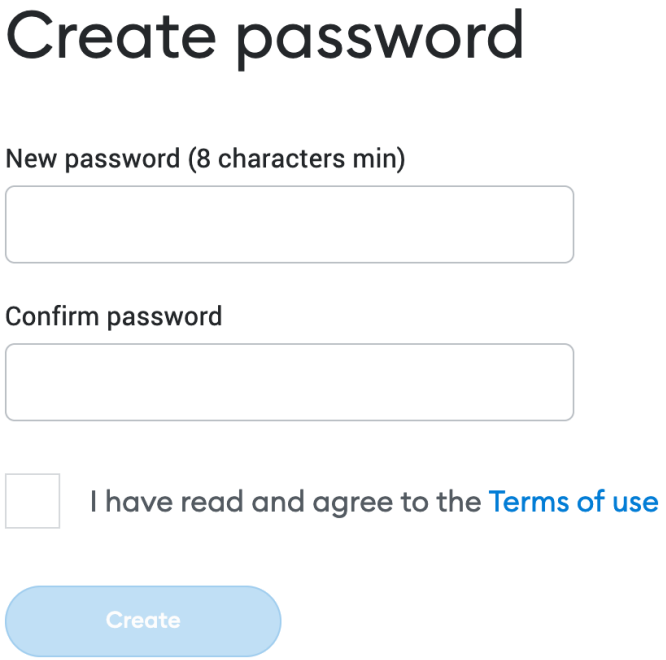
- Feel free to click "No Thanks" if you're concerned about data privacy



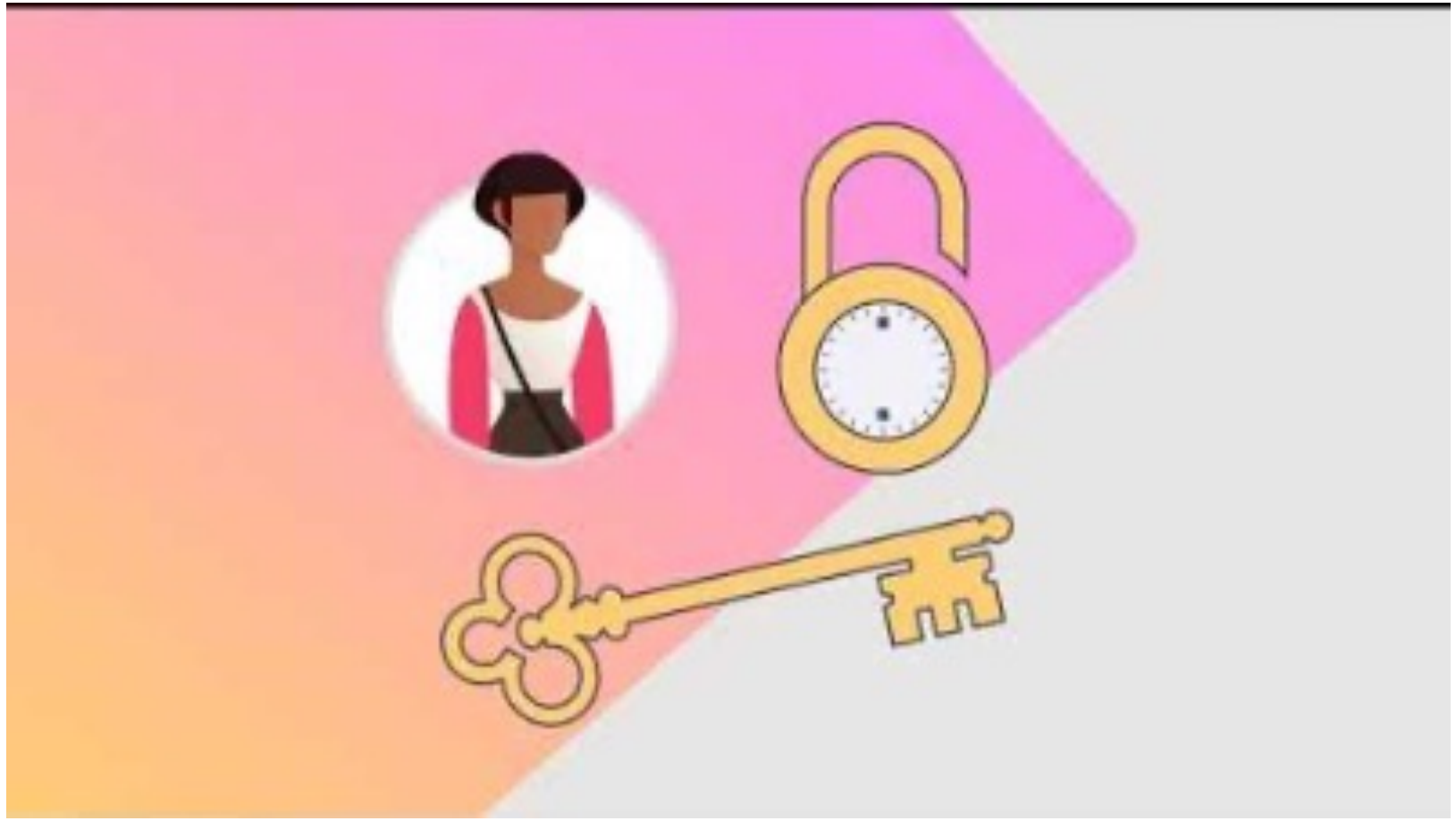
Just some more logistics about account setup…

- Select "Creat a Wallet" and create a strong password

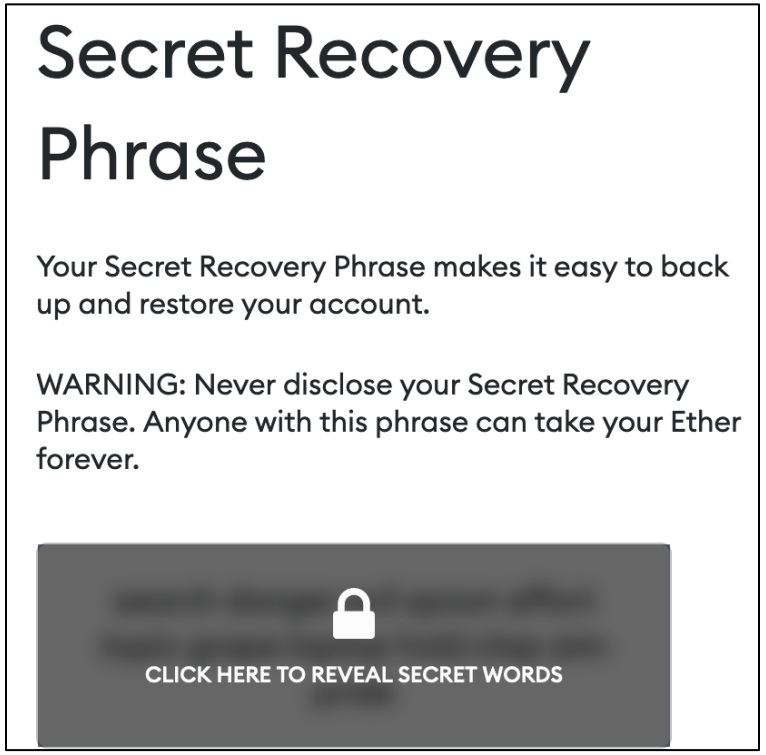




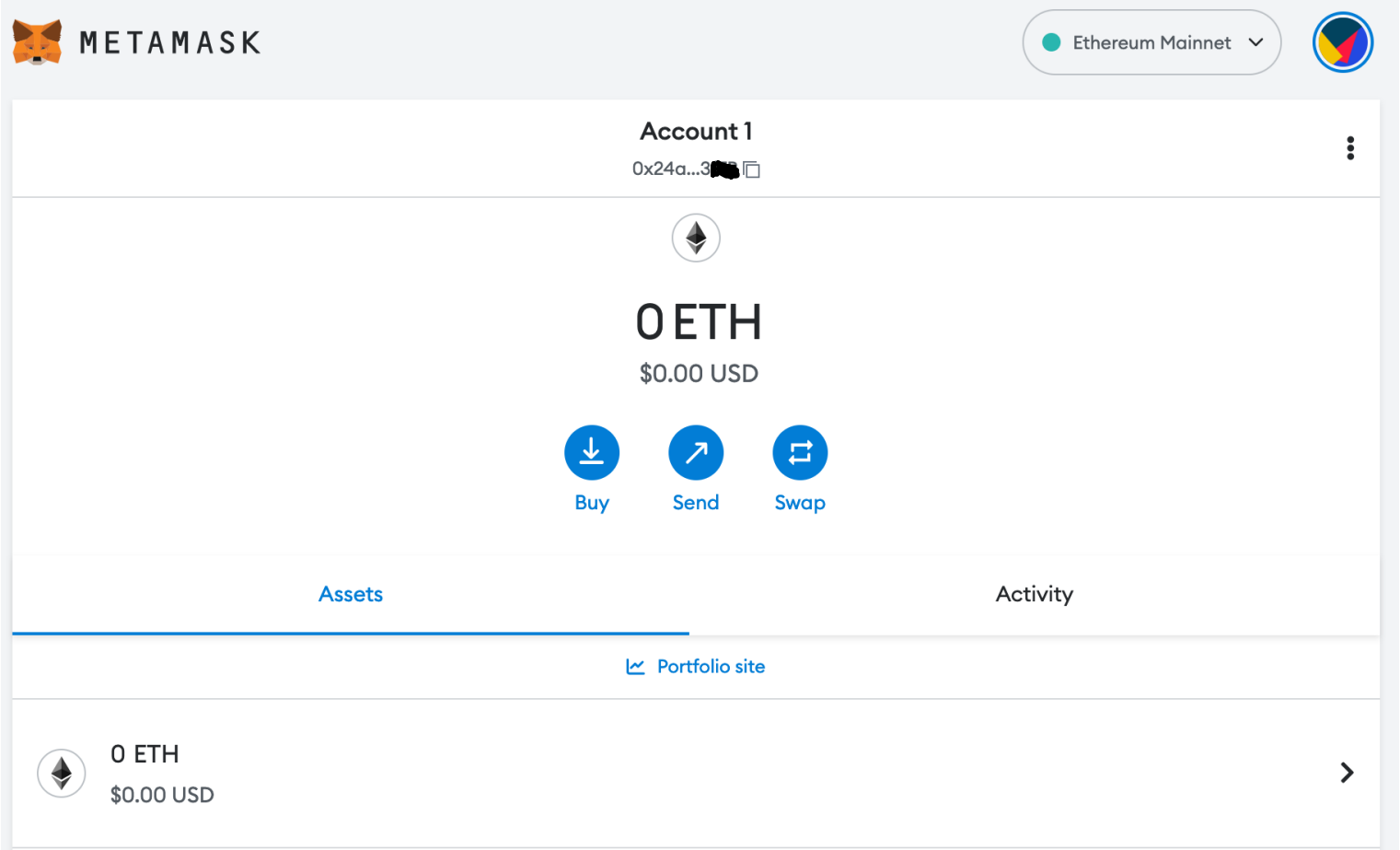
Now comes the critical part – the secret key to your wallet



Remembered the secret key to your wallet? Let's test it out.



If you see this page - Congrats! You just set up your first crypto wallet.



– Time to exercise your lawyer brain –
Read the excerpt from the U.S. Treasury Dept.
Is your wallet hosted or unhosted?

REQUIREMENTS FOR CERTAIN TRANSACTIONS INVOLVING CERTAIN CONVERTIBILE VIRTUAL CURRENCY OR DIGITAL ASSETS

Frequently Asked Questions (FAQs)

What is a hosted wallet?

A hosted wallet is a digital account hosted by a third-party financial institution, which allows the account-holder (the user) to store, send, and receive cryptocurrency.

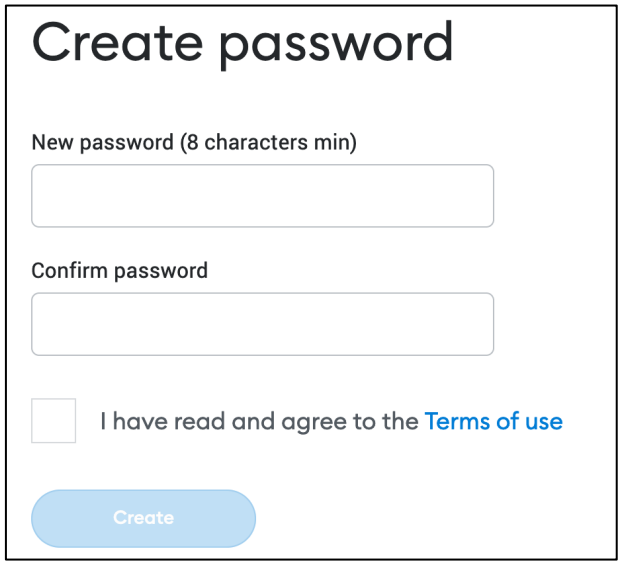
What is an unhosted wallet?

An unhosted wallet is not hosted by a third-party financial system. It can be very difficult or impossible to determine who is accessing or in control of the use of cryptocurrencies in an unhosted wallet. Unhosted wallets allow for anonymity and concealment of illicit financial activity.

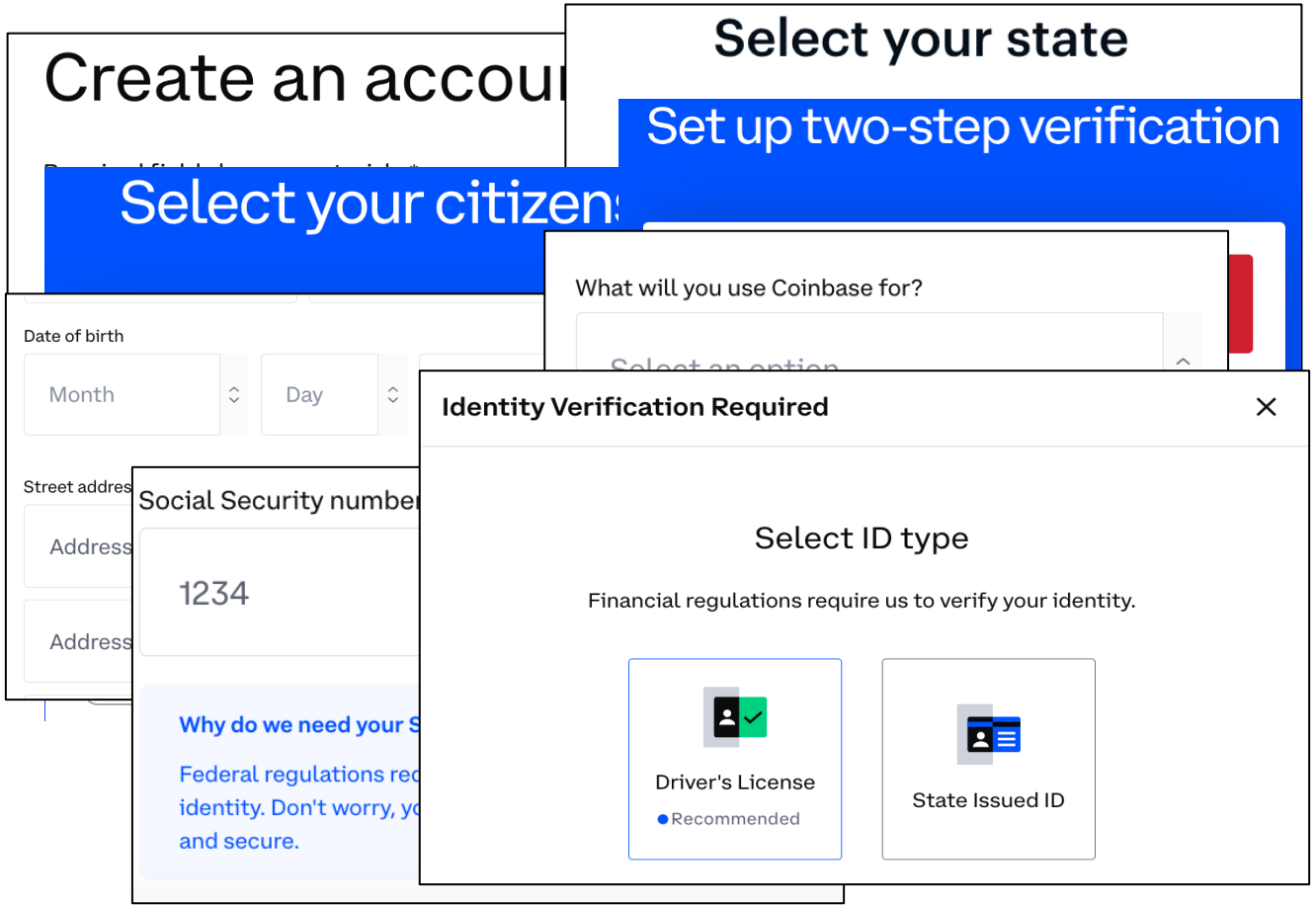
Excerpt from the U.S. Department of Treasurey

Why does the Treasury Dept. say that unhosted wallets allow for greater user anonymity?

When you set up an unhosted wallet on Metamask:



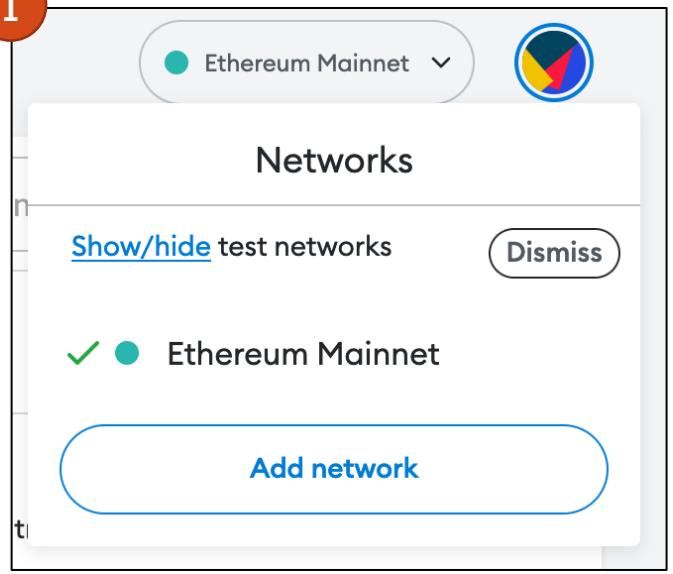
When you set up a hosted wallet:



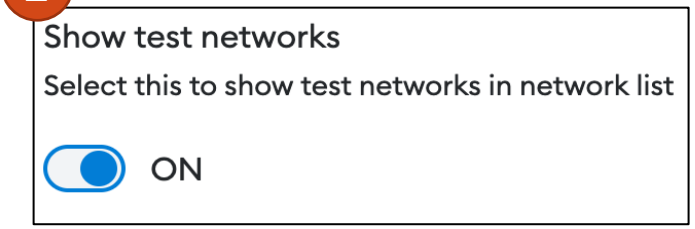
<u>All you gave to the wallet provider is a password</u>

Now let's put your wallet into use – Time for us to send you some crypto tokens

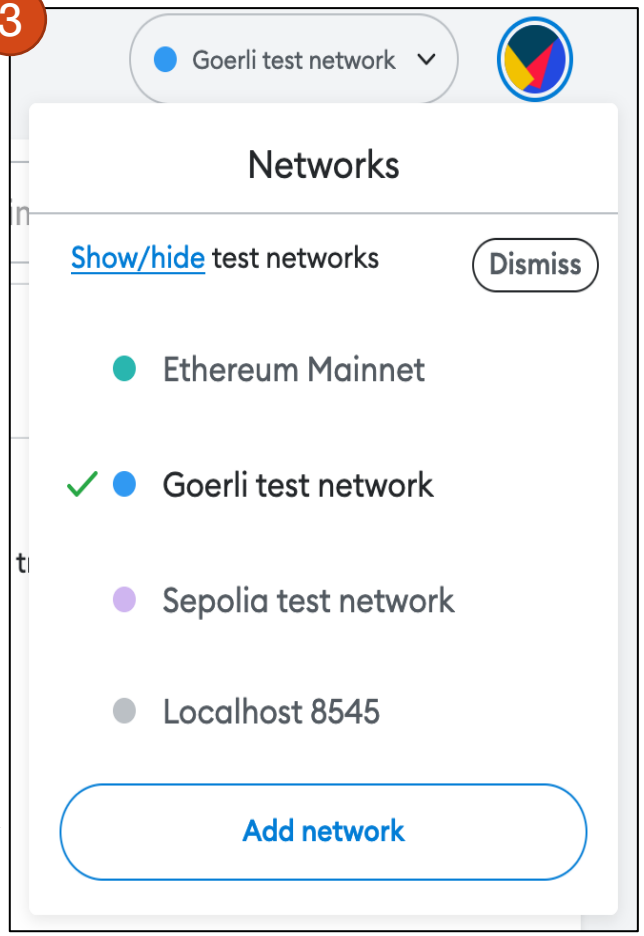
1



2



3



But don't get too excited ☹

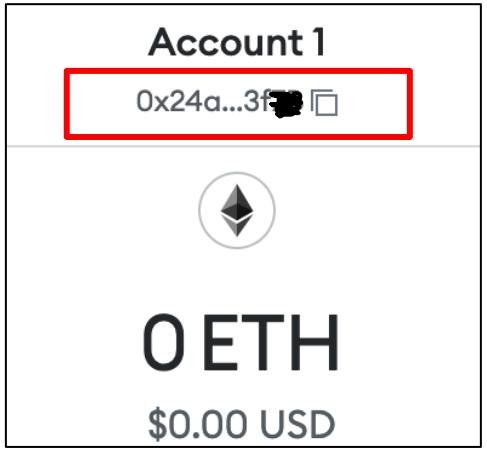
We are not going to send you real crypto tokens (unless you find us sponsors ☺)

Instead, we will send you tokens on test networks. Test tokens mimic how real crypto tokens work, but do not carry monetary value themselves.

Follow the instruments to fire up the "Goerli test network"

Join our Telegram Group and send us your wallet address – You first crypto tokens are on their way!

Three Minute Break



Drop your wallet address @ this group chat

Wallet address is above your account balance

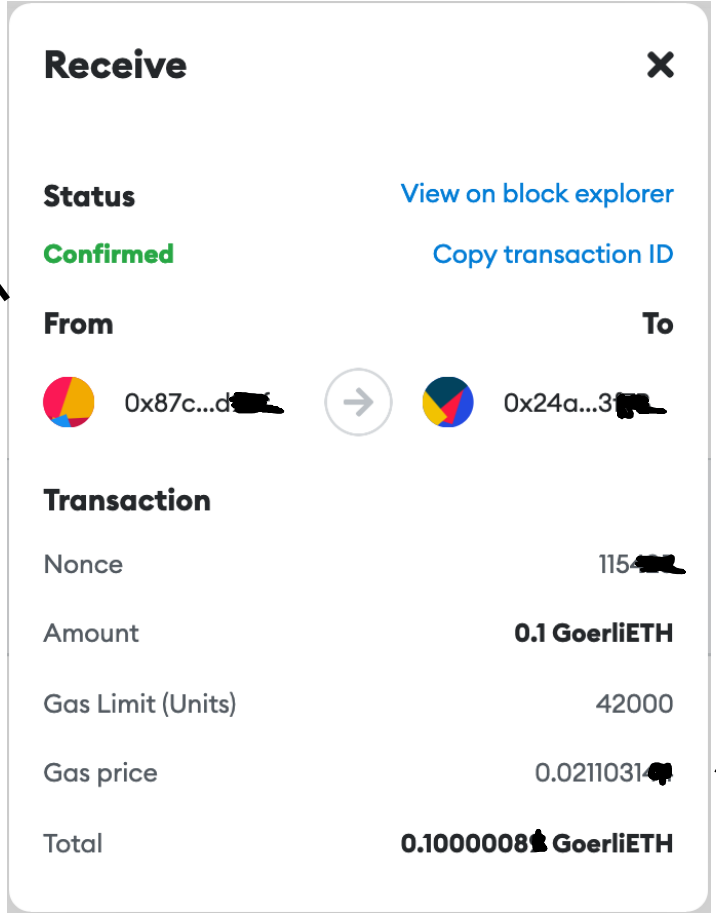
Got your first token? Now click on most recent transaction. Let's take break down what happened.

Sender's wallet address

Implications for privacy law:

Is a wallet address personal data?

An arbitrary string concatenated with the hash of a block



Receiver's (your) wallet address

Cross-border data transfer:

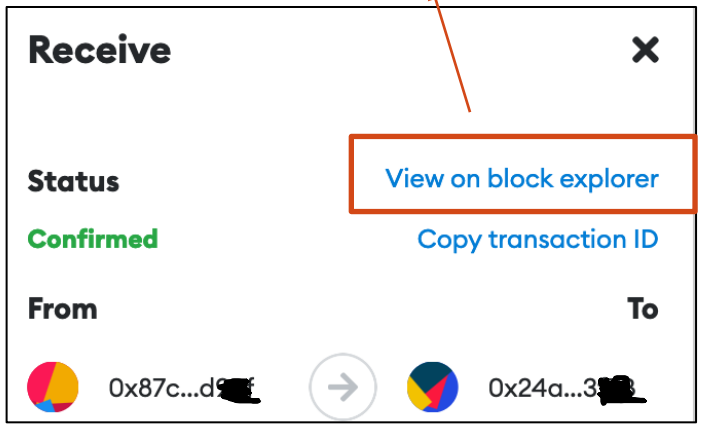
Who & how to comply?

A service fee paid to miners for processing your transactions on the blockchain

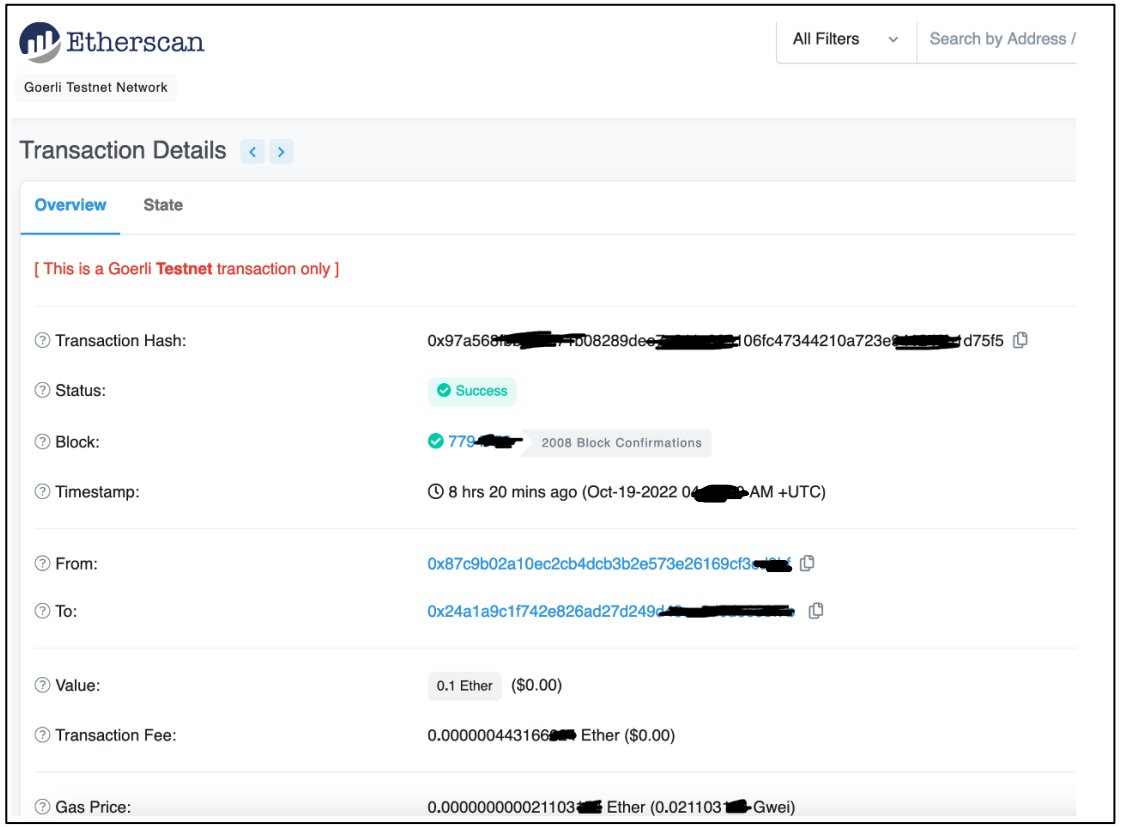
Implications for tax law: How should gas fees be taxed?

All the information you just saw is publicly accessible to everyone - not just to transacting parties

Click here



Your personal wallet



Publicly accessible website

Time for your lawyer brain – According to the IFC publication, which blockchain are we in?

This is where we are

Not all blockchains are as public as the one you just saw

BLOCKCHAIN TYPES		Read	Write	Commit	Example
Open	*Public permissionless*	Open to anyone	Anyone	Anyone*	Bitcoin, Ethereum
Open	*Public permissioned*	Open to anyone	Authorized participants	All or a subset of authorized participants	Sovrin
Closed	*Consortium*	Restricted to an authorized set of participants	Authorized participants	All or a subset of authorized participants	Multiple banks operating a shared ledger
Closed	*Private permissioned ("enterprise")*	Fully private or restricted to a limited set of authorized nodes	Network operator only	Network operator only	Internal bank ledger shared between parent company and subsidiaries

*Requires significant investment either in mining hardware (proof-of-work model) or cryptocurrency itself (proof-of-stake model)

Publication from the International Finance Corporation, World Bank Group

Wrapping up – what we covered today is at the forefront of regulatory debates

…permission-less blockchains might therefore be seen as a huge employer-owned mutual (e.g. John Lewis), that can propose motions and vote on the firm's detailed decision-making, while being unable to delegate decision-making to a board, nor even to recognize one another…

—OECD, "Antitrust and the Trust Machine"

Can distributed ledgers be squared with European data protection law?

—Study from European Parliament

…a permissionless system could…present substantial risk for a CBDC, such that a central bank would be unlikely to adopt…

—U.S. Treasury Dept., "The Future of Money and Payments"

Stay tuned for the next module

Thank you all for attending the workshop!