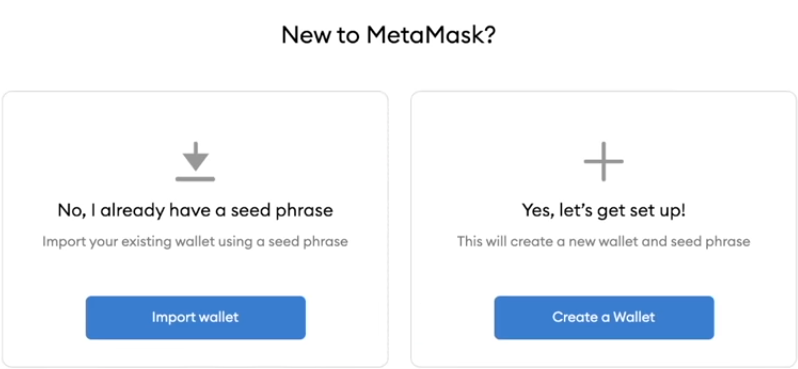
# 3 - Transakce Etherea na Blockchainu

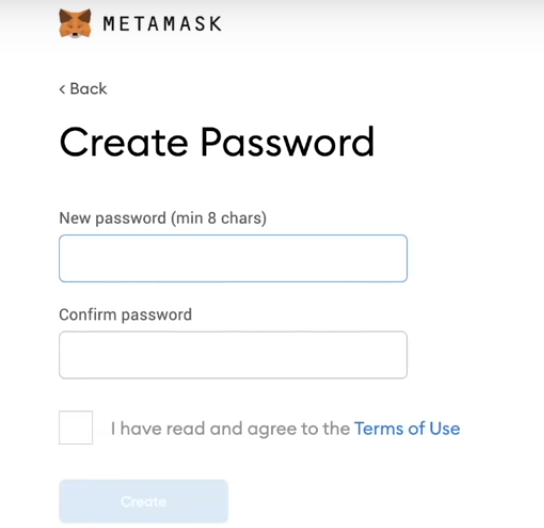
První věc, kterou budeme potřebovat, je peněženka ethereum. Využijeme **metamask**, protože je to jedna z nejpopulárnějších peněženek a jedna z nejjednodušších k použití. Stáhněte si peněženku - jedná se o malé rozšíření v pravém horním rohu prohlížeče. Tímto způsobem můžeme snadno zjistit obsah peněženky.

## Vytvoření peněženky

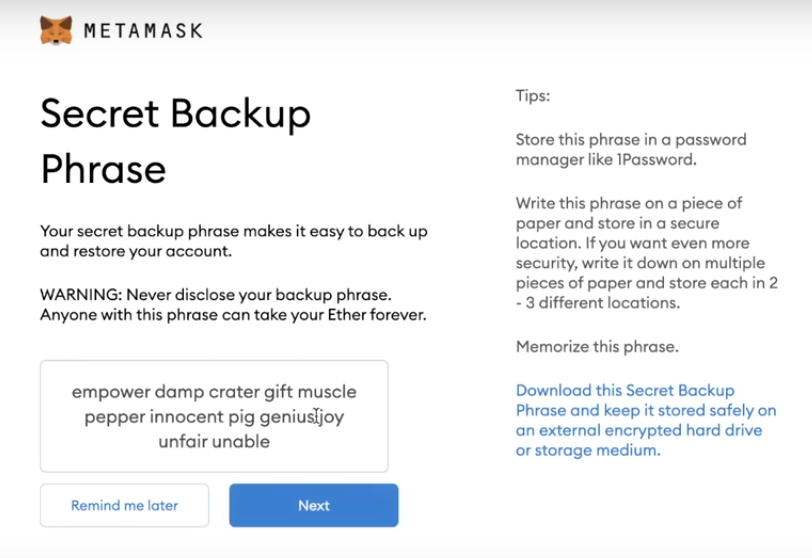
[](https://github.com/spo0ds/Journey-to-become-a-Blockchain-Engineer/blob/main/Images/Day1/a1.png)

Obrázek - Založení peněženky

Chystáme se vytvořit zbrusu novou peněženku -> stiskněte vytvořit peněženku (Create a Wallet). Pokud již peněženku máte, můžete ji importovat. Nyní zadáme heslo a ujistíme se, že je bezpečné.

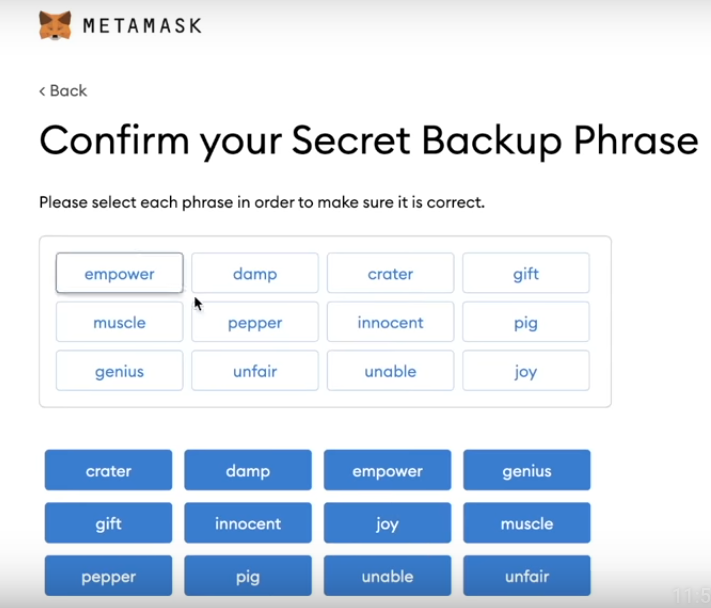
[](https://github.com/spo0ds/Journey-to-become-a-Blockchain-Engineer/blob/main/Images/Day1/a2.png)

Obrázek - Vytvoření hesla

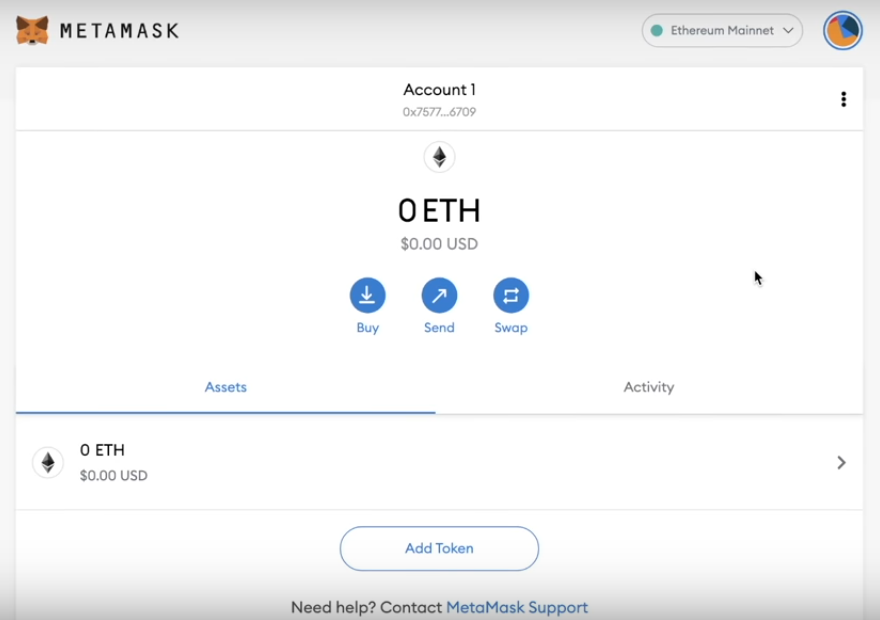
[](https://github.com/spo0ds/Journey-to-become-a-Blockchain-Engineer/blob/main/Images/Day1/a3.png)

Obrázek - Vygenerovaný seed

Jedná se pouze o demo (ukázku), ale pokud ukážete tuto tajnou frázi někomu jinému, budou mít přístup ke všem vašim prostředkům. Takže na vše, co budeme dále dělat, budeme používat falešné peníze (na testnetu).

[](https://github.com/spo0ds/Journey-to-become-a-Blockchain-Engineer/blob/main/Images/Day1/a4.png)

Obrázek 4 - Ověření seedu

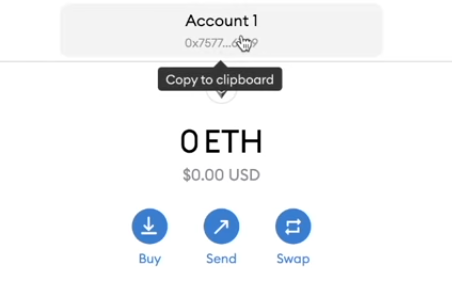
[](https://github.com/spo0ds/Journey-to-become-a-Blockchain-Engineer/blob/main/Images/Day1/a5.png)

Obrázek - Náhled do nově vytvořené ETH peněženky

Na obrázku výše můžeme vidět uživatelské rozhraní námi vytvořené peněženky.

Vytvořením nové peněženky se nám vygenerovaly 3 důležité položky:

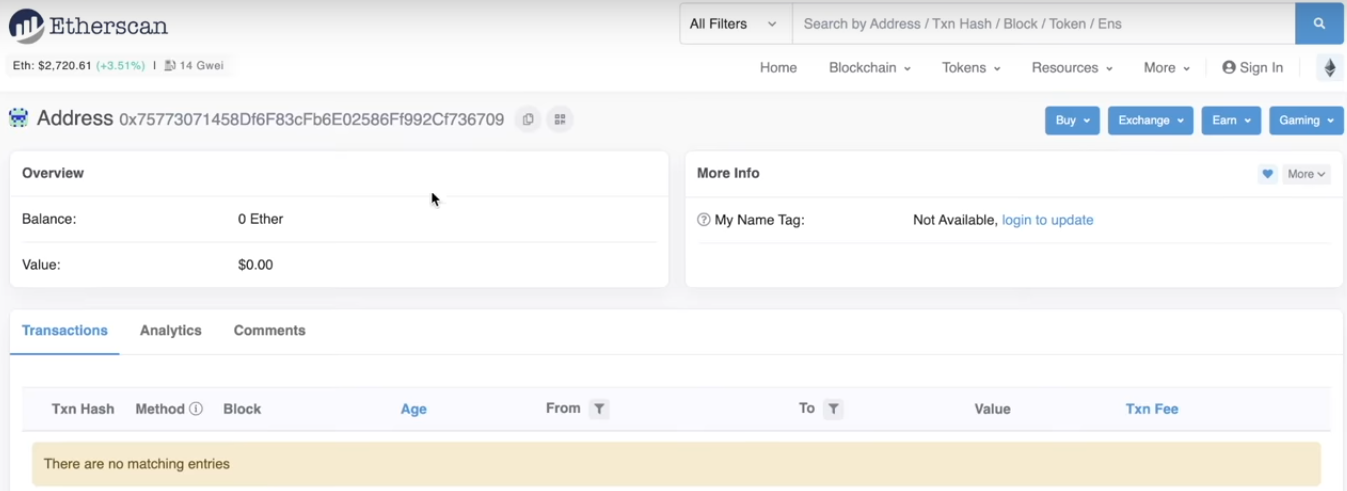
* **Seed** (nejdůležitější část – slouží k případné obnově peněženky)
* **Privátní klíč** (slouží k podpisu transakcí, které odešleme)
* **Veřejný klíč** (něco jako číslo účtu)

[](https://github.com/spo0ds/Journey-to-become-a-Blockchain-Engineer/blob/main/Images/Day1/a6.png)

Obrázek - Veřejný klíč naší peněženky

## Etherscan

Adresa našeho účtu, pro zobrazení detailů naší peněženky můžeme použít online nástroj etherscan.

[](https://github.com/spo0ds/Journey-to-become-a-Blockchain-Engineer/blob/main/Images/Day1/a7.png)

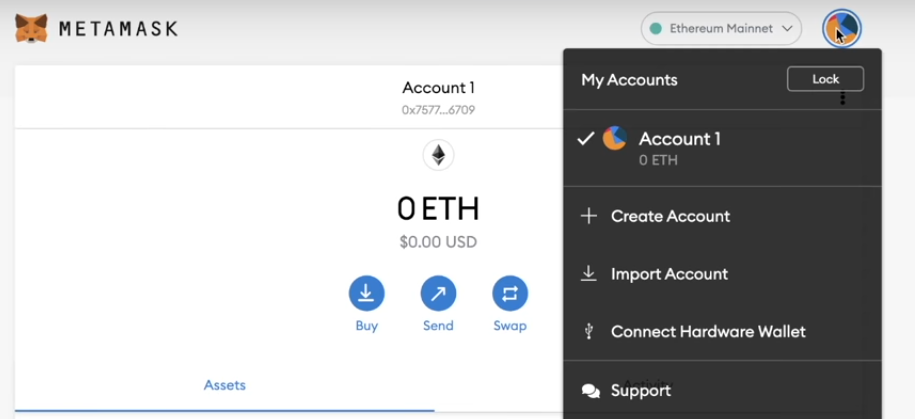
Obrázek - Rozhraní online nástroje Etherscan

Když se podíváme na adresu, kterou jsme právě vytvořili, vidíme, že nedošlo k žádným transakcím. Je prázdná. Má nulový počet ETH, má nulovou hodnotu dolarů. Výše uvedená adresa je jedinečná adresa, která představuje výhradně jediný účet, který jsme právě vytvořili.

## Vytvoření více účtů

Kliknutím na kruh v pravém horním rohu můžeme vytvořit další účet nebo změnit název vytvořeného účtu.

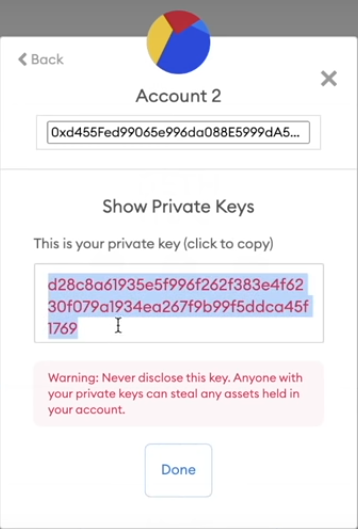
Nový účet bude mít jinou adresu účtu (veřejný klíč) – také naprosto unikátní.

[](https://github.com/spo0ds/Journey-to-become-a-Blockchain-Engineer/blob/main/Images/Day1/a8.png)

Obrázek - Vytvoření dalšího uživatele

## Seed, Privátní a veřejný klíč

Mnemotechnická pomůcka (seed), kterou jsme dostali, nám umožňuje vytvářet více účtů se stejnou mnemotechnickou pomůckou (seedem). Tudíž pokud by se někdo zmocnil našeho seedu, získal by přístup ke každému jednotlivému účtu, který byl kdy vytvořen pod tímto seedem. To je důvod, proč je zabezpečení vašeho seedu tak důležité, zejména pokud vytváříte více různých účtů. Každý účet má také jedinečný identifikátor. Adresa účtu je veřejná adresa. Existuje však také již zmiňovaný privátní klíč pro práci s tímto účtem. Můžeme jej zobrazit kliknutím na tři tečky, přejít na podrobnosti o účtu a exportovat privátní klíč.

[](https://github.com/spo0ds/Journey-to-become-a-Blockchain-Engineer/blob/main/Images/Day1/a9.png)

Obrázek - Zobrazení privátního klíče účtu

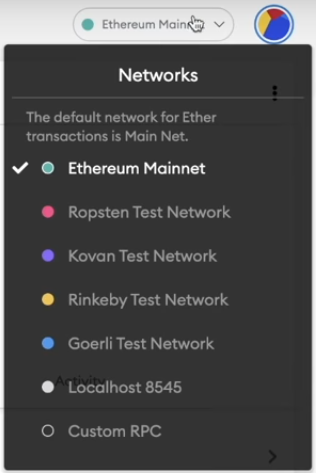
Jedná se o jediné heslo přidružené k tomuto účtu. Pokud někomu udělíte přístup k tomuto privátnímu klíči, bude mít přístup k účtu 2. Nebude mít však přístup k účtu 1, protože soukromý klíč účtu 2 je spojen pouze s účtem 2. Mnemotechnická pomůcka (seed) je však spojena se všemi účty.

To je důvod, proč když lidé říkají, že vaše klíče mají být uloženy na bezpečném místě, mají na mysli jak soukromé klíče, tak mnemotechnickou pomůcku (seed). Pokud ztratíte svůj soukromý klíč, ztratíte přístup k tomuto účtu. Pokud ztratíte mnemotechnickou pomůcku (seed), ztratíte přístup ke všem svým účtům.

## Mainnet & Testnet

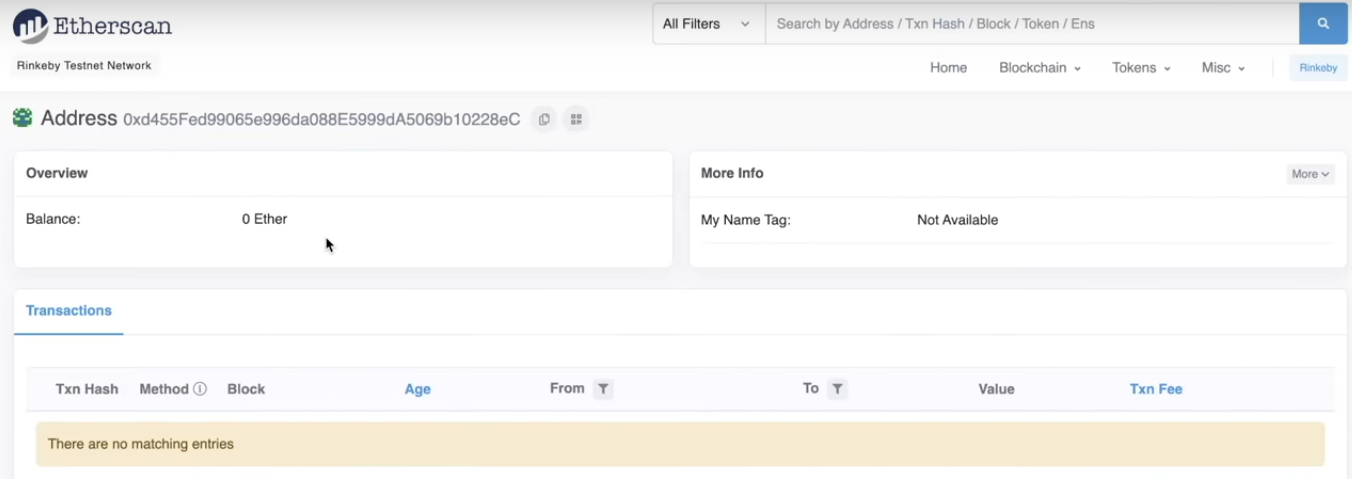
Co dalšího se děje v metamasku, je, že zde vidíme tuto sekci, která říká Ethereum mainnet. Pokud na něj klikneme, můžeme zde skutečně vidět spoustu dalších sítí.

Zobrazení Testnet sítí je třeba povolit v nastavení, defaultně se Vám nezobrazí.

[](https://github.com/spo0ds/Journey-to-become-a-Blockchain-Engineer/blob/main/Images/Day1/a10.png)

Obrázek - Zobrazení Testnet sítí

Když reálně vlastníte nějaké ETH (například si jej koupíte), pracujete na **ethereum mainnetu**. Když interagujete se smart contracty nebo defi, budete pracovat na mainnetu se skutečnou hodnotou. Protože je naším cílem se pouze seznámit s tím, jak transakce na blockchainu Ethera fungují, bohatě nám pro demonstraci budou stačit testovací sítě (testnets). Jedná se o sítě, které se podobají ethereu a fungují přesně stejným způsobem jako ethereum, ale nejsou se skutečnými penězi – slouží v reálném provozu pro testování aplikací. Můžeme jít dokonce do Rinkeby Etherscan a vidět Rinkeby Testnet Explorer, vyhledat naši adresu a zobrazit si detaily transakcí ve stejném rozsahu jako na mainnetu.

[](https://github.com/spo0ds/Journey-to-become-a-Blockchain-Engineer/blob/main/Images/Day1/a11.png)

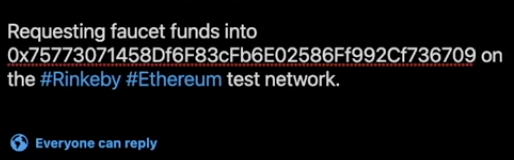
Obrázek - Zobrazení transakcí na Rinkeby Testnet Exploreru

## Jdeme provést první transakci

Naši první transakci provedeme na Rinkeby Testnetu - bude simulovat přesně to, jaké to je provést transakci na mainnetu etherea.

Přejdeme k aplikaci s názvem Rinkeby Faucet. To je místo, kde provedeme naši první transakci. Rinkeby bude jedním ze dvou testnetů, se kterými budeme skutečně pracovat. Další testovací síť, se kterou budeme pracovat, bude Coven. Je důležité vědět, jak přepínat mezi testovacími sítěmi a řetězci kompatibilními s evm, jelikož budeme pracovat s oběmi.

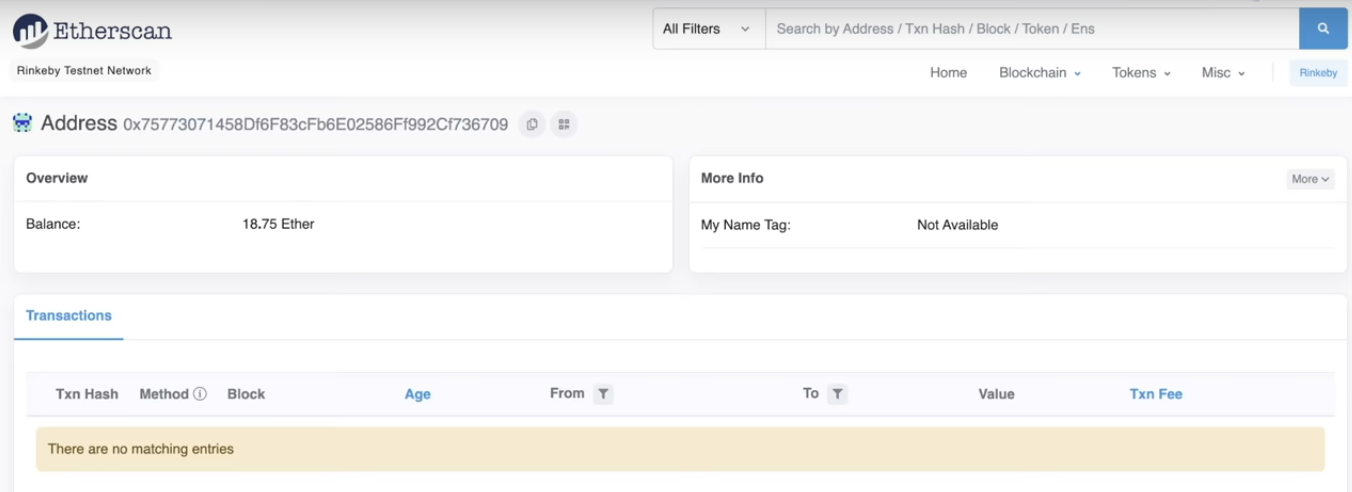
Faucet je testnet aplikace, která nám umožňuje zdarma test etherea. Abychom získali testnet ethereum s faucet.rinkeby.io, musíme ve skutečnosti zveřejnit tweet nebo příspěvek na Facebooku s tweetem.

[](https://github.com/spo0ds/Journey-to-become-a-Blockchain-Engineer/blob/main/Images/Day1/a12.png)

Obrázek - Tweet pro získání testovacích ETH

Nyní po tweetu zkopírujeme odkaz na tweet a umístíme jej do Rinkeby Faucet a stiskneme dejte mi ether (18.75 ether / 3 dny).

Pokud vyhledáme danou adresu účtu na Rinkeby Etherscan, vidíme, že zůstatek je 18,75 ETH.

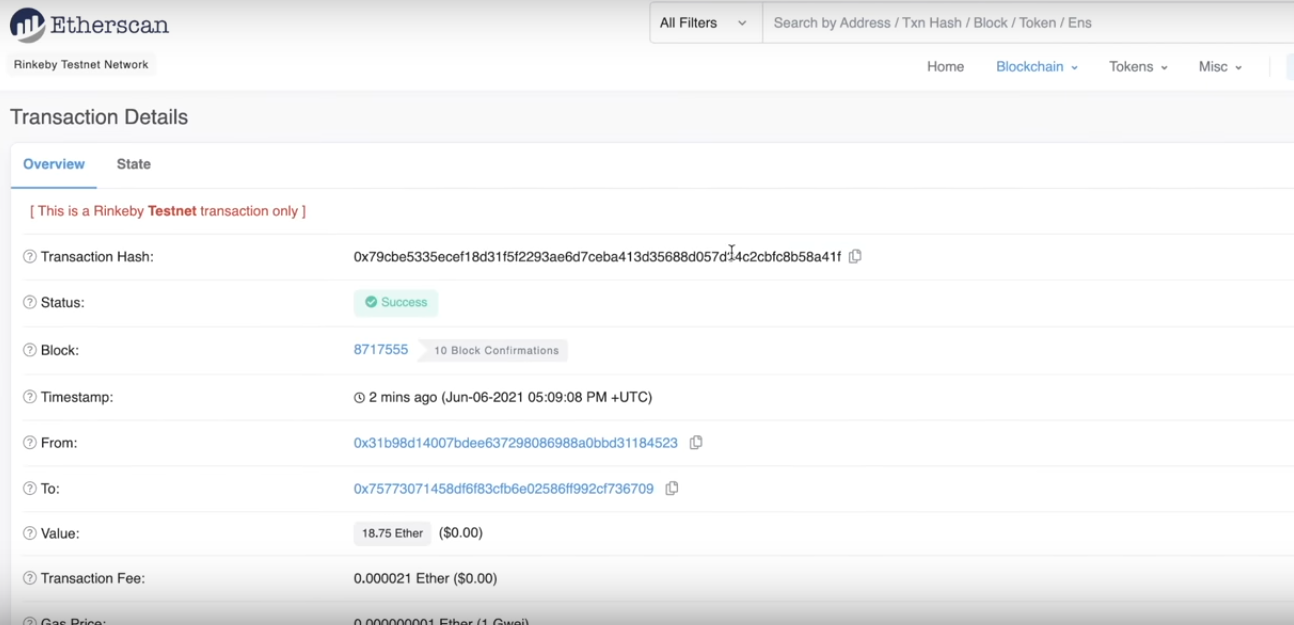
[](https://github.com/spo0ds/Journey-to-become-a-Blockchain-Engineer/blob/main/Images/Day1/a13.png)

Obrázek 13 - Přijetí první transakce v blockchainu

Právě jsme provedli naši první transakci. A pokud stránku Etherscan obnovíme, můžeme vidět, že jsme úspěšně provedli naši první transakci, respektive přijali jsme první transakci. Nějaký účet nám poslal 18.75 ether. Můžeme se dokonce podívat na podrobnosti transakce.

### Detaily transakce

Etherscan si můžeme představit jako Průzkumník bloků. Je to vlastně aplikace, která nám umožňuje snadno zobrazit podrobnosti o věcech, které se dějí na blockchainu. Můžeme vidět podrobnosti o transakci, kterou jsme provedli, a kdykoli pracujeme se smart cntracty, uvidíme je také v transakci podobné tomu, co uvidíme v detailu této transakce.

[](https://github.com/spo0ds/Journey-to-become-a-Blockchain-Engineer/blob/main/Images/Day1/a14.png)

Obrázek 14 - Detaily transakce

Nalezneme zde řadu informací o transakci. Vidíme jedinečnou hash transakce. Tato hodnota hash neboli jedinečný identifikátor identifikuje danou transakci jako klíč k této transakce. Dále vidíme číslo bloku, časovou známku, adresy uživatelů a poplatky za transakci – Gas poplatky.

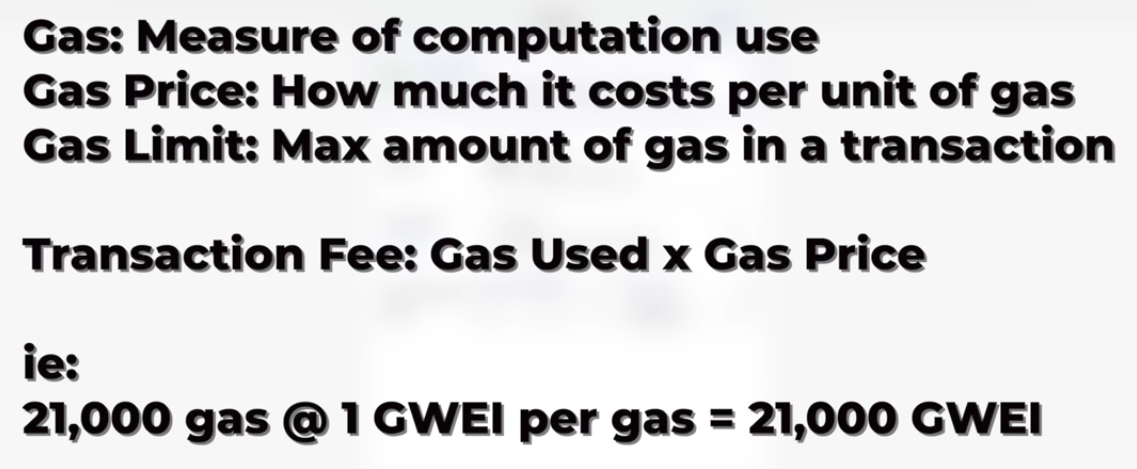
### Gas poplatky (jeho limity, cena) a transakční poplatky

Gas odkazuje na poplatek placený provozovatelům uzlů za úspěšné zahrnutí transakce do blockchainu.

Pro odeslání nějakého etherea nebo provedení jakéhokoli typu transakce, ve skutečnosti musíte zaplatit trochu etherea, abyste tuto transakci mohli provést. Kdykoli uděláme něco na blockchainu, stojí to Gas.

Pokud uděláme něco, co by blockchain potřeboval hodně energie, bude to stát více Gasu. Takže když pošlu jednu transakci, bude to stát například 21000 Gasu. Pokud bych však poslal transakci, která by volala funkci smart contractu a udělala celou řadu dalších věcí, stálo by to více Gasu.

Vidíme zde, že ten, kdo nám ETH poslal, musel rovněž zaplatit blockchainovým těžařům nebo validátorům blockchainu trochu etherea, aby zahrnul naši transakci do blockchainu.

[](https://github.com/spo0ds/Journey-to-become-a-Blockchain-Engineer/blob/main/Images/Day1/a15.png)

Obrázek 15 - Vysvětlení Gasu, ceny a limitu

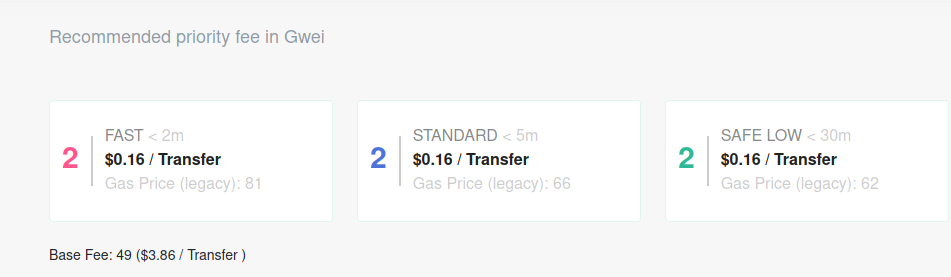
### Gas vs Cena Gasu vs Gas Limit vs Transakční poplatek

Proč bychom někdy chtěli platit vyšší cenu plynu? Proč mám vůbec možnost platit více za transakci?

Blockchain může zpracovat pouze určitý počet transakcí najednou a uzly blockchainu mohou zpracovat pouze určité množství najednou. Takže když provedu transakci, uzel se musí rozhodnout, proč by měl vůbec zahrnout mou transakci do bloku. Pokud existuje spousta lidí, kteří chtějí tyto transakce provést, pak budou uzly vysoce motivovány k výběru transakcí, které jim poskytnou vysokou cenu - která jim dá více ETH za zahrnutí této transakce.

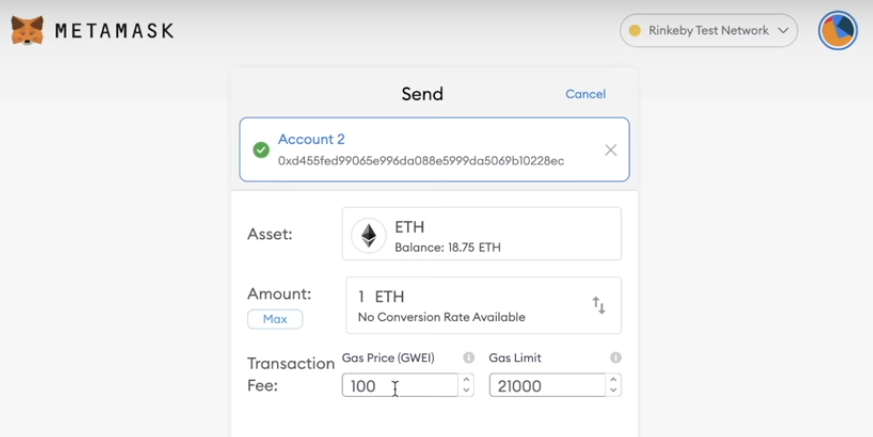
### Gas estimator

Na stránce ethgasstation.info můžeme získat aktuální odhad Gasu blockchainu.

[](https://github.com/spo0ds/Journey-to-become-a-Blockchain-Engineer/blob/main/Images/Day1/a16.png)

V současné době říká, že pokud chcete svou transakci získat hned, bude vás to stát 81 gwei. Pokud to chcete dostat za méně než 5 minut, bude vás poplatek stát asi 62 gwei.

Takže cena Gasu etherea kolísá s tím, kolik lidí ho používá.

[](https://github.com/spo0ds/Journey-to-become-a-Blockchain-Engineer/blob/main/Images/Day1/a17.png)

Obrázek 16 - Příklad stanovení transakčního poplatku v transakci

Tudíž obvykle, když nastavujete cenu plynu v transakci, můžete se podívat na Gas estimator, abyste viděli cenu na základě vašich potřeb, ale vše závisí na tom, kolik lidí chce pracovat s tímto blockchainem současně.

Důvodem, proč tyto ceny Gasu existují, je to, že uzly mohou do bloku vložit pouze tolik transakcí, takže jsou vysoce motivovány k zadávání transakcí, které jim poskytnou vyšší poplatek. Takže v době, kdy chce mnoho lidí použít k transakci blockchain, budou ceny velmi vysoké a když jen velmi málo lidí používá blockchain, ceny budou velmi nízké...

S touto trochou informací nyní víte, jak komunikovat s blockchainy a komunikovat s protokolem ethereum.