



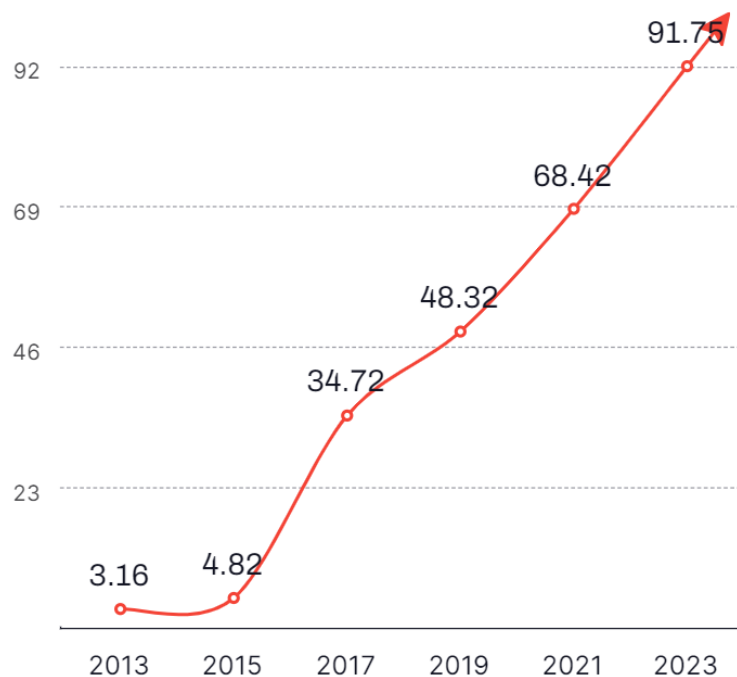
Bezpečné zálohování seedu kryptopeněženek

Komplexní průvodce k dosažení obchodních cílů



Počet krypto peněženek

Počet všech peněženek registrovaných na blockchainech do konce roku 2023 v milionech ks



Zdroj: GlobeNewswire



Problém

Ztráta kryptoměn kvůli nezabezpečeným seedům

Žádná záloha

To je ta nejhorší varianta, obvykle podpořená naivní omluvou: Mám to v mobilu, nemůže se nic stát, až budu mít chvíli čas tak to opíšu.

Focení seedu, kopie do emailu

Dnes jsou speciální viry, které dělají pouze to, že hledají seedy v textech a obrázcích v mobilech, počítačích a cloudech.



Papír hoří, inkoust bledne

Mnoho uživatelů zapisuje seedy do sešitu, knihy nebo prostě jen na papír k peněžence. Není to špatně, ale trvanlivost tohoto záznamu může být krátká.

Raznice, tesání do kamene a DIY

No úplně středověk, téměř nezničitelné, trvanlivé a odolné vůči nějším vlivům. Bohužel také často nepřenosné, komplikované a nedostupné.





Nejznámější ztráty peněženek.

1 BTC = 70 000 USD

Satoshi Nakamoto **70 000 000 000 USD**

Pseudonymní tvůrce bitcoinu vlastní 1 000 000 bitcoinů, které nebyly přesunuty od doby, kdy byly vytěženy. Nikdo neví kdo Satoshi byl a co se s ním stalo.

Mt Gox **5 600 000 000 USD**

Peněženka obsahuje přes 80 000 bitcoinů a nikdy z ní nebyla utracena jediná mince. Jde o bitcoiny ukradené při aféře Mt Gox.

Stefan Thomas **490 140 000 USD**

Programátor, který ztratil seed ke své peněžence obsahující asi 7 002 bitcoinů. Na začátku roku 2021 provedl Thomas osm pokusů z 10 možných a bez úspěchu.

James Howells **560 000 000 USD**

IT pracovník, omylem vyhodil pevný disk obsahující seed k 8 000 bitcoinům. Navzdory četným pokusům se mu nepodařilo najít pevný disk na místní skládce.

Gerald Cotton **280 000 000 USD**

Generální ředitel společnosti QuadrigaCX, nečekaně zemřel v roce 2018, když byl na lůžkách v Indii. Pamatoval si seed k 4 000 bitcoinům.

4 000 000 BTC **280 miliard dolarů, tj. cca 20% BTC**

Se považuje za ztracených z důvodů ztráty seedu, smrti nebo nikdy nebyl proveden žádný pohyb na peněžence.



Řešení

Šifrování seedu a jeho uložení na bezpečné a dostupné místo

01

Bezpečné místo

Nejdůvěryhodnějším a nejbezpečnějším místem v současné době je samotný blockchain.

02

Absolutní dostupnost

Blockchain je dostupný 24 hodin denně, 7 dní v týdnu a odkudkoliv na světě.

03

Vernamova šifra

Nerozlučitelné šifrování odolné jakýmkoliv pokusům o rozluštění včetně hrubé síly.

04

Šifrovací hardware

Překvapivě jednoduché zařízení a software pro šifrování a dešifrování seedů.

05

Opensource

Aby bylo dosaženo plné důvěry je veškerý SW k dispozici pro kontrolu.

06

Webová aplikace

Přístup k vlastním seedům, jejich správa a hlavně zdroj příjmů z poplatků.



Výběr šifry a blockchainu

Co, proč a jak společně tvoří náš projekt

Výsledkem šifrování je náhodný text. Opakované šifrování stejného textu vede vždy k unikátnímu řetězci a proto ho nelze odlišit od libovolného náhodného řetězce.

Blockchain

Moderní blockchain s marketcapem v hodnotě 90 miliard USD ho řadí na 3 místo hned za Bitcoin a Ethereum. Vyznačuje se vysokou propustností a nízkými poplatky.

Příjem

Veškeré informace zapsané do blockchainu jsou dostupné kdykoliv a z libovolného místa na Zemi. Právě veřejná dostupnost dělá z našeho projektu dokonalý nástroj.

Vernamova šifra

Nejbezpečnější místo pro ukládání informací díky decentralizaci a kryptografické ochraně. Kromě transakcí samotných může obsahovat také další údaje.

Solana

Každá transakce na blockchainu je zpoplatněna. Zapsání zašifrovaného seedu na blockchain je podmíněno zaplacením příslušného poplatku.

Dostupnost

Co je seed

A jak vypadá šifra

Kryptopeněženka



To je něco jako číslo účtu. Každá peněženka má jedinečné číslo, na které jsou doručeny jednotlivé transakce stejně jako pohyby na účtu v bance.

Číslo peněženky vypadá takhle:

tb1qz3u3hw9qzvrvruuxdyrnjquv7280t8kva36de

Seed



Je lidsky čitelný kód krypto peněženky. Skládá se ze 12 nebo 24 slov, které reprezentují čísla.

Seed slouží k obnovení ztracené peněženky.

Vypadá takto:

snail speed examine training product leaf milk expand program sales line offer

Zašifrovaný seed



Výsledkem šifrování pomocí našeho HW je náhodný text. Je to výsledek několika kroků, které lze reverzně provést pouze na našem zařízení.

Výsledkem šifrování seedu je:

X762788V_dSUAVsbKcXEAORwoXR\`ENAmSSEELESEBETVEJBOJjDALKIRPN{EJUNEMER{AM



Nekompromisní bezpečnost

Nikomu nechcete dát přístup k vašemu účtu!

Offline zařízení

Mezi Seederem a počítačem neprobíhá žádná komunikace.

Seeder může pracovat zcela offline.



Seed se neukládá

Seeder neobsahuje žádný ze zadaných seedů, jeho práce je pouze zašifrovat nebo dešifrovat seed.



Odposlech nebo virus?

Bez obav, přenos dat je formou QR kódů přes kameru, tedy mimo propojení obou zařízení.

Alternativně lze použít USB nebo BT.



Ztratil jsem Seeder

Nic se neděje. Pro zloděje je tvůj vlastní Seeder nepoužitelný a ty si můžeš koupit nový.



Dešifrování cizích seedů

Tak to bohužel a naštěstí nelze.



Kolik seedů lze zašifrovat?

Počet zašifrovaných seedů není nijak omezen. Seeder zašifruje stejně kvalitně jakýkoliv vložený seed.





Ilustrační foto.

Jaký bude Seeder?

Bude to něco jako malý smartphone.

4" palcový display.

Kamera pro čtení QR kódů.

Čtečka otisků prstů.

USB, BT.





Porozumění našim zákazníkům

Kdo jsou naši klienti?



DEX uživatel

Má desítky peněženek, pro každý projekt jinou, peněženky mají minimální zůstatky určené pouze na transfery a bridge.



Krypto trader

Má peněženky na většině velkých blockchainech, jednu nebo dvě hlavní s pro KYC a NonKYC svět. Přesouvá peníze mezi burzami a fiatem.



Hodler

Krypto nadšenec s několika málo peněženkami na kterých má obvykle Bitcoin a Ethereum, které hromadí s úmyslem nikdy neprodat.



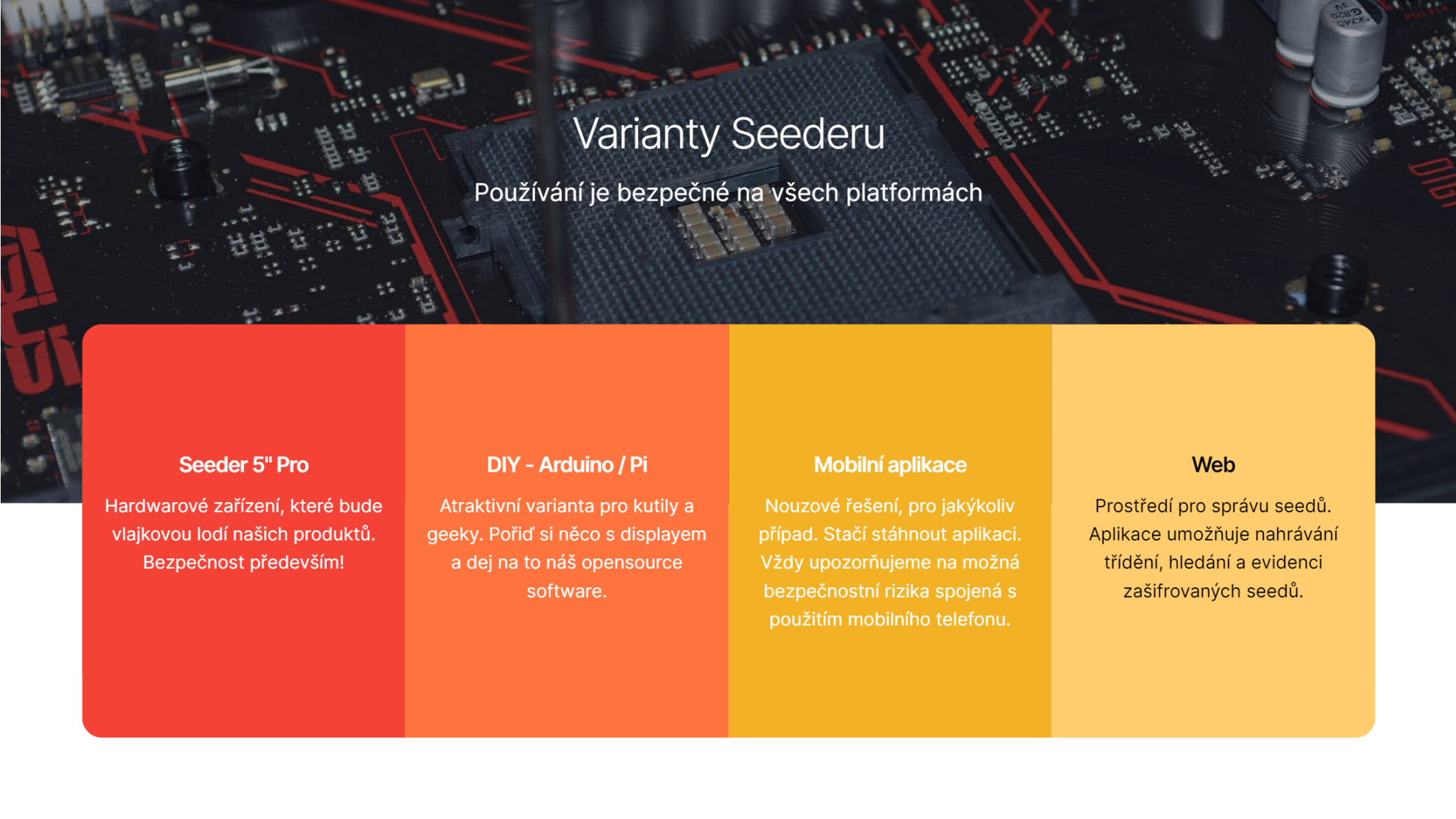
Airdroper

Speciální skupina uživatelů krypta, která vlastní stovky peněženek na všech možných projektech. Živí se tím, že pomáhá rozjíždět nové projekty a očekává za to odměnu v budoucnosti.



Miner - Nodař

Programátor, který se podílí na bezpečnosti blockchainů, provozuje serverovou infrastrukturu obvykle se účastní několika projektů zároveň. Zpracovává nebo validuje jednotlivé transakce.



Varianty Seederu

Používání je bezpečné na všech platformách

Seeder 5" Pro

Hardwarové zařízení, které bude vlajkovou lodí našich produktů.

Bezpečnost především!

DIY - Arduino / Pi

Atraktivní varianta pro kutily a geeky. Poříd' si něco s displayem a dej na to náš opensource software.

Mobilní aplikace

Nouzové řešení, pro jakýkoliv případ. Stačí stáhnout aplikaci. Vždy upozorňujeme na možná bezpečnostní rizika spojená s použitím mobilního telefonu.

Web

Prostředí pro správu seedů. Aplikace umožňuje nahrávání třídění, hledání a evidenci zašifrovaných seedů.

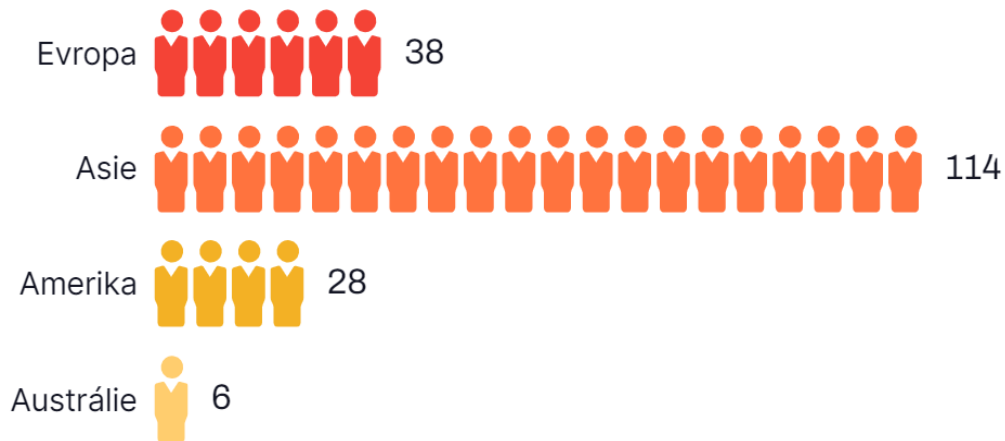


Počet uživatelů krypta, DeFi a Web3

Toto jsou naši zákazníci



Počet uživatelů ve světadílech v roce 2023 v milionech



Zdroj: Companies Market Cap



Finanční plán

Náklady a příjmy



Náklady - Softwarová platforma a provoz

Dlouhodobý vývoj, implementace nových možností a nápadů, rozšiřování služeb. Vývoj platformy, pravidelné upgrady, další lidské zdroje, propagaci a firemní režii odhadujeme na 60% příjmů



Náklady - Provoz vlastního nodu a zálohování

Pro navýšení bezpečnosti uložených dat je základním předpokladem plnohodnotná záloha a provoz vlastního nodu na validaci transakcí. Provoz nodu a hw náročnost by neměla přesáhnout 5% příjmů



Příjmy - Prodej Seederu

Cenu bychom rádi udrželi pod 100 USD. Příjmy z prodeje Seederu by měly být ve výši 30%



Příjmy - Služby ukládání seedu

Za uložení seedu budeme chtít odměnu podle finančního plánu uživatele a podle množství uložených seedů ve výši 5-10 USD Příjmy z těchto služeb odhadujeme na 65%



Příjmy - Udržovací poplatky

Udržovací roční / měsíční poplatky pro přístup k účtu a navázaných služeb. Příjmy z poplatků budou ve výši 5%

Prodejní kanály

Jak dosáhnout prodejních cílů



Výstavy, konference a krypto eventy

Po celém světě se pravidelně pořádají konference, eventy a představení nových technologií v oblasti web3, DeFi a krypta.



Influenceři

Krypto samotné a jeho propagaci šíří převážně influenceři. Na sociálních sítích existuje řada specializovaných kanálů a nadšených propagátorů kryptosvěta.



Přímý prodej

Náš hardware chceme distribuovat formou prodeje přes náš eshop přímo koncovým uživatelům. Od mobilní aplikace, přes DIY prototyp, až po designové kousky.



Velkoobchod

Kryptopeněženky se dnes běžně prodávají v internetových obchodech jako je Alza, Amazon, Ebay, Alibaba... Tyto distribuční kanály jsou také k dispozici.



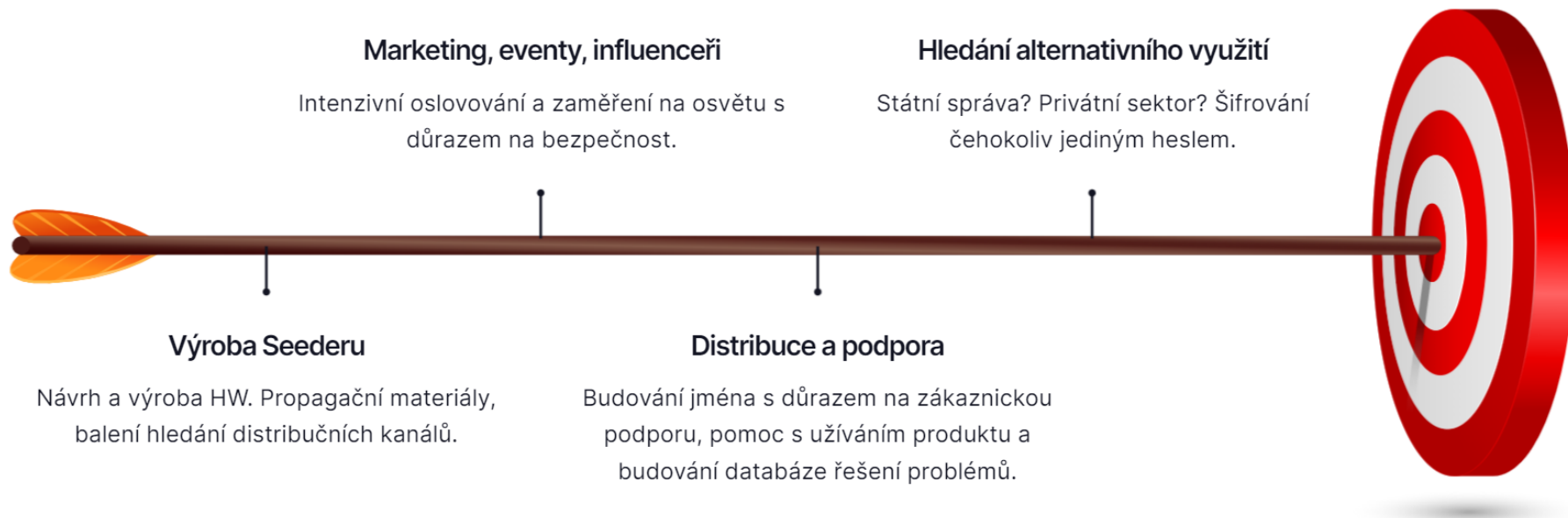
Služby

Za každé uložení nového seedu bude nutné zaplatit poplatek podle zvoleného obchodního plánu každého uživatele. Tyto poplatky budou nedílnou součástí příjmů.



Cesta k cíli a budoucnost

Společně to dokážeme



Konkurence

Různé způsoby uchování seedu



Náš tým

Ruku na to...



Mirek Šalamon

Programátor HW, kryptominer a cestovatel.
Má rodinu a 7 letého kluka.



Adam Hrubý

Programátor SW, správce webů, nadšenec
do inovací a kryptohodler.



Hledáme pomoc

Kolik to bude stát

Výroba

Víme co chceme, máme konkrétní představu o designu zařízení a dokážeme ho vyrobit. Potřebujeme nakoupit díly na prvních 3000 kusů.

Marketing

Hledáme pomoc v oblasti marketingu, známe prodejní kanály, chceme připravit úspěšnou reklamní kampaň a realizovat prezentace na kryptoeventech.

04

02

03

01

Zkušenosti

Uvítáme zkušenosti, informace, mentoring a kontakty v oblasti globálního prodeje, skladování a distribuce našeho výrobku a služeb.

Peníze

Hledáme finance na provoz, lidské zdroje, prostory, marketing, díly a další nezbytné věci spojené se startem nové společnosti.



Slovníček pojmů

Abychom si rozuměli

- Decentralizace - prostředí, které má provozní kapacity a řízení rozložené mezi velké množství jednotlivých entit. Na rozdíl od centralizace, kde je uplatněná vertikální struktura řízení a rozhodování je jedinou, centrální, entitou.
- Fiat - peníze, které běžně používáme, Koruny, Dolary, Eura.
- Krypto, kryptoměna - decentralizované, alternativní peníze.
- DeFi - Decentralizované Finance, ekosystém, ve kterém lze používat běžné finanční nástroje v krypto světě. Půjčky, pojištění, směnárny...
- DEX - Decentralizovaná burza, místo kde se obchodují kryptoměny.
- Hodler - držitel kryptoměny, který ji nakupuje s úmyslem neprodat.
- Airdrop - odměna za nezištnou pomoc při rozjezdu nového projektu.
- Blockchain - tzv. účetní kniha, do které jsou zapsané všechny transakce. Nedá se změnit a je veřejně přístupná.
- Miner - Nodař - počítač nebo osoba, která se živí zapisováním transakcí do blockchainu a dostává za to odměnu.
- Web3 - decentralizovaný internet postavený na decentralizovaných



seeder



Děkujeme za Váš čas...

Máme odpověď na všechny Vaše otázky...

