ജലവൈദ്യുത പദ്ധതി:
ബ്ലോക്ക്ചൈനിലുള്ള പൊതു പ്രാമാണീകരണം

ജനുവരി 2018

ഉള്ളടക്ക പട്ടിക

സംഗ്രഹം

ഹൈഡ്രോ: എട്ടിമോളജി - പുരാതന ഗ്രീക്ക് ὑδρο- (ഹുഡ്രോ-), ὕδωρ (húdōr, "ജലം")

അപേക്ഷ, പ്രമാണ സുരക്ഷ, ഐഡന്റിറ്റി മാനേജ്മെന്റ്, ഇടപാടുകൾ, കൃത്രിമ ഇന്റലിജൻസ് എന്നിവ വർദ്ധിപ്പിക്കുന്നതിനായി ഒരു പൊതു ബ്ലോക്ക് ചില്ലിന്റെ സുതാര്യവും സുതാര്യവുമായ ഡൈനാമിക്സുകളെ ഏകോപിപ്പിക്കുന്നതിനും, നിലവിലുള്ളതിനും പുതിയതും നിലവിലുള്ളതുമായ സ്വകാര്യ സംവിധാനങ്ങൾ ഹൈഡ്രോ സജ്ജമാക്കുന്നു.

പൊതുജനങ്ങൾക്ക് സുരക്ഷ ഉറപ്പാക്കാൻ ഹൈഡ്രോ പബ്ളിക് ബ്ലോക്കിനൊപ്പം എപിഐകൾ പോലെയുള്ള സ്വകാര്യ സംവിധാനങ്ങൾക്ക് ഒരു കേസ് നിർമ്മിക്കും.

നിർദിഷ്ട ടെക്നോളജിക്ക് "റെയിൻ ഡിപ്റ്റ്" എന്ന് വിളിക്കപ്പെടുന്നു - സ്വകാര്യ സംവിധാനത്തെ പൊതുവായി ഉറപ്പാക്കുന്ന ഒരു സ്മാർട്ട് കോൺട്രാക്റ്റിലൂടെ നടത്തുന്ന ട്രാൻസാക്ഷൻ, കൂടാതെ നിലവിലുള്ള സ്വകാര്യ പ്രാമാണീകരണ രീതികൾ പൂർത്തീകരിക്കും. ഹാക്കിംഗ്, ഉന്മൂലനം എന്നിവയിൽ നിന്ന് കൂടുതൽ അപകടസാധ്യതയുള്ള സെൻസിറ്റീവ് സാമ്പത്തിക വിവരങ്ങൾക്ക് കൂടുതൽ സുരക്ഷ നൽകാനാണ് ഈ സാങ്കേതിക വിദ്യ ഉദ്ദേശിക്കുന്നത്.

`Hydro Raindrop-` ന്റെ പ്രാരംഭ നടപ്പാക്കൽ `Hydrogen API Platform-` ൽ നടത്തപ്പെടുന്നു. പ്രോട്ടോടൈപ്പ്, ബിൽഡ്, ടെസ്റ്റ്, ആധുനിക സാങ്കേതികവിദ്യാ പ്ലാറ്റ്ഫോമുകളും ഉൽപ്പന്നങ്ങളും വിന്യസിക്കുന്നതിന് ആഗോളതലത്തിൽ സംരംഭകരുടെയും ഡവലപ്പർമാരുടെയും ഈ മോഡുലർ സെറ്റ് ലഭ്യമാണ്.

ഹൈഡ്രോ റെയിൻഡ്രോപ്പ്, ലോക ഡെവലപ്പർ കമ്യൂണിറ്റിയുടെ ഓപ്പൺ സോഴ്സ് സോഫ്റ്റ്വെയറിലേക്ക് ലഭ്യമാക്കും, ഡവലപ്പർമാർ ഏതെങ്കിലും `REST API` ഉപയോഗിച്ച് ഹൈഡ്രോ റെയിൻഡ്രോപ്പ് സമന്വയിപ്പിക്കാൻ അനുവദിക്കും.

ബ്ലോക്ക്ചെയിനും & Ethereum

എഥേറം നെറ്റ്വർക്കിൽ ഹൈഡ്രോ പ്രവർത്തിക്കുന്നു. പ്രോജക്ടിൽ കൂടുതൽ വിശദാംശങ്ങൾ നൽകുന്നതിന് മുമ്പ്, ബ്ളോക്കിൻ, എടെരേയം എന്നിവയെ കുറിച്ചുള്ള ചില അടിസ്ഥാന ആശയങ്ങൾ മനസ്സിലാക്കേണ്ടത് വളരെ പ്രധാനമാണ്.

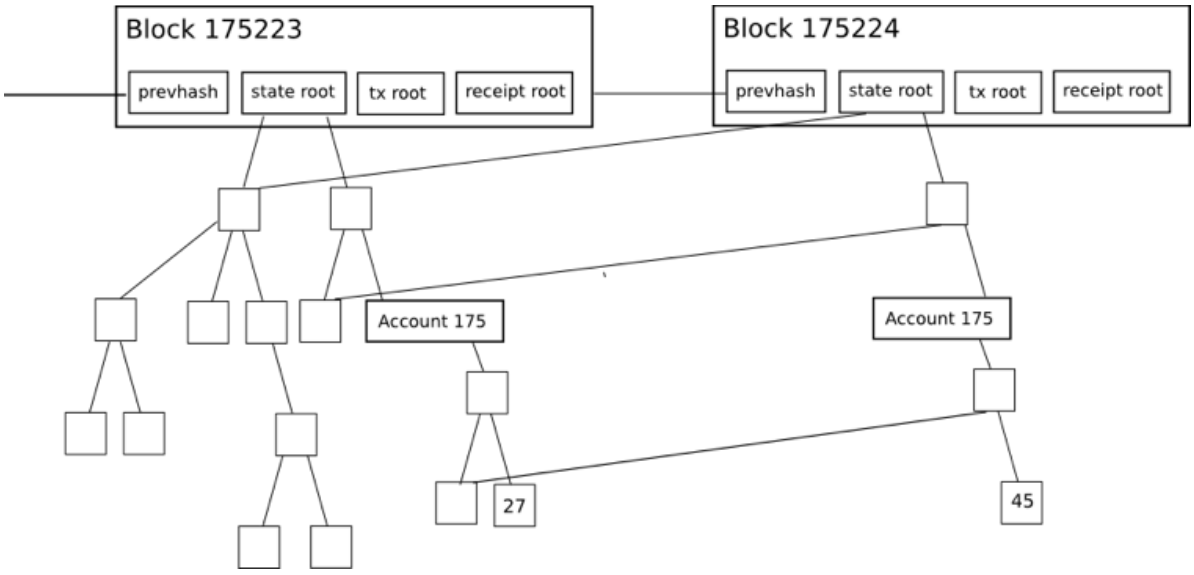
എവെരെറിലുള്ള ബിൽഡിംഗ്

ആപ്പിൾ ഐഒഎസ് പ്ലാറ്റ്ഫോമിന് മുകളിലുള്ള സ്പിഫറും മറ്റ് ഉപകരണങ്ങളും ഉപയോഗിച്ച് സ്നാപ്പ് ചാറ്റ് പോലുള്ള ആപ്ളിക്കേഷനുകൾ നിർമ്മിച്ചതുപോലെ, `Ethereum-` ൽ മുകളിലായി ആപ്ലിക്കേഷനുകൾ ബ്ലോക്കിന് ഉപയോഗിക്കാനാകും. സ്നാപ്പ് ഇൻകോ. ഐഒഎസ് നിർമ്മാണത്തിന് ആവശ്യമില്ല, ഗെയിം മാറുന്ന സോഷ്യൽ മീഡിയ ആപ്ലിക്കേഷൻ തുടങ്ങുന്നതിന് ഇത് അടിസ്ഥാനമായി ഉപയോഗിച്ചു.

പ്രോജക്റ്റ് ഹൈഡ്രോ സമാനമാണ്. ബ്ളോക്കിൻ സാങ്കേതികവിദ്യ കൂടുതൽ വേഗത്തിലാക്കുന്നതിന് ആഗോളതലത്തിൽ പ്രവർത്തിക്കുന്ന ആയിരക്കണക്കിന് ഡവലപ്പർമാരെ ഇത് ആശ്രയിക്കുന്നു, കൂടുതൽ ശക്തവും കൂടുതൽ കാര്യക്ഷമവുമാണ്. ബ്ലോക്ക്ച്ചെയ്ന് ടെക്നോളജി ഉപയോഗിച്ചുള്ള പ്രോഡക്ട്-ഫോക്കസ് പരസ്പര പ്രവർത്തനങ്ങൾ വികസിപ്പിച്ചുകൊണ്ട് ഹൈഡ്രോ നിരന്തരം മെച്ചപ്പെടുത്തുന്നു.

മെർക്കുൾ ട്രീസ്

കാര്യക്ഷമമായ ഡേറ്റാ വെരിഫിക്കേഷനായി വിതരണ സിസ്റ്റങ്ങളിൽ മെർക്കുൾ മരങ്ങൾ ഉപയോഗിക്കുന്നു. അവർ ഫുൾഫയലുകൾക്ക് പകരം ഹാഷുകൾ ഉപയോഗിക്കുന്നത് കൊണ്ട് കാര്യക്ഷമമാണ്. ഫയലുകളുടെ എൻകോഡിങ്ങിന്റെ വഴികളാണ് ഹാഷ്സ്, യഥാർത്ഥ ഫയൽ തന്നെ വളരെ ചെറുതാണ്.



`Ethereum-` ൽ ഉള്ള എല്ലാ ബ്ലോക്ക് ഹെഡററുകളും ട്രാൻസാക്ഷൻസ്, രസീതികൾ, സ്റ്റേറ്റുകൾക്കായി മൂന്ന് മെർക്കുൾ ട്രീസ് ഉണ്ട്: ഉറവിടം: ഇർറെറിയത്തിൽ മെർക്കുലിംഗ്; വിറ്റാലിക് ബ്യൂറെറിൻ, എറ്റെരെം സ്ഥാപകൻ

ചോദ്യങ്ങൾക്കുള്ള ലളിതമായ ക്ലയന്റ് ലഭിക്കാൻ ഇത് എളുപ്പമാക്കുന്നു, ഉദാഹരണത്തിന്:

- ഈ അക്കൗണ്ട് നിലവിലുണ്ടോ?
- നിലവിലെ ബാലൻസ് എന്താണ്?
- ഈ ഇടപാട് ഒരു പ്രത്യേക ബ്ലോക്കിൽ ഉൾപ്പെട്ടിട്ടുണ്ടോ?
- ഈ വിലാസത്തിൽ ഒരു പ്രത്യേക പരിപാടി നടന്നിട്ടുണ്ടോ?

സ്മാർട്ട് കോൺട്രാക്റ്റുകൾ

Ethereum, മറ്റ് ബ്ളോക്ക്ചെയിൻ നെറ്റ്വർക്കുകൾ എന്നിവയിലൂടെ ഒരു സുപ്രധാന ആശയം സ്മാർട്ട് കോൺട്രാറ്റിന്റെ ഭാഗമാണ്. ഒന്നിലധികം കക്ഷികൾ ആശയവിനിമയം നടത്താനാകുന്ന കോഡുകളുടെ സ്വയം നടപ്പാക്കൽ ബ്ലോക്കുകളാണ്. വിശ്വസനീയരായ ഇടനിലക്കാരെ ആവശ്യമില്ല. പരമ്പരാഗത പേപ്പർ കരാർ ലെ നിയമപരമായ clauss പോലെ ഒരു സ്മാർട്ട് കരാർ കോഡ് കാണാം, എന്നാൽ കൂടുതൽ വിപുലമായ പ്രവർത്തനം നേടാൻ കഴിയും. കരാറുകൾക്കു ചട്ടങ്ങൾ, വ്യവസ്ഥകൾ, നിർബന്ധമല്ലാത്തതിനാലുള്ള പിഴകൾ അല്ലെങ്കിൽ മറ്റേതെങ്കിലും പ്രക്രിയകൾ കിക്ക്സ്റ്റാർട്ട് ചെയ്യാം. ഇടപെടൽ നടത്തുമ്പോൾ, പൊതു ശൃംഖലയിൽ വിന്യസിക്കുന്ന സമയത്ത് യഥാർത്ഥത്തിൽ പ്രസ്താവിച്ചതുപോലെ കരാറുകൾ നടപ്പിലാക്കി, സ്ഥിരതയില്ലാത്തതും വികേന്ദ്രീകരണവും ഉള്ള ബിൽറ്റ്-ഇൻ ഘടകങ്ങൾ വാഗ്ദാനം ചെയ്യുന്നു.

Ethereum വിർച്ച്വൽ മഷീൻ

Ethereum ഇൻഫ്രാസ്ട്രക്ചറിൽ ഒരു സ്മാർട്ട് കോൺട്രാക്റ്റ് ഒരു സുപ്രധാന ഉപകരണം ആണ്. ഈ പ്രബന്ധത്തിൽ പിന്നീട് ചർച്ച ചെയ്തതു പോലെ, ഹൈഡ്രോ ബ്ലോക്ക്ഷെയിനിന്റെ ലെയർ കോർ ഫങ്ഷണാലിറ്റി ഇഷ്ടാനുസൃത കോൺട്രാക്റ്റുകൾ വഴി നേടാം.

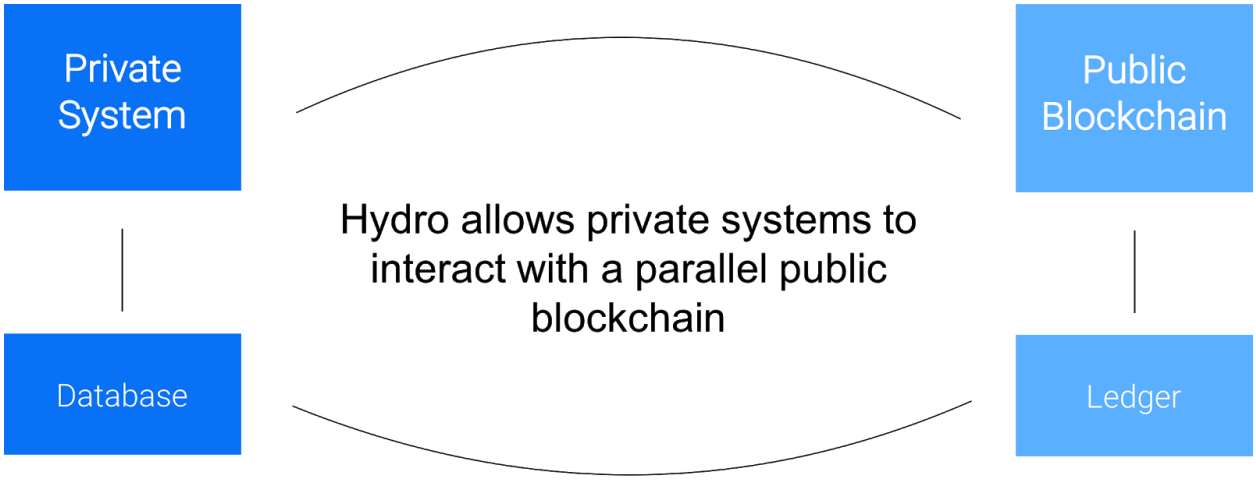
Ethereum- ലെ സ്മാർട്ട് കോൺട്രാക്റ്റുകൾക്ക് റൺടൈം പരിസ്ഥിതിയാണ് Ethereum Virtual Machine (EVM). EVM, സേവന നിരസിക്കൽ ആക്രമണങ്ങൾ തടയാൻ സഹായിക്കുന്നു, പ്രോഗ്രാമുകൾ സ്റ്റേറ്റുചെയ്ത് നിലനിർത്താനും, തടസ്സപ്പെടുത്താൻ കഴിയാത്ത ആശയവിനിമയം സാധ്യമാക്കാനും ഇത് സഹായിക്കുന്നു. ഇവിഎമിലെ പ്രവർത്തനങ്ങൾ, അവയുമായി ബന്ധപ്പെട്ട ഗ്യാസ് എന്നു വിളിക്കുന്ന ചെലവുകൾക്കനുസൃതമായി, ആവശ്യമുള്ള കമ്പ്യൂട്ടേഷണൽ റിസോഴ്സുകളെ ആശ്രയിച്ചിരിക്കുന്നു. ഓരോ ഇടപാടിനും ഗ്യാസ് ലിമിറ്റഡ് എന്നറിയപ്പെടുന്ന പരമാവധി അളവ് ഗ്യാസ് ഉണ്ട്. ഒരു ഇടപാട് ഉപയോഗിച്ചിരിക്കുന്ന ഗ്യാസ് പരിധിയിലെത്തിയാൽ, അത് തുടർന്നും തുടരുകയും ചെയ്യും.

പൊതു ലെഡ്ജർ

ഒരു സ്വകാര്യ ലെഡ്ജർ ഫോർ പ്രൈവറ്റ് സിസ്റ്റംസ്

സാമ്പത്തിക ഇടപാടുള്ള പ്ലാറ്റ്ഫോമുകൾ, വെബ്സൈറ്റുകൾ, ആപ്ലിക്കേഷനുകൾ തുടങ്ങിയവ മിക്കപ്പോഴും ഡാറ്റാ ഫ്ലോകളുടെ മാദ്ധ്യമങ്ങളായി വിവരിക്കാറുണ്ട് – അവർ അവരുമായി സമ്പർക്കം പുലർത്തുന്ന എന്റിറ്റികൾക്കായി അവ അയയ്ക്കുക, വീണ്ടെടുക്കുക, സംഭരിക്കുക, അപ്ഡേറ്റുചെയ്യുക, പ്രോസസ്സ് ചെയ്യുക. ഈ ഡാറ്റയുടെയും സാമ്പത്തിക സേവനങ്ങളുടെയും സ്വഭാവം കാരണം സാധാരണയായി, ഈ സംവിധാനങ്ങൾ പലപ്പോഴും സ്വകാര്യവും കേന്ദ്രീകൃതവുമായ രീതിയിൽ സങ്കീർണ്ണ പ്രവർത്തനങ്ങൾ നടക്കുന്നു. സ്വകാര്യഘടകങ്ങളിലുള്ള റിലയൻസ്, അതോടൊപ്പം, ആന്തരിക വ്യവസ്ഥിതിയുടെ പരിധിക്ക് പുറത്തുള്ള ബാഹ്യശക്തികളെ സംയോജിപ്പിച്ച് വിവിധതരം സുരക്ഷ, സുതാര്യത, കാര്യക്ഷമത നേടുന്നതിന് വാതിൽ തുറക്കുന്നു.

ഹൈഡ്രജന്റെ എപിഐ പ്ലാറ്റ്ഫോം ഇതുപോലെയാണ്. സ്വകാര്യ ഹൈഡ്രജന്റെ പരിസ്ഥിതി വ്യവസ്ഥയിൽ പരിക്രമണം ചെയ്യപ്പെടുന്ന വിധത്തിൽ ഹൈഡ്രജൻ ഉപയോക്താക്കൾ ഒരു ബ്ലോക്കച്ചിനുമായി ഇടപഴകുന്നതിലൂടെ ഹൈഡ്രോ ലക്ഷ്യം നേടുന്നു.

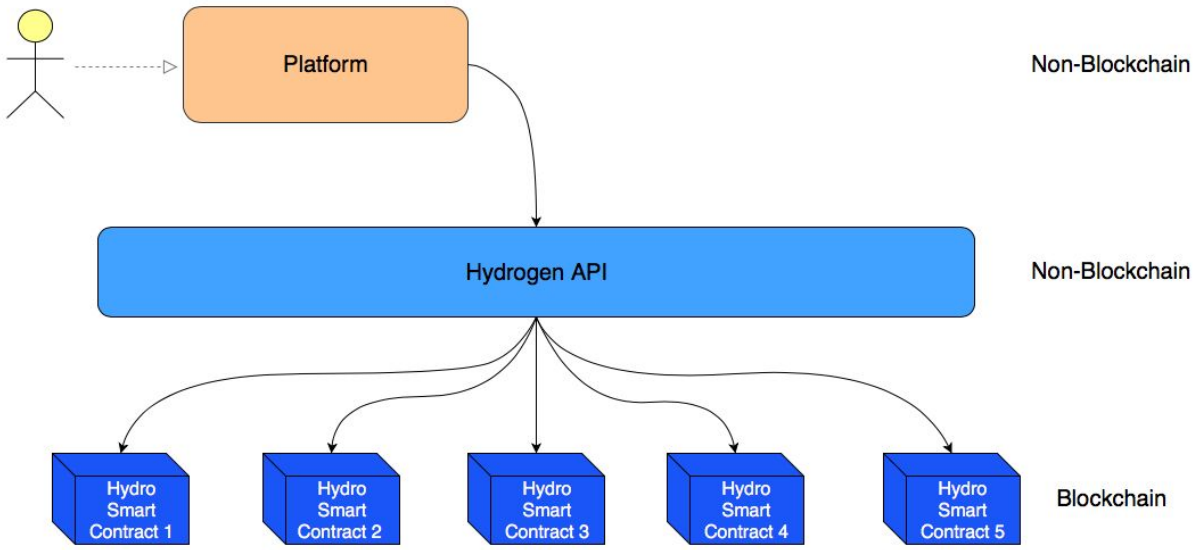


സ്വകാര്യ പ്രവർത്തനത്തിന് മുമ്പോ, അതിനിടയിലോ അല്ലെങ്കിൽ അതിനുശേഷമോ പൊതു തടയൽ അടിസ്ഥാനത്തിലുള്ള പ്രവർത്തനങ്ങൾ നടത്താവുന്നതാണ്. സ്വകാര്യവും പൊതുവുമായ ഘടകങ്ങൾ തമ്മിലുള്ള പരസ്പരബന്ധം ഒരു പരിസ്ഥിതിക്കുള്ളിൽ പ്രക്രിയകൾ ഉറപ്പാക്കാനോ സ്റ്റാമ്പ് ചെയ്യാനോ റെക്കോർഡ് ചെയ്യാനോ മെച്ചപ്പെടുത്താനോ ഉപകരിക്കുന്നു.

ബ്ലാക്ക് സാങ്കേതിക വിദ്യയുടെ പ്രയോജനത്തെ സ്പർശിക്കുന്നതിലൂടെ, ഈ മോഡലിന്റെ പ്രാധാന്യം കൂടുതൽ കരുത്തുറ്റതാക്കുന്നു. ഈ ഹൈബ്രിഡ് ഫ്രെയിംവർക്ക് എല്ലാ പ്ലാറ്റ്ഫോമുകളിലും ബാധകമായേക്കില്ലെങ്കിലും, ഹൈഡ്രോ അത് ഏത് കേസുകളിൽ വച്ചുകൊണ്ട് മൂല്യവത്താകും.

അഡോപ്ഷൻ വേണ്ടി ആർക്കിടെക്ട്

നിലവിലുള്ള നിലവിലുള്ള ബ്ലോക്കിചെയിൻ സംരംഭങ്ങളിൽ നിന്ന് ഹൈഡ്രോ വ്യത്യാസപ്പെട്ടിരിക്കുന്നു. കാരണം, വ്യവസ്ഥാപരമായ മാറ്റം ആവശ്യമില്ലാതെ തന്നെ നിലവിലുള്ളതോ നിലവിലുള്ളതോ ആയ സംവിധാനങ്ങളെ സ്വതന്ത്രമായി നിലനിർത്താൻ കഴിയും. പകരം പകരം, ജലവൈദ്യുതി വർദ്ധിപ്പിക്കുന്നതിന് ലക്ഷ്യമിടുന്നു. ഹൈഡ്രജൻ `API`-കളിലേക്ക് പ്ലഗ് പ്ലാറ്റ്ഫോമുകളും ഇൻസ്റ്റിറ്റ്യൂട്ടുകളും ബ്ലോക്കിൻ സ്വപ്രേരിതമായി പ്രവേശിക്കാൻ കഴിയും.



ഹൈഡ്രജനെ അനുകൂലിക്കുന്ന സാമ്പത്തിക സേവന പ്ലാറ്റ്ഫോമുകളുടെ വ്യാപ്തി വിശാലമാണ്. ഈ പ്ലാറ്റ്ഫോമുകൾക്കുമാത്രമേ ഏതെങ്കിലും അനുഭവത്തിൽ അധികാരമോ, ഏതെങ്കിലും കുത്തകാവകാശ സേവനങ്ങളിലോ, ഏതെങ്കിലും സ്വകാര്യ ഡാറ്റാ പ്രവർത്തനം നടത്താനും, ഏതൊരു പരിതസ്ഥിതിയിൽ വിന്യസിക്കാനും കഴിയും. ഇത് ഹൈഡ്രജന്റെ ഘടനാപരമായ മോഡുലറിയാണ്, ഹൈഡ്രോയുമായി ചേർന്ന്, ദത്തെടുപ്പിന്റെ ഒരു പര്യവേക്ഷണ ഡ്രൈവറായി പ്രവർത്തിക്കുന്നു.

മഴവില്ല്

ഹൈഡ്രോ പബ്ലിക് ലിറ്റററിൻറെ മുകളിൽ നിർമ്മിച്ചിരിക്കുന്ന ഒരു ബ്ലോക്ക്ചെയിൻ-അധിഷ്ഠിത ആധികാരികത സേവനമാണ് "റെയിൻഡ്രോപ്പ്." ഇത് ഒരു വ്യത്യസ്തമായ, സ്വഭാവമില്ലാത്ത, ആഗോളതലത്തിൽ കാണാവുന്ന ഒരു സുരക്ഷാ തലം നൽകുന്നു, അത് ഒരു അംഗീകൃത ഉറവിടത്തിൽ നിന്നും ഒരു ആക്സസ് അഭ്യർത്ഥന വരുന്നുവെന്ന് സ്ഥിരീകരിക്കുന്നു.

OAuth 2.0 പോലുള്ള സ്വകാര്യ പ്രാമാണീകരണ പ്രോട്ടോക്കോളുകൾ നിലനിന്നിരുന്ന ഉപയോഗങ്ങളുടെ സ്പെക്ട്രംക്കായി പലതരത്തിലുള്ള റോബസ്റ്റും ഉപയോഗവും വാഗ്ദാനം ചെയ്യുന്നു. ഈ പ്രോട്ടോകോളുകൾക്ക് പകരം മത്സരിക്കാനോ അല്ലെങ്കിൽ ശ്രമിക്കാനോ കുറച്ച് ആവശ്യമില്ല- ഹൈഡ്രോ ബ്ലോക്ക്ചെയിൻ മെക്കാനിക്സ് ഒരു ആധാരീകരണ പ്രക്രിയയുടെ ഭാഗമായി കൂട്ടിച്ചേർക്കാൻ അവരെ സഹായിക്കുന്നു. സിസ്റ്റം ലംഘനങ്ങൾ തടയുന്നതിനും ഡാറ്റാ ലംഘനങ്ങളെ തടയുന്നതിനും ഇത് ഒരു സുരക്ഷാ ലെയറാണ് ചേർക്കാൻ കഴിയുക.

Raindrop ന്റെ സാങ്കേതിക വശങ്ങളെ പരിശോധിക്കുന്നതിനുമുമ്പ് ആദ്യം അത് പരിഹരിക്കാൻ ശ്രമിക്കുന്ന പ്രശ്നം പരിശോധിക്കാം.

സാമ്പത്തിക സുരക്ഷ സംസ്ഥാന

ഡേറ്റായുടെ പ്രായം ഉയർന്നുവരുന്നു. ഇത് കേടുപാടുകൾ കൂടുന്നതിന് കാരണമാവുകയും ഇത് സാമ്പത്തിക സേവനങ്ങൾക്ക് വളരെ പ്രധാനമാണ്. ഗവൺമെന്റ് ഐഡി നമ്പറുകൾ, അക്കൗണ്ട് ക്രെഡൻഷ്യലുകൾ, ട്രാൻസാക്ഷൻ ചരിത്രങ്ങൾ തുടങ്ങിയ സ്വകാര്യവും സെൻസിറ്റീവ് ഡാറ്റയും വലിയ അളവിൽ ഗേറ്റ്വേകൾ സാമ്പത്തിക പ്ലാറ്റ്ഫോമാണ്. ഈ ഡാറ്റ എത്രത്തോളം വളരെ പ്രധാനപ്പെട്ടതാണെന്നത് കൊണ്ട്, അനാവശ്യമായ ആക്സസ് സാധാരണഗതിയിൽ ദുരന്തപൂർണ്ണമായ ഫലങ്ങൾ കൈവരുന്നു.

വ്യക്തിപരമായ ഐഡൻറിഫയബിൾ ഇൻഫർമേഷൻ (പി ഐ ഐ) മോഷ്ടിച്ച ഇനങ്ങളുടെ വിവരങ്ങൾ ഡീപ് വെബിൽ $ 1 ആയി വിറ്റഴിയുന്നുവെന്നാണ് ഒരു ഗവേഷണ സ്ഥാപനമായ ട്രെൻഡ് മൈക്രോ റിപ്പോർട്ട് ചെയ്തിരിക്കുന്നത്. പാസ്പോർട്ട് പോലുള്ള സ്കാനുകൾക്ക് 10 ഡോളർ വരെ ലഭിക്കുന്നു, കൂടാതെ ബാങ്ക് പ്രവേശന ക്രെഡൻഷ്യലുകൾ ചുരുങ്ങിയത് 200 ഡോളർ, മോഷണം പോയ ഡാറ്റയെ കൂടുതൽ വിഭജിച്ച് സൂക്ഷിക്കാനാവില്ല.

നിർഭാഗ്യവശാൽ, നിലവിലുള്ള സാമ്പത്തിക വ്യവസ്ഥ അസ്ഥിരമായ ട്രാക്ക് റെക്കോർഡ് ചെയ്യുന്നില്ലെങ്കിൽ, അതിന്റെ ലംഘനങ്ങളെ തടഞ്ഞുനിർത്തുന്നതിനും, രോഗനിർണയം നടത്തുന്നതിനും, ആശയവിനിമയം നടത്തുന്നതിനും വരുമ്പോൾ.

- ജാവലിൻ സ്ട്രാറ്റജി & റിസർച്ച് നടത്തിയ ഒരു പഠന പ്രകാരം 2017 ലെ ഐഡന്റിറ്റി വഞ്ചന പഠനം - 2016 ൽ 15.4 ദശലക്ഷം യുഎസ് ഉപഭോക്താക്കളിൽ നിന്നും 16 ബില്ല്യൺ ഡോളർ മോഷണം നടത്തി, വ്യക്തിപരമായി തിരിച്ചറിയാൻ കഴിയുന്ന വിവരങ്ങൾ (പിഐഐ) സംരക്ഷിക്കുന്നതിനായി സാമ്പത്തിക സംവിധാനത്തിന്റെ പരാജയങ്ങൾ കാരണം.
- 2016 ഏപ്രിലിൽ സിമന്റ്സെക് ഇന്റർനെറ്റ് സെക്യൂരിറ്റി ട്രീറ്റ് റിപ്പോർട്ട് പ്രസിദ്ധീകരിച്ചു. 1.1 ബില്ല്യൻ പിഐഐ 2016 കാലഘട്ടത്തിൽ വിവിധ കഴിവുകളിൽ വിട്ടുവീഴ്ച ചെയ്തു.
- 2016 ൽ ആഗോളതലത്തിൽ 4,149 ഡാറ്റ വ്യാപാരികൾ സംഭവിച്ചതായാണ് കണക്കുകൾ സൂചിപ്പിക്കുന്നത്. 4.2 ബില്ല്യൻ റെക്കോഡുകൾ.

- 2017 തലേസ് ഡാറ്റ ട്രീറ്റ് റിപ്പോർട്ട് - പ്രൊഫഷണൽ സേവനങ്ങളിലെ ആഗോള ഐ.ടി പ്രൊഫഷണലുകളുടെ ഒരു സർവ്വേയിൽ കണ്ടെത്തി, 49% സാമ്പത്തിക സേവന സംഘടനകൾ കഴിഞ്ഞ കാലഘട്ടത്തിൽ ഒരു സുരക്ഷാ ലംഘനം നേരിട്ടുവെന്നും 78% സ്വയം സംരക്ഷിക്കുന്നതിനായി കൂടുതൽ ചെലവിടുന്നു എന്നും 73 % AI, IOT, ക്ലൗഡ് ടെക്നോളജി എന്നിവയുമായി ബന്ധപ്പെട്ട പുതിയ സംരംഭങ്ങൾ ഉദ്ഘാടനം ചെയ്യുകയാണ്.

Equifax Breach

2017 ജൂലായ് 29 ന്, ഇക്വിഫാക്സ് എന്ന 118 കാരനായ ഒരു ക്രെഡിറ്റ് റിപ്പോർട്ടിംഗ് ഏജൻസി ഹാക്ക് ചെയ്തു. സോഷ്യൽ സെക്യൂരിറ്റി നമ്പരുകൾ ഉൾപ്പെടെ 143 ദശലക്ഷം ഉപഭോക്താക്കൾ പാരിതോഷികം വെളിപ്പെടുത്തിയിരുന്നു. 209,000 ഉപഭോക്താക്കൾക്ക് ക്രെഡിറ്റ് കാർഡ് ഡാറ്റ അപഹരിക്കപ്പെട്ടു.

ഈ ലംഘനത്തിൻറെ കാരണം എന്തായിരുന്നു?

ഇക്വിഫാക്സ് ഉപയോഗിക്കുന്ന ബാക്കെൻഡ് ടെക്നോളജികളുമായി ഇത് ആരംഭിക്കുന്നു. അപ്പാച്ചെ സോഫ്റ്റ്വെയർ ഫൗണ്ടേഷൻ നിർമ്മിച്ച ജാവ പ്രോഗ്രാമിങ് ഭാഷയിലെ വെബ് ആപ്ലിക്കേഷനുകൾ വികസിപ്പിക്കുന്നതിനുള്ള ഒരു ഓപ്പൺ സോഴ്സ് ചട്ടക്കൂടാണ് സ്ട്രാറ്റ്സ്. എക്സ്ട്രീം കൈകാര്യം ചെയ്യുന്നതിനായി XStream ഹാൻഡലർ ഉപയോഗിച്ച് സ്ട്രൗസ് REST പ്ലഗിൻ ഉപയോഗിച്ച് അപ്പാച്ചെ സ്ട്രോട്ടുകൾ ഉപയോഗിക്കുന്നത് CVE-2017-9805 ആണ്. ചൂഷണം ചെയ്തിട്ടുണ്ടെങ്കിൽ, വിദൂര അനൌട്ടിക്കാത്ത ആക്രമണകാരിയെ ആപ്ലിക്കേഷൻ സെർവറിൽ മെഷീൻ ഏറ്റെടുക്കുകയോ അതിൽ നിന്ന് കൂടുതൽ ആക്രമണങ്ങൾ നടത്തുകയോ ചെയ്യുന്നതിന് ക്ഷുദ്ര കോഡ് പ്രവർത്തിപ്പിക്കാൻ ഇത് അനുവദിക്കുന്നു. ഇക്ഫാഫാക്സ് ലംഘനത്തിന് രണ്ട് മാസങ്ങൾക്ക് മുൻപ് അപ്പാച്ചിയായിരുന്നു ഇത്.

പ്രോഗ്രാമിനായി XML അഭ്യർത്ഥനകളിൽ ഉപയോക്തൃ ഉപഭോഗ ഇൻപുട്ട് സീരിയൽ ഡി-സീരിയലൈസ് ചെയ്യുന്നതിനാൽ REST Plugin XStream- ൽ ഒരു അപര്യാപ്തത അടങ്ങിയിരിക്കുന്നു. കൂടുതൽ വ്യക്തമായി, XStreamHandler ന്റെ toObject () രീതിയിൽ പ്രശ്നം സംഭവിക്കുന്നു, ഒരു വസ്തുവായി XStream ഡെസിറേലൈസേഷൻ ഉപയോഗിക്കുമ്പോൾ ഇൻകമിംഗ് മൂല്യത്തിൽ ഏതെങ്കിലും നിയന്ത്രണങ്ങൾ ഏർപ്പെടില്ല, ഇത് ഏകപക്ഷീയമായി കോഡ് എക്സിക്യൂഷൻ വൈകല്യങ്ങൾ ഉണ്ടാക്കുന്നു.

ഈ REST പ്ലഗിൻ സൌകര്യമൊരുക്കിയാലും, അത് പ്രധാനമായും ചെയ്യേണ്ടതുണ്ടോ? ഇപ്പോഴും നിലവിലുള്ള REST API, Java അടിസ്ഥാന സിസ്റ്റങ്ങൾ എന്നിവയിൽ ആശ്രയിക്കുന്ന സമയത്ത് 143 ദശലക്ഷം ഉപഭോക്താക്കളെക്കുറിച്ചുള്ള സാമ്പത്തിക വിവരങ്ങൾ സുരക്ഷിതമാക്കാൻ ബ്ലാക്ക്സൈൻ ടെക്നോളജിയെ ഉപയോഗിക്കാനുള്ള മാർഗമുണ്ടോ?

ഒരു ബ്ലോക്ക്ചെയിൻ ലേയർ ചേർക്കുന്നു

സാമ്പത്തിക വിവര ഗേറ്റ്വേകളുടെ സമഗ്രത മെച്ചപ്പെടുത്താൻ കഴിയുമെന്ന് വ്യക്തം. ഹൈഡ്രോയിലൂടെ ഒരു അധിക സുരക്ഷാ പാളി എങ്ങനെ നേടാം എന്ന് നമുക്ക് പരിശോധിക്കാം.

Ethereum നെറ്റ്വർക്കിന്റെ അടിസ്ഥാന ഏകീകൃത സംവിധാനങ്ങൾ ട്രാൻസാക്ഷണൽ സാധുത ഉറപ്പാക്കുന്നു കാരണം പങ്കെടുക്കുന്നവർ സംയുക്തമായി ശരിയായി ഒപ്പുവച്ച

ട്രാൻസാക്ഷനുകൾ സംക്രിയരാണ്. ഈ യാഥാർത്ഥ്യം വികേന്ദ്രീകരണത്തിനും അപര്യാപ്തതയിലേക്കും നയിക്കുന്നു, പക്ഷേ, പ്രധാനമായും, സെൻസിറ്റീവ് ഡാറ്റ കൈകാര്യം ചെയ്യുന്ന ഗേറ്റ്വേയിലേക്ക് അനധികൃത ആക്സസ് കുറയ്ക്കുന്നതിന് ഒരു വെക്ടർ നൽകുന്നു.

ഹൈഡ്രോ ഉപയോഗിച്ച്, ബ്ലോക്കിനിയുമായി ഇടപാടുമായി ബന്ധപ്പെട്ട പ്രവർത്തനങ്ങളിൽ നിന്നും പ്രാമാണീകരണം നിർണ്ണയിക്കാവുന്നതാണ്. ഉദാഹരണത്തിന് ഒരു `API`, പ്രത്യേക ട്രാൻസാക്ഷനുകൾക്ക് മുൻകൈയെടുക്കുന്നതിലൂടെ ഡവലപ്പർമാർക്കും ആപ്ലിക്കേഷനുകൾക്കും സാധുതയുണ്ടാക്കാൻ കഴിയും, ഒരു പ്രത്യേക പ്രാമാണീകരണ പ്രോട്ടോക്കോൾ കിക്ക് ചെയ്യുന്ന ഒരു മുൻപായി ബ്ലോക്ക്ചൈനിലെ പ്രത്യേക വിലാസങ്ങൾ തമ്മിലുള്ള പ്രത്യേക ഡാറ്റാ പേലോഡുകൾ.

ഹൈഡ്രോ റെയിൻഡ്രോപ്പ്

മഴയിൽ വ്യാസമുള്ള `0.0001` മുതൽ `0.005` സെന്റീമീറ്റർ വരെ വ്യാസമുള്ള ജലത്തിൽ അടങ്ങിയിരിക്കുന്നു. ഒരു സാധാരണ മഴയിൽ, ഈ പാക്കറ്റുകളിലൊന്നായി ശതകോടിക്കണക്കിന് പേരാണ് ഉണ്ടാവുക, ഓരോ റാൻഡം വലുപ്പവും വേഗതയും ആകൃതിയും ഉണ്ട്. അതിനാൽ, മഴയുടെ കൃത്യമായ സ്വഭാവം കൃത്യമായി പ്രവചിക്കാൻ കഴിയുകയില്ല. അതുപോലെ, എല്ലാ ഹൈഡ്രോ ആധികാരികത ഉറപ്പാക്കൽ ഇടപാടുകളും അതുല്യവും അസാധ്യവും യാദൃച്ഛികമായി സംഭവിച്ചതാണ് - അതുകൊണ്ടാണ് നമ്മൾ അവയെ `Raindrops` എന്ന് വിളിക്കുന്നത്.

ക്ലയന്റ് അക്കൌണ്ടുകൾ സാധൂകരിക്കുന്നതിനായി മൈക്രോ ഫൊറ്റിറ്റ് വെരിഫിക്കേഷൻ സാധാരണയായി ഫിനാൻഷ്യൽ സേവന പ്ലാറ്റ്ഫോമുകൾ ഉപയോഗിക്കുന്നു. ആശയം ലളിതമാണ്: ഉപയോക്താവിന് ക്ലെയിം ബാങ്ക് അക്കൌണ്ടുകളിലേക്ക് റാൻഡം തുകയുടെ ചെറിയ നിക്ഷേപം പ്ലാറ്റ്ഫോം നൽകുന്നു. ഉപയോക്താവിന് സ്വന്തം അക്കൌണ്ട് ഉണ്ടെന്ന് തെളിയിക്കാനായി, ആ തുക തിരിച്ചടയ്ക്കുകയും പ്ലാറ്റ്ഫോമിലേക്ക് തുക തിരിച്ചുനൽകുകയും ചെയ്യും, അവ പിന്നീട് മൂല്യനിർണ്ണയം ചെയ്യപ്പെടും. ചോദ്യം ചെയ്യാവുന്ന ബാങ്ക് അക്കൌണ്ടുകൾ ആക്സസ് ചെയ്തുകൊണ്ട് സാധുതയുള്ള തുക (ഊഹക്കച്ചവടം കൂടാതെ) ഉപയോക്താവിന് അറിയാവുന്ന ഒരേയൊരു മാർഗം.

ഹൈഡ്രോയോടുകൂടിയുള്ള റെയിൻഡ്രോപ്പ് അടിസ്ഥാനത്തിലുള്ള പരിശോധിച്ചുറപ്പിക്കൽ സമാനമാണ്. ഉപയോക്താവിനെ ഒരു തുക അയയ്ക്കുകയും അത് വീണ്ടും റിലേ ചെയ്യുകയും ചെയ്യുന്നതിനു പകരം, ഒരു ഇടപാട് ഞങ്ങൾ നിർവ്വചിക്കുന്നു കൂടാതെ ഉപയോക്താവ് അറിയപ്പെടുന്ന ഒരു വാലറ്റിൽ നിന്ന് അത് നടപ്പിലാക്കുകയും വേണം. സംശയാസ്പദമായ ഇടപാടുകൾ നടത്താൻ ഉപയോക്താവിന് സാധിക്കുന്ന ഒരേയൊരു മാർഗം ചോദ്യത്തിൽ വാലറ്റ് ആക്സസ് ചെയ്താണ്.

`Raindrops` ഉപയോഗിച്ച്, സിസ്റ്റത്തേക്കും ആക്സസ്സറിനും ഒരു സ്ഥായിയായ പൊതു ലാപറിലുള്ള അധികാരപ്പെടുത്തൽ ശ്രമങ്ങളെ നിരീക്ഷിയ്ക്കുവാൻ സാധ്യമാകുന്നു. ഈ ബ്ലോക്കിചെയിൻ അധിഷ്ഠിത ഇടപാട് അടിസ്ഥാന സിസ്റ്റത്തിലെ പ്രവർത്തനങ്ങളിൽ നിന്നും നിരസിക്കപ്പെടുകയാണ്, വിതരണ നെറ്റ്വർക്കിൽ സംഭവിക്കുന്നത്, സ്വകാര്യ കീകളുടെ ഉടമസ്ഥതയെ ആശ്രയിച്ചിരിക്കുന്നു. അതുകൊണ്ടു, ഒരു ഉപയോഗപ്രദമായ സാധൂകരണം വെക്റ്റർ.

വിശദമായ ഒരു കാഴ്ച

ഹൈഡ്രോ ആധികാരികത പ്രക്രിയയിൽ നാല് സ്ഥാപനങ്ങൾ പ്രവർത്തിക്കുന്നു:

1. ആക്സസർ - ഒരു സിസ്റ്റം ആക്സസ് ചെയ്യാൻ ശ്രമിക്കുന്ന പാർട്ടി. ഹൈഡ്രജന്റെ കാര്യത്തിൽ, ആക്സസർ എന്നത് ഒരു സാമ്പത്തിക സ്ഥാപനമോ ഹൈഡ്രജൻ എപിഐകളോ അതിന്റെ പ്രധാന ഡിജിറ്റൽ ഇൻഫ്രാസ്ട്രക്ചറിനുപയോഗിക്കുന്ന ആപ്ലിക്കേഷനാണ്.
2. സിസ്റ്റം - ആക്സസ് ചെയ്യുന്ന ആക്സസ് ചെയ്യുന്ന സിസ്റ്റമോ ഗേറ്റ്വേയോ. ഹൈഡ്രജനെ സംബന്ധിച്ചിടത്തോളം സിസ്റ്റം ഹൈഡ്രജൻ എപിഐ തന്നെ ആണ്. ആക്സസർ - ഒരു സിസ്റ്റം ആക്സസ് ചെയ്യാൻ ശ്രമിക്കുന്ന പാർട്ടി. ഹൈഡ്രജന്റെ കാര്യത്തിൽ, ആക്സസർ എന്നത് ഒരു സാമ്പത്തിക സ്ഥാപനമോ ഹൈഡ്രജൻ എപിഐകളോ അതിന്റെ പ്രധാന ഡിജിറ്റൽ ഇൻഫ്രാസ്ട്രക്ചറിനുപയോഗിക്കുന്ന ആപ്ലിക്കേഷനാണ്.
3. ഹൈഡ്രോ - ബ്ലോക്ക്ചെയ്നുമായി ആശയവിനിമയം നടത്തുന്നതിനും ഇന്റർഫേസ് ചെയ്യുന്നതിനും സിസ്റ്റം ഉപയോഗിയ്ക്കുന്ന ഘടകം.

ബ്ലോക്ക്ചെയിൻ - ഹൈവഡ ട്രാൻസാക്ഷനുകളെ പ്രക്രിയപ്പെടുത്തുന്ന ഹൈവേ ലപ്ടർ, ഹൈഡ്രോ സ്മാർട്ട് കോൺട്രാക്റ്റുകൾ ഉൾക്കൊള്ളുന്നു. ഇതിലൂടെ വിവരങ്ങൾ തള്ളിക്കളയുകയോ, പിൻവലിക്കുകയോ അല്ലെങ്കിൽ മറ്റൊരു രീതിയിൽ പ്രവർത്തിപ്പിക്കുകയോ ചെയ്യാം.

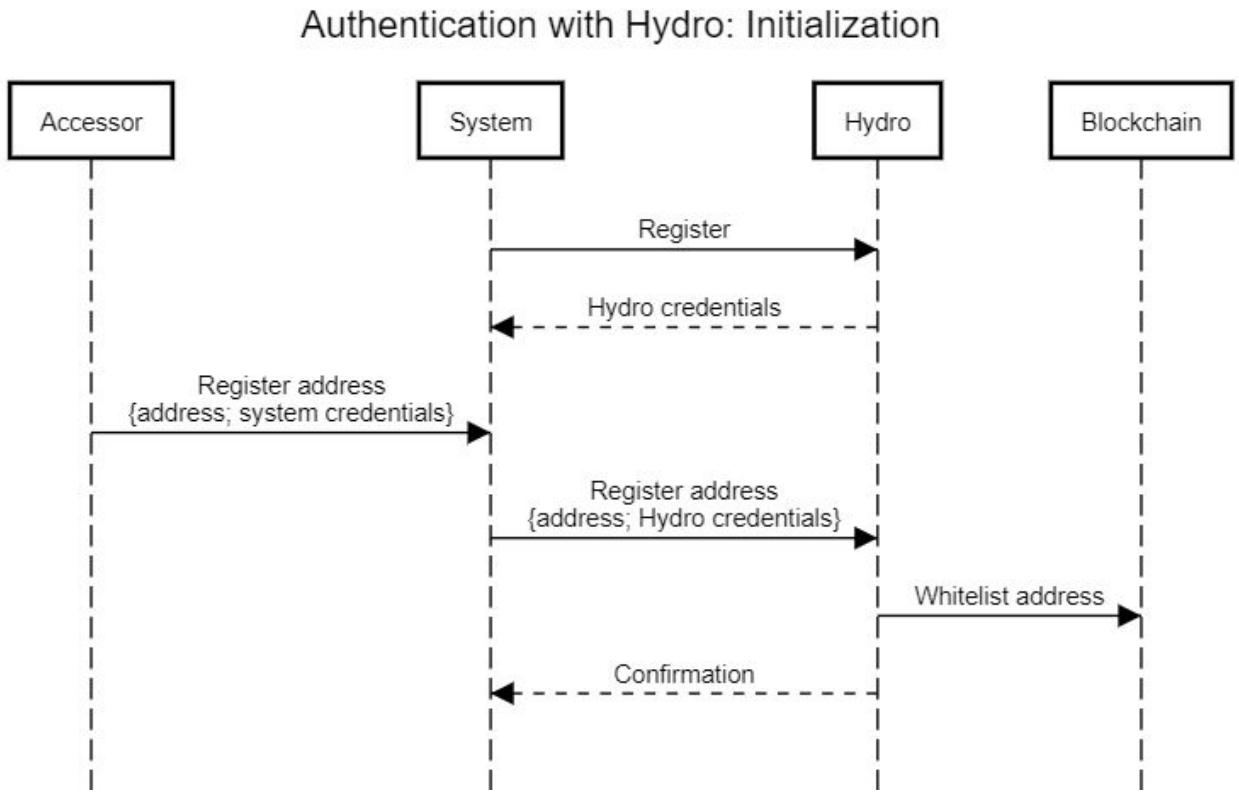
ഓരോ റെയിൻ ഡ്രോപ്പും സമ്പൂർണ്ണമായി അഞ്ച് ഇടപാടുകാരുടെ പരാമീറ്ററുകളുടെ ഒരു കൂട്ടമാണ്:

1. പ്രേഷിതാവ് - ഇടപാടുകൾ ആരംഭിക്കുന്നതിനുള്ള വിലാസം.
2. റിസീവർ - ഇടപാടിന്റെ ലക്ഷ്യസ്ഥാനം. ഒരു ഹൈഡ്രോ സ്മാർട്ട് കരാറിൽ ഒരു രീതി വിളിക്കാൻ ഇത് യോജിക്കുന്നു.
3. ഐഡി - സിസ്റ്റവുമായി ബന്ധപ്പെട്ട ഐഡന്റിഫയർ.
4. അളവ് - അയയ്ക്കാവുന്ന ഒരു കൃത്യമായ ഹെയ്റൊആർഒ.
5. വെല്ലുവിളി - ഒരു ക്രമരഹിതമായി സൃഷ്ടിച്ച ആൽഫാന്യൂമെറിക് സ്ട്രിംഗ്.

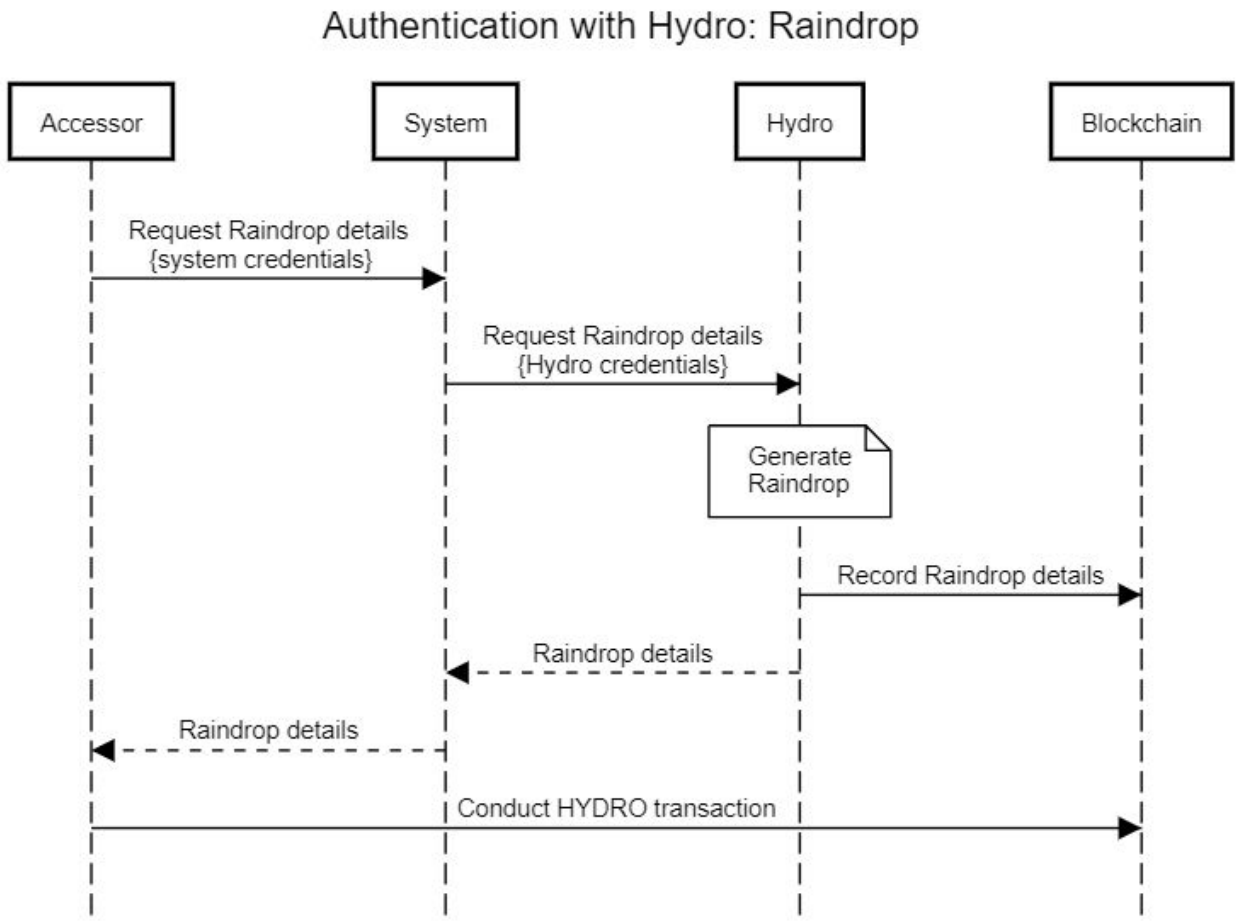
ആധികാരികപ്രക്രിയയുടെ ഒരു ഔട്ട്ലൈൻ ആണ് താഴെ കൊടുത്തിരിക്കുന്നത്, ഇത് പൊതുവേ മൂന്ന് ഘട്ടങ്ങളായി തരംതിരിക്കാം:

1. സമാരംഭിക്കൽ
2. മഴവില്ല്
3. മൂല്യനിർണ്ണയം

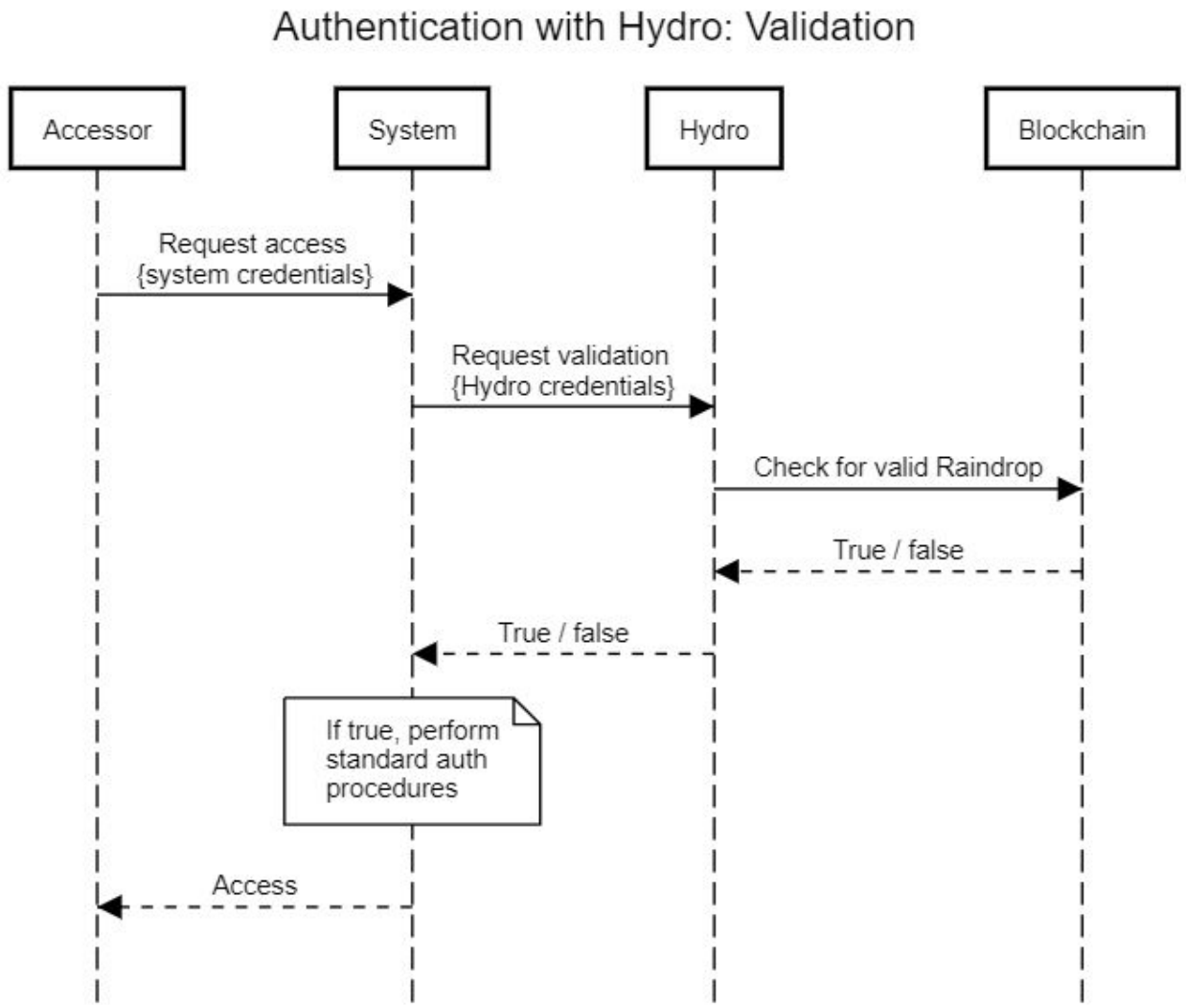
ഹൈഡ്രോ ഘടകം വഴി ബ്ലോക്കഷണുമായി ആശയവിനിമയം നടത്തുന്നതിനായി, ഹൈഡ്രോയും ക്രെഡൻഷ്യലുകളും ഉപയോഗിക്കുന്നതിനായി രജിസ്ടർ ചെയ്ത ഒരു സിസ്റ്റം (ഉദാ: ഹൈഡ്രജൻ) ആരംഭിക്കുന്നു. ഒരു പൊതു വിലാസത്തിൽ രജിസ്റ്റർ ചെയ്യുകയും, രജിസ്റ്റർ ചെയ്ത അഡ്രസ്സ് ഹൈഡ്രോയിലേയ്ക്ക് അയക്കുകയും ചെയ്യുന്ന ഒരു അക്സസറായ സിസ്റ്റം ഓവർബോർഡുകൾ (ഉദാ: ഒരു സാമ്പത്തിക സ്ഥാപനം). ഹൈഡ്രോ സ്മാർട്ട് കരാറിൽ സൂക്ഷിച്ചിരിക്കുന്ന ഒരു വൈറ്റ്ലിസ്റ്റിലേക്ക് ബ്ളോക്ക്ചൈനിലേക്ക് ഈ വിലാസം പകർത്തുക. വിലാസം വൈറ്റ്ലിസ്റ്റുചെയ്തിട്ടുണ്ടെന്ന് സ്ഥിരീകരണം സിസ്റ്റം സ്വീകരിക്കുന്നു, ഇത് എല്ലാവർക്കുമായി കാണാവുന്ന ഒരു ഇവന്റായി പരിശോധിച്ചുറപ്പിക്കാനാകും. സിസ്റ്റം രജിസ്ട്രേഷൻ ഒരിക്കൽ മാത്രമേ ഉണ്ടാകൂ, ആക്സസ്സറിന്റെ അനുമതി ആവശ്യമെങ്കിൽ ഒരു ആക്സസർ മാത്രമേ ഉണ്ടാകൂ.



സമാരംഭിക്കൽ പൂർത്തിയായിക്കഴിഞ്ഞാൽ, ഹൈഡ്രോ പരിശോധനാ പ്രക്രിയയുടെ കോർ ആരംഭിക്കാം. ഒരു റെയിൻ ഡിപ്രോ ഇടപാടുകൾ നടപ്പിലാക്കുന്ന ആക്സസ്സർ, സിസ്റ്റത്തിലെ മഴവെള്ളത്തിന്റെ വിശദാംശങ്ങൾ ആവശ്യപ്പെട്ട്, ഹൈഡ്രോയിലേക്കുള്ള അഭ്യർത്ഥന വഴി സിസ്റ്റം വഴികൾ അഭ്യർത്ഥിച്ചുകൊണ്ടാണ് ഈ പ്രക്രിയ പ്രവർത്തിപ്പിക്കുന്നത്. ഹൈഡ്രോ ഒരു പുതിയ റെയിൻഡ്രോപ്പ് ഉണ്ടാക്കുന്നു, ബ്ളോക്കിചെയിനിന് സാവധാനത്തിൽ ചില വിശദാംശങ്ങൾ സംഭരിക്കുന്നു, ഒപ്പം സിസ്റ്റം വഴി ആക്സസ്സറിലേക്ക് പൂർണ്ണ വിശദാംശങ്ങൾ നൽകുകയും ചെയ്യുന്നു. ആവശ്യമായ എല്ലാ വിവരങ്ങളും ഉള്ള ആക്സസ്സർ, രജിസ്റ്റർ ചെയ്ത വിലാസത്തിൽ നിന്ന് ഹൈഡ്രോ സ്മാർട്ട് കരാറിലെ ഒരു ഇടമാക്കി മാറ്റുന്നു. വിലാസം വൈറ്റ്ലിസ്റ്റ് ചെയ്തിട്ടില്ലെങ്കിൽ, പ്രവർത്തനം നിരസിക്കപ്പെടും – അല്ലെങ്കിൽ സ്മാർട്ട് കരാറിൽ അത് റെക്കോർഡ് ചെയ്യപ്പെടും. ആക്സസറിന്റെ സ്വകാര്യ കീയിൽ (ആക്സസ്സർ മാത്രമേ നേടാൻ കഴിയൂ) ഇത് ഒപ്പുവച്ചതിനാൽ, നേരിട്ട് ആക്സസ്സർ മുതൽ ബ്ലോക്കിചെയിൻ വരെ, ഈ ഇടപാട് സിസ്റ്റത്തിന് പുറത്തുള്ളതായിരിക്കണം.



പ്രക്രിയയുടെ അവസാന ഘട്ടം മൂല്യനിർണ്ണയമാണ്. ഈ പടിയായി, സിസ്റ്റത്തിന്റെ സ്ഥാപിത സംവിധാനത്തിലൂടെ സിസ്റ്റം ആക്സസ്സർ ഔദ്യോഗികമായി ആക്സസ് അഭ്യർത്ഥിക്കുന്നു. ഏതെങ്കിലും തരത്തിലുള്ള ആധികാരികത ഉറപ്പാക്കൽ പ്രോട്ടോക്കോളുകൾ നടപ്പിലാക്കുന്നതിന് മുൻപ്, ആക്സസ്സർ ഒരു സാധുവായ റെയിൻഡ്രോപ്പ് ട്രാൻസാക്ഷൻ നടത്തണോ വേണ്ടയോ എന്ന് `Hydro` ചോദിക്കുന്നു. സ്മാർട്ട് കരാറുമായുള്ള ഹൈഡ്രോ ഇന്റർഫെയ്സുകൾ, സാധുതയുള്ള പരിശോധനകൾ, ഒരു യഥാർത്ഥ / വ്യാജ പേര് നൽകി പ്രതികരിക്കുകയും ചെയ്യുന്നു. സിസ്റ്റം ഈ എന്തിന്റെ അടിസ്ഥാനത്തിൽ മുന്നോട്ട് പോകണമെന്ന് എങ്ങനെ തീരുമാനിക്കാൻ കഴിയും - അത് തെറ്റാണെങ്കിൽ, സിസ്റ്റം ആക്സസ് നിരസിക്കാൻ കഴിയും, അതു ശരിയാണെങ്കിൽ, സിസ്റ്റം ആക്സസ് അനുവദിക്കാൻ കഴിയും.



അടിസ്ഥാന സിസ്റ്റത്തിന്റെ ക്രെഡൻഷ്യലുകൾ - അഥവാ നിലവിലെ ഏത് സിസ്റ്റം പ്രോട്ടോക്കോളാണ് - ആധികാരികതയുടെ ഒരു ഘടകം വരെ, ഹൈഡ്രോ ലെയർ ഉപയോഗപ്രദമായ ഒരു രണ്ടാമത്തെ ഘടകം നൽകേണ്ടത് വളരെ പ്രധാനമാണ്. രണ്ട് പ്രാഥമിക ആക്രമണ സദിശങ്ങളെ പരിശോധിക്കുന്നതിലൂടെ, അതിന്റെ പ്രയോജനത്തെ നമുക്ക് ഉടനടി സ്ഥിരീകരിക്കാം:

- വെക്ടർ 1 - ആക്രമണകാരി ആക്സസറിന്റെ അടിസ്ഥാന സിസ്റ്റം യോഗ്യതകൾ മോഷ്ടിക്കുന്നു
  - ശരിയായ സിസ്റ്റത്തിന്റെ ക്രെഡൻഷ്യലുകൾ ഉപയോഗിച്ച് സിസ്റ്റത്തിലേക്ക് ആക്സസ് നേടുന്നതിന് ആക്രമണം ശ്രമിക്കുന്നു
  - ബ്ലോക്ക്ഷെയിനിൽ സാധുവായ ഇടപാട് ഉണ്ടോയെന്ന് തീരുമാനിക്കാൻ ഹൈഡ്രോയുമായി സിസ്റ്റം പരിശോധിക്കുന്നു
  - ഹൈഡ്രോ തെറ്റ് നൽകുന്നു, കൂടാതെ സിസ്റ്റം ആക്സസ്സ് നിരസിക്കുന്നു
- വെക്റ്റർ 2 - ആക്സസറിന്റെ പേഴ്സിലേക്ക് സ്വകാര്യ കീ (കൾ) മോഷ്ടിക്കുന്നു
  - റെഡ്ഡ്രോപ്പ് വിശദാംശങ്ങൾ ആവശ്യമില്ലാതെ രജിസ്റ്റർ ചെയ്ത വിലാസത്തിൽ നിന്ന് ജലവൈദ്യുതി നടത്താൻ ആക്രമണം നടത്തുന്നയാൾ ശ്രമിക്കുന്നു
  - ആക്രമണകാരി ഒരു സാധുതയുള്ള ബ്ലോക്ക്ച്ചെയ്ൻ ഇടപാട് നടത്താൻ കഴിയില്ല

- ശരിയായ സിസ്റ്റത്തിന്റെ ക്രെഡൻഷ്യലില്ലെങ്കിൽ ആക്രമണകാരിയ്ക്കും സിസ്റ്റത്തിലേക്കുള്ള പ്രവേശനം അഭ്യർത്ഥിക്കാൻ കഴിയില്ല

സിസ്റ്റം ആക്സസ് ചെയ്യാനായി അടിസ്ഥാന ആക്രമണകാരികളുടെയും ആക്സസറിന്റെ സ്വകാര്യ വാലറ്റ് കീ (കൾ) ഉം ആക്രമകൻ മോഷ്ടിക്കണം. ഇക്കാര്യത്തിൽ ഹൈഡ്രോ ആധികാരികതയുടെ ഒരു അധിക ഘടകം വിജയകരമായി കൂട്ടിച്ചേർത്തു.

പൊതുജനങ്ങൾക്ക് റെയിൻ ഡ്രോപ്പ് തുറക്കുന്നു

ഹൈഡ്രജൻ എപിഐ സംവിധാനം ഉപയോഗപ്പെടുത്തുന്നതിന് ഈ ബ്ലോക്ക്ഷിൻ അടിസ്ഥാനമാക്കിയുള്ള ആധികാരികത ഉറപ്പാക്കൽ സംവിധാനം രൂപകൽപ്പന ചെയ്യപ്പെട്ടിരുന്നെങ്കിലും, വിവിധ പ്ലാറ്റ്ഫോമുകളിലും സിസ്റ്റങ്ങളിലും അത് വ്യാപകമായിരുന്നു. ഈ സ്ഥിരീകരണ പാളിയിൽ നിന്ന് മറ്റുള്ളവർക്ക് പ്രയോജനം നേടാനാകുമെന്നതിനാൽ, ഞങ്ങൾ അത് ഉപയോഗിക്കുന്നത് തുറക്കുന്നു.

എപിഐ `ecosystem` ലേക്കുള്ള ആക്സസ് ഒരു മുൻകൂർ ഹൈഡ്രജൻ അതിനെ ഏകീകരിക്കുകയും പോലെ, അതുപോലെ ഏത് സിസ്റ്റം നിലവിലുള്ള നടപടിക്രമങ്ങൾ, പ്രോട്ടോക്കോളുകൾ ചേർക്കാൻ കഴിയും. ഏത് പ്ലാറ്റ്ഫോമും - ഒരു `API`, ആപ്ലിക്കേഷൻ, എന്റർപ്രൈസ് സോഫ്റ്റ്വെയർ, ഗെയിമിംഗ് പ്ലാറ്റ്ഫോം തുടങ്ങിയവ - ആധികാരികത ആവശ്യകതകൾക്കായി ഹൈഡ്രോയെ ലിവറേജ് ചെയ്യാൻ കഴിയും. ഈ ബ്ലോക്കിചെയിൻ ലേയർ ഒരു പ്രാമാണീകരണ ചട്ടക്കൂടിനെ അല്ലെങ്കിൽ `REST API` ആയി സംയോജിപ്പിക്കാൻ ആഗ്രഹിക്കുന്നവർക്ക് `GitHub`- ൽ ഔപചാരിക ഡോക്യുമെന്റേഷൻ ലഭ്യമാകും.

കേസ് പഠനം - OAuth 2.0 ഓടെ Raindrop

`Raindrop` റിലീസ് സ്വകാര്യ സംഘടനകൾ ഉപയോഗിച്ച് ഡസൻ കണക്കിന് വഴികൾ ഉണ്ട്. സെൻസിറ്റീവ് ഡാറ്റ സുരക്ഷിതമാക്കാൻ കഴിഞ്ഞ പതിറ്റാണ്ടുകളിൽ സ്വകാര്യ `API` കൾ, ഡാറ്റാബേസുകൾ, നെറ്റ്വർക്കുകൾ എന്നിവ ടോക്കൺ, കീകൾ, ആപ്സ്, പ്രോട്ടോക്കോളുകൾ എന്നിവയുടെ വിപുലമായ സംവിധാനം സൃഷ്ടിച്ചു. ഉദാഹരണത്തിന് `Google`, `Google Authenticator` അപ്ലിക്കേഷൻ ഉപയോഗിച്ച് ഏറ്റവും പ്രചാരമുള്ള ഉൽപ്പന്ന ദാതാക്കളിൽ ഒന്നായി മാറും. മുമ്പ് സൂചിപ്പിച്ചതുപോലെ, നിലവിലുള്ള പ്രോട്ടോക്കോളുകളുമായി മത്സരിക്കുകയോ പകരം വെയ്ക്കുകയോ ചെയ്യുന്നതിന് ഒരു കാരണവുമില്ല.

ഒരു കേസിന്റെ പഠനപ്രകാരം, ഹൈഡ്രജൻ ആധികാരികത എപ്രകാരമാണ് എപിഐ സുരക്ഷാ ചട്ടക്കൂടിൽ ഒരു സുരക്ഷാ പാളി ആയി ഹൈഡ്രോ ഓതന്റിക്കേഷൻ നടപ്പിലാക്കുന്നത് എങ്ങനെയെന്ന് ചുരുക്കപ്പേരാണ്:

1. ഹൈഡ്രജൻ `API` പങ്കാളികൾ ആദ്യം അവരുടെ വൈവിധ്യമാർന്ന വൈവിധ്യമാർന്ന ഐപി വിലാസങ്ങളിൽ ഉണ്ടായിരിക്കണം.
2. പൊതു ജലവൈദ്യുതി വിലാസത്തെ വൈറ്റ്ലിസ്റ്റ് ചെയ്യാൻ പങ്കാളികൾ അഭ്യർത്ഥിക്കണം.
3. ഹൈഡ്രജൻ എപിഐകളിലേക്കുള്ള എല്ലാ കോളുകളും ഡാറ്റ കൈമാറ്റങ്ങളും `HTTPS` പ്രോട്ടോക്കോളിലൂടെ എൻക്രിപ്റ്റ് ചെയ്യുകയും പ്രക്ഷേപണം ചെയ്യുകയും ചെയ്യുന്നു.
4. പങ്കാളികൾ രജിസ്റ്റർ ചെയ്ത ഹൈഡ്രോ വിലാസത്തിൽ നിന്നും സാധുവായ ഒരു ഹൈഡ്രോ റെയിൻഡ്രോപ്പ് ട്രാൻസാക്ഷൻ പൂർത്തിയാക്കിയിരിക്കണം.

5. പങ്കാളികൾ `OAuth 2.0` മൂല്യനിർണ്ണയം ഉപയോഗിക്കണം. `OAuth` (ഓപ്പൺ ഓതറൈസേഷൻ) എന്നത് ടോക്കൺ അടിസ്ഥാനമാക്കിയുള്ള ആധികാരികത ഉറപ്പാക്കലിനും അംഗീകാരത്തിനും തുറന്ന മാനദണ്ഡമാണ്. "റിസോഴ്സ് ഓണർ പാസ്വേഡ് ക്രെഡൻഷ്യലുകൾ", "ക്ലയന്റ് ക്രെഡൻഷ്യലുകൾ" ഗ്രാന്റ് ടൈപ്പുകൾ ഹൈഡ്രജൻ പിന്തുണയ്ക്കുന്നു, ഓരോ എപിഐയും ഒരു അംഗീകരണ അഭ്യർത്ഥനയ്ക്കായി ക്രെഡൻഷ്യലുകൾ നൽകണം.
6. മുകളിലുള്ള അഞ്ച് ഘടകങ്ങളിൽ ഏതെങ്കിലും ലംഘിക്കുന്നില്ലെങ്കിൽ, ഹൈഡ്രജൻ പങ്കാളിക്ക് ഒരു അദ്വതീയ ടോക്കൺ നൽകിയിട്ടുണ്ട്, ഓരോ `API` കോളിലും പരിശോധിച്ച് പരിശോധിക്കേണ്ടതാണ്.
7. ടോക്കൺ `24` മണിക്കൂർ നേരത്തേക്ക് സാധുവാണ്, പിന്നീട് പങ്കാളി വീണ്ടും സ്വയം ക്രമീകരിക്കേണ്ടതുണ്ട്.

ഈ ഘട്ടങ്ങളൊന്നും ലംഘിക്കപ്പെട്ടിട്ടുണ്ടെങ്കിൽ, ഉപയോക്താവ് ഉടൻ `API` ആക്സസ്സിൽ നിന്ന് ലോക്ക് ചെയ്യും. ഒരു സുരക്ഷാസംവിധാനത്തെ ഹാക്കർമാർ മറികടക്കാൻ കഴിയില്ല, കാരണം കോടിക്കണക്കിന് വ്യത്യസ്ത കോമ്പിനേഷനുകളുണ്ട്.

ഹൈഡ്രജന്റെ സെക്യൂരിറ്റി പ്രോട്ടോക്കോളിലെ ഒരു പ്രധാന ഘടകമാണ് ഹൈഡ്രോ ബ്ലോക്ക്ചെയിൻ അടിസ്ഥാനത്തിലുള്ള ആധികാരികത. ഹൈഡ്രജൻ സംഘം മൾട്ടി-ഒപ്പ് ക്ലെയിമുകൾ സജ്ജമാക്കുന്നതിന് സഹായിക്കുന്നു, കൂടാതെ മറ്റ് ക്രെഡൻഷ്യലുകളിൽ നിന്നും സ്വതന്ത്രമായി സുരക്ഷിത സ്ഥാനങ്ങളിൽ സ്വകാര്യ കീകൾ സൂക്ഷിക്കുന്നു, അതിനാൽ ഒരൊറ്റ പോയിന്റ് പരാജയമില്ല. ഒരു ശരിയായി സുരക്ഷിതമായ മൾട്ടി-ഒപ്പ് വാലറ്റ് മോഷ്ടിക്കുന്നത് ബുദ്ധിമുട്ടാണ്, പക്ഷേ ബ്ലോക്കിഞ്ചിന്റെ പൊതു സ്വഭാവം എപിഐയുടെ സുരക്ഷയുമായി ബന്ധപ്പെട്ട മോഷണത്തെ വേഗത്തിലാക്കുന്നതിനെ അനുവദിക്കുന്നു.

ഹൈഡ്രോ സ്മാർട്ട് കരാറിന് ഒരു ആധികാരിക പരിശ്രമത്തെ ആരെങ്കിലും നോക്കിക്കാണാം. അതായത്, മാസാവസാനങ്ങളിൽ വിട്ടുവീഴ്ച ചെയ്യപ്പെടുന്ന പ്ലാറ്റ്ഫോമിന്റെ ദിവസങ്ങൾ കഴിഞ്ഞ ഒരു കാര്യമായിരിക്കാം. ലോകത്തിൽ എവിടെ നിന്നും, തത്സമയ സമയത്ത് അപ്രതീക്ഷിത അംഗീകാര ശ്രമങ്ങൾ തിരിച്ചറിയാനുള്ള കഴിവ് കാരണം `API` ഹാക്കർമാരെ ഇപ്പോൾ എളുപ്പത്തിൽ നീക്കംചെയ്യാൻ കഴിയും.

അപകടസാധ്യതകൾ

സോഷ്യൽ മീഡിയയുടെ ആദ്യ ദിവസങ്ങൾ, ഇമെയിൽ, സ്ട്രീമിംഗ് ആപ്ലിക്കേഷനുകൾ (ഡയൽ-അപ് കണക്ടിവിറ്റിയിൽ ആശ്രയിച്ചിരുന്നവ) തുടങ്ങിയ നവീന സാങ്കേതികവിദ്യ പോലെ, വളരെ പ്രധാനമാണ് അത് എറ്റെർയോം ട്രാൻസാക്ഷൻ വേഗതയിലും വോള്യൂങ്ങളിലും പുതിയ സംഭവവികാസങ്ങൾ വളരെ ശ്രദ്ധയോടെ കൈകാര്യം ചെയ്യുന്നു. 1995-ൽ YouTube ആരംഭിക്കാൻ ശ്രമിക്കുമോ? അല്ലെങ്കിൽ ആദ്യത്തെ സ്മാർട്ട് ബ്ലാക്ക്ബെറിയിൽ ഓഫർ ചെയ്യാറുണ്ടോ?

Vitalik Buterin ഉം ജോസഫ് Poon ഉം പോലുള്ള കോർ സെറ്റുകളുടെ വികസിപ്പിച്ചവർ Plasma നിർദേശിച്ചിട്ടുണ്ട്: സ്കാളബിൾ ഓട്ടോണോമസ് സ്മാർട്ട് കോൺട്രാക്റ്റുകൾ Ethereum പ്രോട്ടോക്കോളിലേക്ക് അപ്ഗ്രേഡ് ചെയ്യുക:

> പ്ലാസ്മ എന്നത് സ്മാർട്ട് കോൺട്രാക്റ്റുകളുടെ പ്രോത്സാഹിപ്പിക്കുന്ന ഒരു നിർദ്ദിഷ്ട ചട്ടക്കൂടാണ്, ഇത് ഒരു സെക്കൻഡിന് (ലോകമെമ്പാടും വിപുലീകരിച്ചത്) വികസിച്ചു കൊണ്ടിരിക്കുന്ന സാമ്പത്തിക പരിഷ്കാരങ്ങളുടെ പ്രധാന അളവുകളെ പ്രതിനിധീകരിക്കുന്നത് തടയുന്നു. ഈ സ്മാർട്ട് കരാറുകൾ നെറ്റ്വർക്ക് ഇടപാടി ഫീസ് വഴി സ്വമേധയാ പ്രവർത്തിക്കുന്ന പ്രവർത്തനം തുടരാൻ പ്രോത്സാഹിപ്പിക്കും, ഇത് ട്രാൻസാക്ഷണൽ സ്റ്റേറ്റ് ട്രാൻസിഷനെ നിർവ്വചിക്കുന്നതിന് താഴെയുള്ള ബ്ലോക്ക്ചൈനിൽ (ഉദാഹരണത്തിന്, Ethereum) ആശ്രയിക്കുന്നതാണ്.

ദ്രുതഗതിയിലുള്ള ഇടപാടുകൾക്കും കുറഞ്ഞ ഫീസുകൾക്കും വേണ്ടി രൂപകൽപ്പന ചെയ്ത ഓഫ്-ചെയിൻ സ്കെലിംഗ് സൊല്യൂഷൻ, ദി റൈഡൻ നെറ്റ്വർക്ക് പോലുള്ളവർ

നിർദ്ദേശിച്ചിട്ടുണ്ട്. ഈ സമയത്ത്, `Raindrop Ethereuem` ചട്ടക്കൂടിൽ വളരെ കുറഞ്ഞ ബുദ്ധിമുട്ട് ഉണ്ടാക്കും, അങ്ങനെ സ്കേലബിളിറ്റി സാങ്കേതികവിദ്യയുടെ വിജയത്തിന് വളരെ ചെറിയ റിസ്ക് ആണ്.

ഉപസംഹാരം

ഒരു പൊതു ബ്ലോക്കിൻസിന്റെ അപര്യാപ്തത, എ.പി.ഐകൾ പോലെയുള്ള സ്വകാര്യ സംവിധാനങ്ങളുടെ സുരക്ഷ വർദ്ധിപ്പിക്കുന്നതിനുള്ള പുതിയ മാർഗ്ഗങ്ങൾ പ്രദാനം ചെയ്യുന്നു.

ഈ പേപ്പർ മൂന്ന് പ്രധാനപ്പെട്ട കാര്യങ്ങൾ കാണിച്ചിരിക്കുന്നു:

1. പൊതു ബ്ലോക്കിഞ്ചിന് സാമ്പത്തിക സേവനങ്ങളിൽ മൂല്യത്തെ ചേർക്കാൻ കഴിയും.
2. ഹൈഡ്രേ റെയിൻഡ്രോപ്പ് സ്വകാര്യ സംവിധാനത്തിന്റെ സുരക്ഷ വർദ്ധിപ്പിക്കും.
3. ഹൈഡ്രജൻ എപിഐ പ്ലാറ്റ്ഫോമിനുള്ളിൽ ഹൈഡ്രോ റെയിൻഡ്രോപ്പ് ഉടൻ പ്രയോഗങ്ങളുണ്ട്.

ഹൈബ്രിഡ് സ്വകാര്യ-പൊതു സംവിധാനത്തിന്റെ പുതിയ മോഡലിന് നിലവാരമുള്ള സുരക്ഷാ ഇൻഫ്രാസ്ട്രക്ചറാണ് രൂപകൽപ്പന ചെയ്തിരിക്കുന്നതെന്ന് ഹൈഡ്രോ ടീം വിശ്വസിക്കുന്നു, ഇത് സാമ്പത്തിക സേവന വ്യവസായത്തിലെയും അതിനപ്പുറവും എല്ലാ പങ്കാളികളെയും പ്രയോജനപ്പെടുത്തും.

ഉറവിടങ്ങൾ:

Ethereum; എഥെരെമിൽ മെർക്കുലിംഗ്
ട്രെൻഡ് മൈക്രോ; നിങ്ങളുടെ മോഷണ ഐഡന്റിറ്റി ഉപയോഗിച്ച് ഹാക്കർമാർ എന്തുചെയ്യുന്നു?
ജാവലിൻ സ്ട്രാറ്റജി & റിസർച്ച്; *ദി 2017 ഐഡന്റിറ്റി ഫ്രോഡ് സ്റ്റഡി*
Symantec; *ഇന്റർനെറ്റ് സെക്യൂരിറ്റി ട്രീറ്റ് റിപ്പോർട്ട്*
റിസ്ക് അടിസ്ഥാനമാക്കിയുള്ള സുരക്ഷ; *2016 ഡാറ്റാ ബ്രേക്ക് ട്രെൻഡ്സ് - റിവ്യൂ ഇൻ ദി റിവ്യൂ*
തലെസ്; *2017 തേൽസ് ഡാറ്റ ട്രീറ്റ് റിപ്പോർട്ട് - ഫിനാൻഷ്യൽ സർവീസസ് എഡിഷൻ*
Apache.org; Apache Struts 2 ഡോക്യുമെന്റേഷൻ - S2-052
ജോസഫ് പൂനും വിൽടിക് ബ്യൂറെറിനും; പ്ലാസ്മ: സ്കേലബിൾ ഓട്ടോണോമസ് സ്മാർട്ട് കോൺട്രാക്റ്റുകൾ