Block chain Technology LLC

Fisa Tehnica a proiectului Districts

Ultima actualizare: 11/10/2017

v 1.0.2

www.districts.io

Rezumat. In prezent, o parte tot mai mare a tranzactiilor si serviciilor fondurilor se realizeaza printr-un sistem monetar de tip peer to peer (P2P) cunoscut sub numele de Bitcoin; o criptomoneda open source dezvoltata de echipa lui Satoshi Nakamoto in 2008 si lansata in 2009. Sistemul se bazeaza pe tehnologia de criptografie publica si tehnologia blockchain, acordand un nivel fara precedent anonimatului. Exploatarea acestei tehnologii intr-o masura suplimentara vine de la Districts, o platforma de realitate virtuala 3D care promoveaza criptomonedele oamenilor fara expertiza in informatica, permitandu-le sa construiasca sau sa utilizeze aplicatii descentralizate intr-o lume vie, pentru o mai buna prezentare si gestionare a serviciilor, afacerilor, fara scrierea sau compilarea codului. In paralel, bazat pe codul sursa Bitcoin si Dash, cu un bloc de caractere caracterizat, care permite multe functii in Districts, va prezentam 3DCoin, noua noastra criptomoneda.

Cuprins:

1. Introducere
2. Proiectul Districts
3. Reteaua blockchain 3DCoin
4. Tranzactii conditionale
5. Aplicatii descentralizate
6. Visual Studio Districts
7. Token-uri
8. Concluzie

1. Introducere

Realitatea virtuala si reteaua Blockchain ar trebui considerate noi canale de prezentare, canale prin care utilizatorii pot lansa aplicatii intr-un spatiu sigur. Nu numai ca se poate elabora o prezentara bazata pe mai multe stiluri, dar ofera si avantaje de business: costuri mai mici, durata mai mica si abilitatea de a ajunge la audiente mari in mod efficient. Districts este un spatiu unde posibilitatile creative ale aplicatiilor descentralizate de magazine, servicii si management sunt nelimitate. Fiecare utilizator poate sa aleaga orice proiect il intereseaza. Este o platforma autoreglanta bazata pe criptomonede, care asigura elaborarea de prezentari atractive, impresionante si eficiente pentru proiectele utilizatorilor. Este o oportunitate pentru patronii afacerilor mici, care nu-si permit taxe de publicictate si au dificultati in a strange o baza de clienti. Platforma ii asista in activitati, ii ajuta sa isi prezinte mai bine magazinul, serviciile, afacerea. Misiunea noastra este de a ajuta utilizatorii sa fie parte a comunitatii criptomonedelor, prin promovarea proiectului nostrum, ce foloseste conceptul de realitate virtuala 3D, combinate cu avantajele retelei blockchain.

2. Districts:

Aducand toata lumea intr-un singur oras, cu o libertate totala de actiune si afisat cu o grafică de inalta calitate, dar foarte bine optimizat, Districts va fi locul unde visele tale se vor implini, cu tot felul de aplicatii descentralizate care vor rula alaturi, oamenii vor fi scufundati intr-o lume vie in care autovehiculele, casele, magazinele, terenurile de joc sau orice alta activitate imaginabila le va apartine; utilizatorul ramane complet fuzionat cu realitatea, deoarece serviciile pot fi furnizate atat in interiorul, cat si in afara districtelor, dand astfel o expunere maxima pentru intreprinderi la un cost mic.

Este conceput ca un ansamblu de platforme in formă de inele concentrice deasupra apei, iar centrul detine toate facilitatile de pornire care ofera tutoriale si exemple de aplicatii; alaturi de ele, primul inel serveste ca o vitrina cu cladiri inaugurale pre-fabricate care vor da nastere vietii districtelor; vor fi impartite in districte specializate, jocuri de noroc, afaceri si private. Cresterea ulterioara implica o creare treptata a altor platforme, fapt datorat de saturarea celor vechi.

Optiunile de miscare sunt multiple, atat in modul standard, cat si in modul VR, transferul fluidelor directionate pentru deplasări scurte sau lungi, miscari prin dispozitive precum plachete de hover sau vehicule de toate felurile, care pot fi personalizate. Deplasarea nelimitata pe jos pentru VR nu este posibila cu tehnologia actuala, iar implementarea sa se va face in viitor.

Realismul adus de VR trebuie, de asemenea, urmat de realism in comunicare; acesta este motivul pentru care chat-ul de proximitate vocala este implementat, dar sunt disponibile si moduri traditionale, cum ar fi “Voice on IP” pentru simularea smartphone-urilor sau mesagerie text criptata si posta electronică.

Pentru **afaceri,** acest fenomen de scufundare creste toate interactiunile posibile: cu dezvoltatori imobiliari, de automobile sau chiar dealeri vestimentari; acesstia vor putea sa

isi prezinte produsele si personalizarile posibile intr-o maniera realistica si plina de viata. Acestea sunt expuse in spatiul orasului sau chiar in instante accesibile dintr-un magazin sau mall. Achizitionarea clientilor va fi mai simpla si mai ieftina datorita stimulentelor disponibile si reinnoite, care le sunt induse de prezenta unor activitati interesante in fiecare colt al orasului digital Districts. Oamenii vor fi mereu in tranzit. Acest lucru se datoreaza libertatii care permite comunitatii sa-si exprime toata creativitatea.

Aveti abilitatea de a vizita de la distanta o casa sau o camera de motel si de a inspecta fiecare colt al acesteia, de a incerca mobilierul intr-un model virtual al casei dvs. si de a vedea ce vi se potriveste cel mai bine. Puteti sa vizualizati si sa experimentati o masina in medii diferite, fapt ce va imbunătăţi procesul de luare a deciziilor si va oferi clientilor o mai mare satisfactie.

In afara Districts, eforturile creatorilor sunt puternic impozitate in moduri diferite, in Districts, nu exista astfel de taxe. Toate veniturile vor merge pe deplin la proprietarii lor de drept.

Jocurile de noroc din VR zdruncina fiecare experienta anterioara, deoarece ofera jucatorilor sansa de a trai actiunea in loc sa declanseze functii simple si indepartate. Dar lucrurile se transforma incet, deoarece dezvoltarea jocului necesita abilitati complexe, in special de codare. In Districts, consideram ca posibilitatea ca toata lumea sa-si aduca ideile la viata prin utilizarea versiunii Visual Studio va declansa o crestere in acest domeniu.

Educatie: Invatarea online arata o rata ridicata de abandon scolar, mai putin de cinci la suta din elevii inscrisi termina cursurile, iar motivul evident este ca metodele obisnuite nu reusesc sa mentina motivatia elevilor pe aceasta tema, acestia se plictisesc si devin inactivi. Imaginati-va o clasa de fizica in care elevii sunt transportati in fata unui oras asediat pentru a afla despre balistici prin utilizarea unui catapult sau o clasa de programare care sa ofere fiecarui elev posibilitatea de a-si codifica propriul robot personalizat si de a vedea cum devine din ce in ce mai avansat, in timp ce abilitatile de codificare ale cursantului cresc. Invatarea va inceta sa fie plictisitoare atunci cand se face in scene epice si cu tot felul de setari interactive.

Sanatatea mintală poate profita foarte mult de VR, deoarece senzatia de prezenta a unei persoane care ingrijeste are un efect mai bun ca orice alta interactiune online, cum ar fi dialogul textual sau chiar videoconferintele. Adunari virtuale anonime pentru sprijin psihologic, terapie, tratament personalizat pentru fobie cu mediu personalizat, ajutand pacientul sa-si confrunte treptat temerile, sa traiasca sesiuni ASMR unde specialistul se poate misca in jurul audientei si ii poate da acesteia cea mai intensa si realista atentie. Acestea sunt cateva din functionalitatile pe care ni le propunem.

Oferta de locuinte private ofera utilizatorilor posibilitatea de a crea un spatiu personalizabil, care ar putea avea multe scopuri, cum ar fi adunarea prietenilor la fata locului, vizionarea unui film mpreuna, jocuri arcade sau jocuri de carti, chiar o galerie. Gazda trebuie sa fie online pentru ca altii sa acceseze spatiul privat.

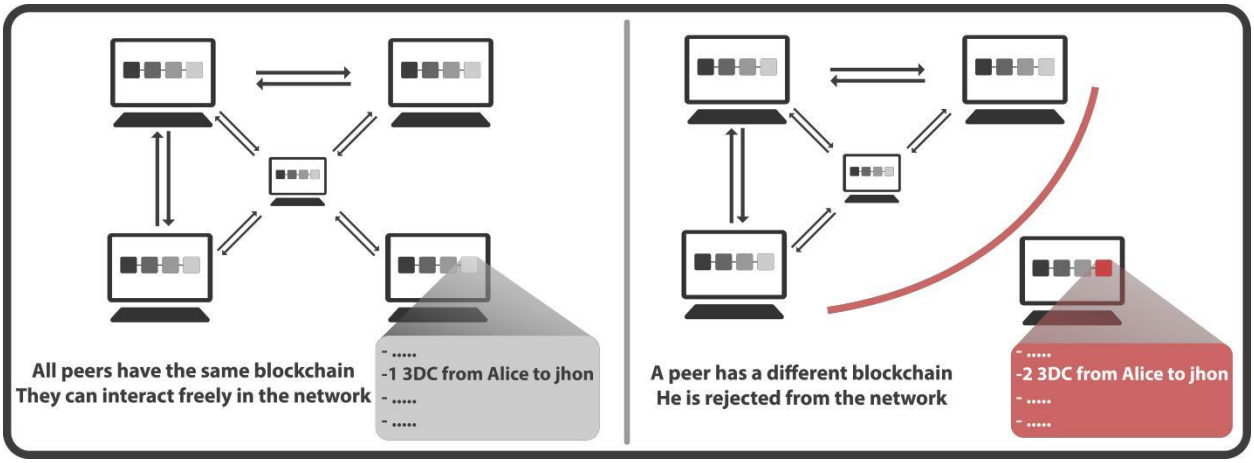
Descentralizarea este un element cheie al proiectului nostru, nu exista nicio autoritate centrala, ceea ce in seamna ca tot controlul continutului este in mainile comunitatii, printr-un sistem de votare.

Toate datele, exceptand datele personale ale utilizatorilor, vor fi stocate in reteaua blockchain **3DCoin,** care nu serverse doar pe post de criptomoneda.

3. Reteaua blockchain 3DCoin

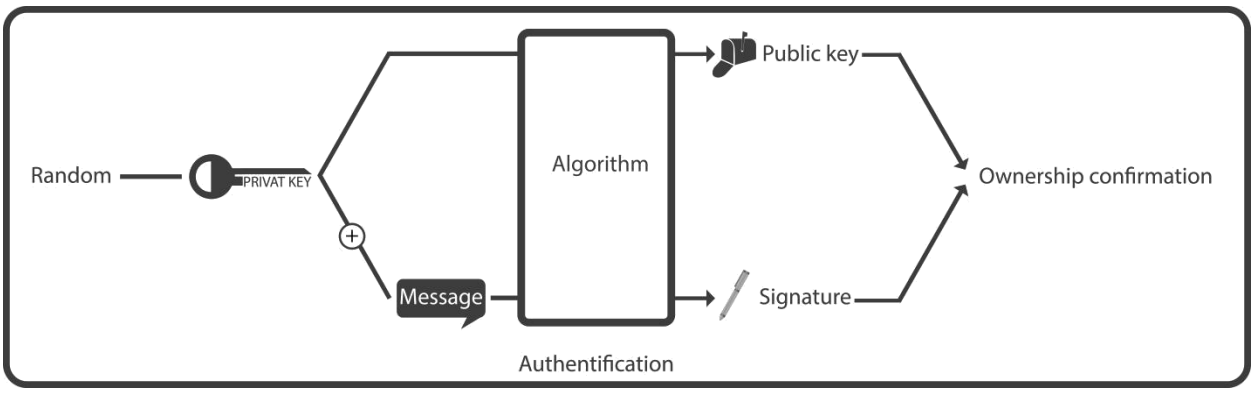
3DCoin este o noua criptomoneda pe care am dezvoltat-o. Protocolul foloseste Bitcoin si Dash ca baza pentru codul sursa, pentru a mosteni siguranta si puterea acestor monede, la acestea fiind adaugate si alte functionalitati, corespunzatoare cerintelor Districts.

Reteaua blockchain este un sistem unde stocarea si autentificarea datelor, precum si operatiunile sunt efectuate intr-o modalitate transparenta si cumulata, de fiecare computer care ruleaza protocolul respectiv, oferind utilizatorilor o cunoastere completa si un control colectiv asupra procesului. Actualizarile nu pot fi facute fara un acord, spre deosebire de sistemele uzuale, care se bazeaza pe o entitate centrala. Functiile matematice fac toate sarcinile, iar codul are o natura open-source. Reteaua blockchain este ca un registru public, sau ca un server descentralizat pentru aplicatii. [1]

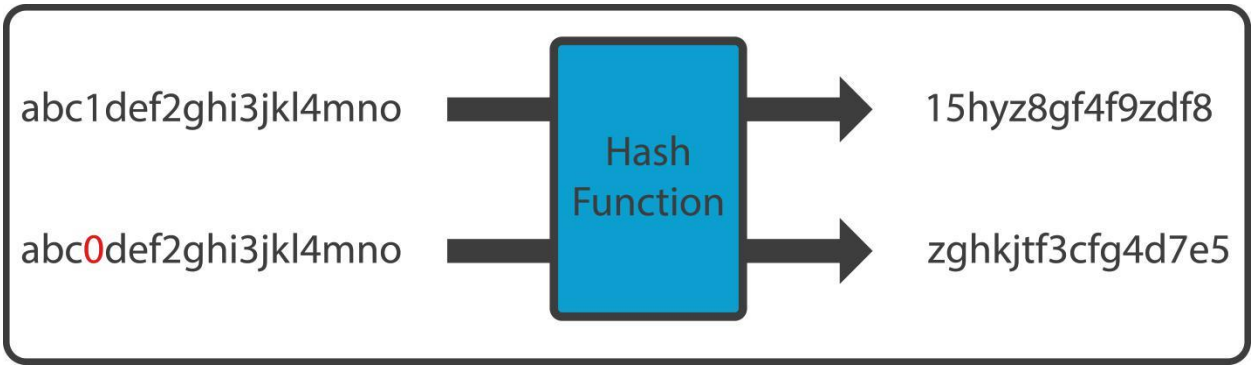


Identitatea se bazeaza pe o cheie publica, foloseste perechi de chei: una privata care trebuie tinuta secret de catre utilizator, legata printr-o functie eliptica de o cheie publica, o adresa pentru a primi banii. Cand posesorul vrea sa cheltuiasca monedele 3DCions, poate face o cerere, insotita de semnatura sa virtuala. Reteaua va verifica daca mesajul vine de la proprietarul contului si va confirma tranzactia.

Sistemul 3DCoin permite utilizarea multor metode de criptare a cheilor publice, imbunatatind siguranta si permitand utilizarea cheilor deja existente de la alte criptomonede, sau alte sisteme. De exemplu, daca folosesti o cheie PGP pentru emailurile tale, vei putea sa o folosesti pentru a obtine token-uri 3DCoin.



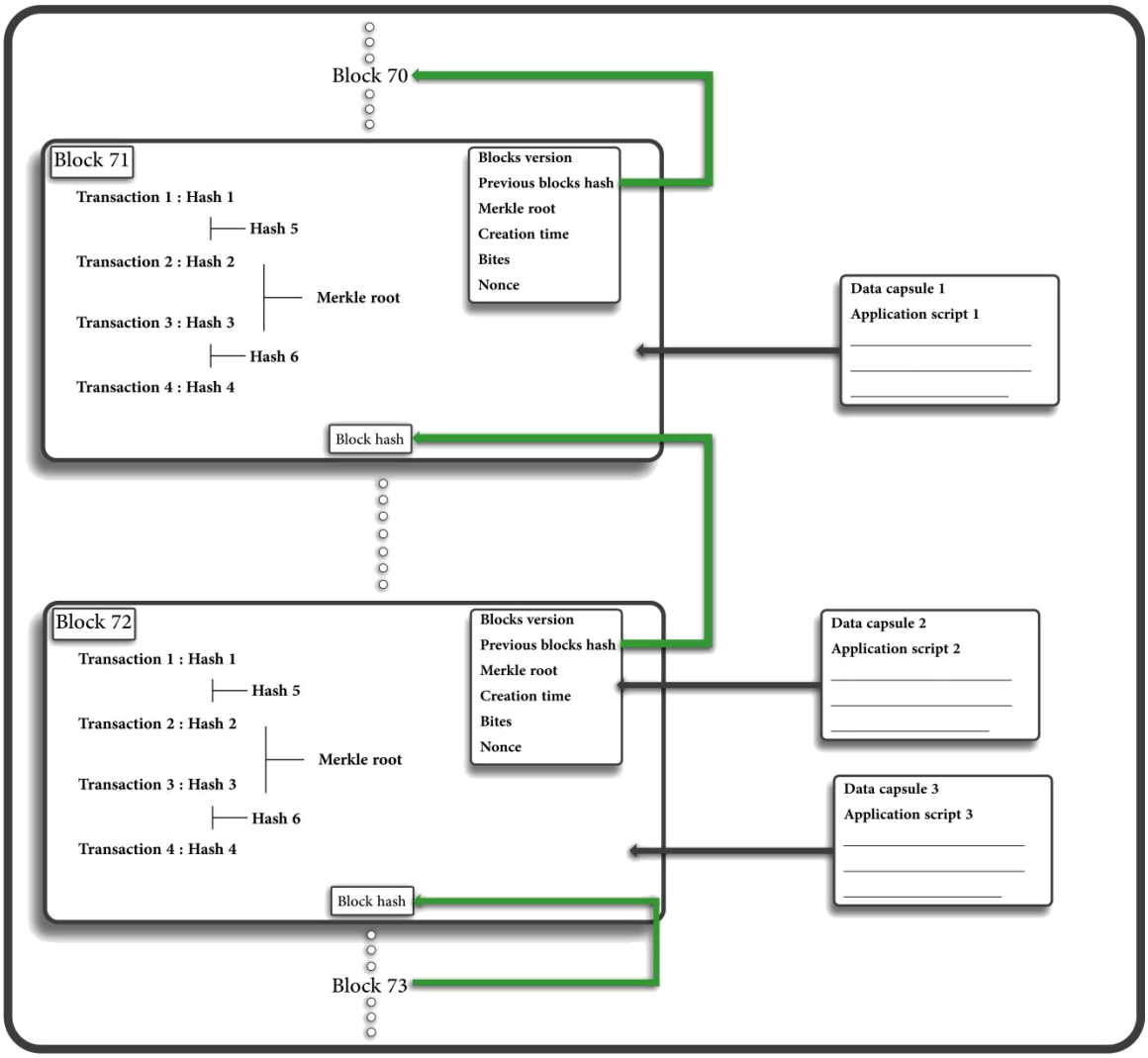
Hash = serie de caractere generate de o functie cu sens unic din alte serii. Datele introduse se transforma intr-un set de date de iesire, care se schimba drastic in functie de modificarile codului initial. De aceea, hashing-ul este nucleul autentificarii. [2]



Un copac **Merkle** este o metoda rapida si sigura de a verifica continutul unor structuri mai de date, deoarece e altacuit dintr-o secventa de coduri hash care se termina cu un singur hash, nodul **Merkle.** Acest arbore este bazat pe tranzactii.

Blocuri: Datele de toate tipurile, istoric de tranzactie sau referinte ale versiunilor, sunt inregistrate in reteaua blockchain, care e alcatuita din blocuri de 8 Mb care sunt legate pentru a forma un lant simplu, unde fiecare bloc se refera la suma hash anterioara. Din cei 8 Mb, 1 va fi alocat tranzactiilor mici, netaxabile.

Fiecarui bloc ii pot fi atribuite mia multe **Capusule de date**; acestea tin codul aplicatiilor descentralizate, iar marimea acestora are dimensiunea maxima de 1 Mb.

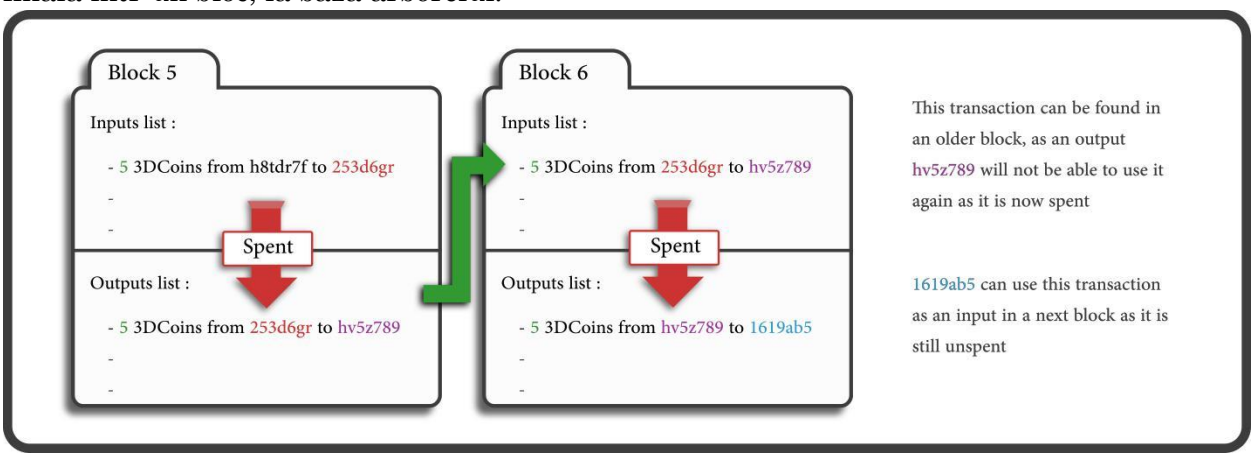


Tranzactii si sold:

Tranzactiile sunt unitatile inalterabile din care se calculeaza soldul, ele detin cantitatea de token-uri 3DCoin transferate, cheia publica a expeditorului si a receptorului. O tranzactie cuprinde o microtaxa platita de expeditor catre mineri; acesta poate creste cu dimensiunea tranzactiei, deoarece tranzactiile pot avea atasate script-uri, acestea fiind utilizate pentru programarea tranzactiilor sau pentru a defini proprietatea asupra parcelelor de teren si a aplicatiilor descentralizate in raioane.

Spre deosebire de un registru normal, soldul in reteaua blockchain nu este notat ca o anumita suma, este definit de istoricul tranzactiilor inalterabile salvate periodic pe blocuri. Aplicatia portofel va rasfoi intregul blockchain in cautarea tranzactiilor necheltuite si va calcula soldul de la acestea.

Cand utilizatorul doreste sa trimita bani, **aplicatia portofel** va transmite un mesaj care contine tranzactiile primite pe care doreste sa le utilizeze, o tranzactie de iesire directionată catre cheia publica pe care doreste sa o transfere. Verificarile atat a proprietatii cat si a suficientei intrarilor sunt efectuate de catre colegi, pana la adaugarea finala intr-un bloc, la baza arborelui.



Tranzactiile care definesc posesia de teren sau a unor aplicatii decentralizate, nu au token-uri asupra lor. Ele se refera la Capusla de Date care pastreaza scriptul aplicatiei, posesorul si coordonatele parcelei.

Codul:

3DCoin foloseste un sistem de codare al tranzactiilor; Acesta este ca o stiva si proceseaza de la stanga la dreapta.

Acesta nu are bucle si nu este complet de tip Turing.

Un script este in esenta o lista de instructiuni inregistrate, unde fiecare tranzactie care descrie modul in care urmatoarea persoana care doreste sa transfere 3DCoin poate obtine acces. Scriptul pentru un transfer tipic 3DCoin catre o adresa D (o adresa este hash-ul unei chei publice) pur si simplu impovareaza cheltuielile viitoare ale 3DCoin cu doi factori: cel care cheltuie trebuie sa furnizeze:

O cheie publica care, atunci cand este aplicata asupra ei o functie hash, produce adresa de destinatie D incorporata in script.

O semnatura care sa ateste cheia privata corespunzatoare cheii publice furnizate.

Exista un grad de flexibilitate, putandu-se schimba parametrii a ceea ce este necesar pentru a cheltui token-urile 3DCoin transferate. De exemplu, sistemul de scripting ar putea fi folosit pentru a solicita doua chei private sau o combinatie de mai multe sau chiar nici o cheie. [3]

O stiva e o structura de date bazata pe principiul <LIFO>: *last in first out (ultimul sosit, primul plecat)*, ceea ce inseamna ca ultimul element adaugat este primul eliminat; exista 2 operatori: **Push**: adauga element in stiva si **Pop**: elimina elementul din stiva.

Specificatiile codului 3DCoin

Pentru a imbunatati posibilitatile de programare, multe operatii standard, in cazul in care sunt imbunatatite, vor avea ca efecte directe: o mai buna citire a scripturilor si o scadere masiva a complexitatii planificarii codului, in loc sa existe o operatiune limitata care sa interactioneze numai cu anumite elemente de stiva, programatorul va putea folosi stiva in toată dimensiunea sa cu comenzi extrem de scurte. Prefixul OP a fost eliminat, deoarece limitarea pe care a fost setata sa o obtina a devenit irelevanta (numele functiilor nu pot incepe cu un numar). Nu exista mai multe variante multiple ale unei functii, variantele sunt unificate intr-o singura functie care accepta argumentele impinse anterior in stiva .

De exemplu:

Bitcoin are trei operatiuni de duplicare (OP_1DUP, OP_2DUP, OP_3DUP), primele duplicate la elementul de varf, al doilea copiaza cele doua elemente de top si cel de-al treilea duplicat.

Duplicarea se face acum cu o singură functie, DUP (fara op), pentru a duplica un element, un numar <x> trebuie sa fie impins inainte de executarea DUP, <x> reprezinta locul in stiva. Daca argumentul este facut din mai multe numere separate prin virgule <x, y, z>, inseamna ca mai multe elemente sunt duplicate, operatia DUP va citi elementul, va efectua operatiunea conform argumentului, daca argumentul este compus din doua numere separate printr-o linie, va fi considerat ca fiind un interval, <xy>, toate elementele de la x la y sunt duplicate. Aceeasi imbunatatire este adusa si altor functii.

Optimizarea inteligenta a codului se realizeaza automat prin reducerea pasilor inutili care ar pot fi facuti, rezultand scripturi mai scurte, dar la fel de functionale, economisind alocarea spatiului in blocuri si in Capsule de date.

Modulul de verificare a script-urilor adauga un nivel de siguranta prin verificarea tuturor secventelor posibile de operare si a argumentului, permitand doar tranzactii fara bug-uri si intotdeauna accesibile, iar aplicatia descentralizata trebuie sa fie acceptata in retea, acest lucru fiind realizat de toti colegii.

Codul este scris cu cuvinte cheie care inseamna functii si este executat de la stanga la dreapta [4]; mai jos aveti un exemplu de cod**:**

⟶<numberA><numberB> <1,2> EQUAL, de la stanga la dreapta:

<numberA> impinge numarul A in stiva
<numberB> impinge numarul B in stiva
<1,2>Argumentul functiei EGAL este adaugat in stiva.
EQUAL adauga armulentul, verifica egalitatea dintre cele 2 elemente (<1,2>Primul si al doilea element din stiva) si le elimina, apoi adauga 1 daca operatia este adevarata si 0, daca nu.

Acesta este codul pentru o **tranzactie standard** (o combinatie intre 2 coduri):

scriptSig (<sig> <pubKey>), gasit in tranzactia **de iesire**.
scriptPubKey, gasit in tranzactia **de intrare** (<1> DUP <160>HASH <pubKeyHash> <1,2><EQUALVERIFY <1,2>CHECKSIG).

Combinate:

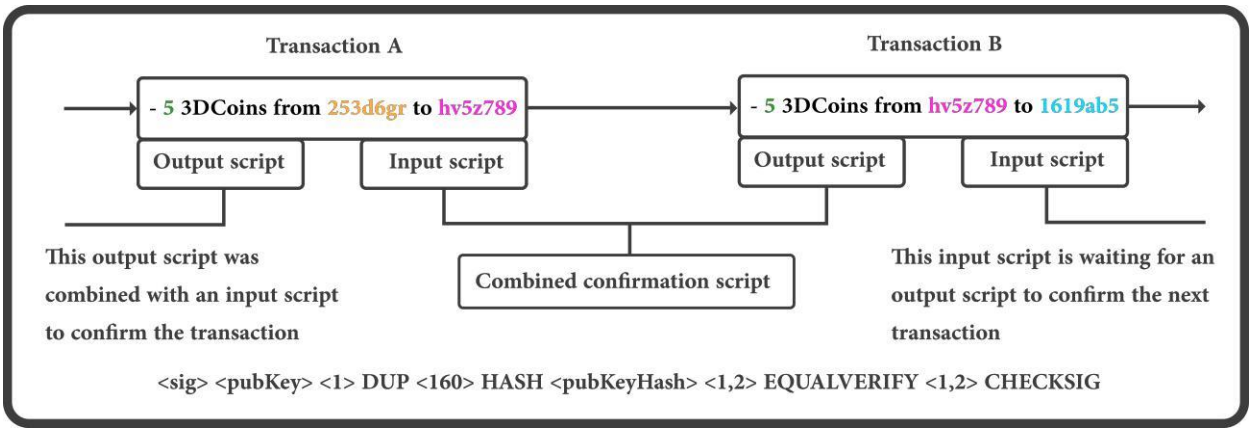
⟶ <sig> <pubKey> <1>DUP <160>HASH <pubKeyHash> <1,2>EQUALVERIFY <1,2> CHECKSIG

Acest cod incepe prin a verifica daca cheia publica afisata de cel care trimite suma de token-uri este acceasi ca cheia publica de intrare si apoi verifica semnatura. **(De retinut**: Operatiunile elimina argumentele din stiva)

1- <sig> adauga semnatura in stiva; <pubKey> adagua cheia publica in stiva.
2- <1> Argument pentru functia DUP.
3- DUP copiata elementul cu care incepe stiva (pubKey) si apoi adauga o copie in stiva.
4- <160> Argument pentru funtia HASH.
5- HASH, elementul cu care incepe stiva (pubKey) este eliminat, ii este efectuata o functie hash, apoi rezultatul este adaugat la stiva.
6- <pubKeyHash> adauga hash-ul cheii publice in stiva.
7- <1,2> Argumentele functiei EQUALVERIFY.
8- EQUALVERIFY elimina argumentul, verifica egalitatea dintre primele elemente ale stive si apoi le elimina, adauga True (Adevarat) in stiva, daca rezultatul este egal, apoi il elimina, daca rezultatul nu este egal.
9- <1,2> Argumente pentru functia CHECKSIG.
10- CHECKSIG, verifica semnatura cu primele 2 elemente ale stivei (sig si pubKey), apoi le elimina din stiva, intoarce valoarea True cand este corecta operatia, ceea ce inseamna ca tranzactia este confirmata. In caz contrar tranzactia este anulata.

Operatiuni	**Stiva**
	Goala
<sig><pubKey><1>	<sig><pubKey><1>
DUP	<sig><pubKey><pubKey>
<160>	<sig><pubKey><pubKey><160>
HASH	<sig><pubKey><pubHashA>
<pubKeyHash>	<sig><pubKey><pubHashA><pubKeyHash>
<1,2>	<sig><pubKey><pubHashA><pubKeyHash><1,2>
EQUALVERIFY	<sig><pubKey>
<1,2>	<sig><pubKey><1,2>
CHECKSIG	TRUE

Concluzie: Toate tranzactiile contin atat un script de iesire, cat si un script de intrare, de fiecare data cand un utilizator doreste sa-si petreaca o tranzactie existenta, trebuie sa livreze un script de iesire corect care, atunci cand este combinat cu scriptul de intrare, rezulta intr-un nou script de intrare in noua tranzactie de iesire pentru a defini viitoarele conditii de cheltuieli. Scripturile sunt generate automat de aplicatia portofel, dar pot fi si scrise manual.



Noduri

Acestia sunt contribuitorii care trebuie sa detina o intreaga copie a blocului, sarcina lor consta in colectarea, verificarea si asamblarea tranzactiilor intr-o anumita ordine pentru a pregati crearea blocurilor, dar numai un singur bloc poate fi adaugat lantului la un moment dat. Acesta este motivul pentru care se utilizeaza mecanismul de extractie.

Activitatea miniera are scopul de a oferi o dovada a muncii; scopul este de a reduce probabilitatea de a crea doua blocuri in acelasi timp si se efectueaza prin rularea unui set de date unice prin intermediul algoritmului de hashing NIST5, care este o combinatie a celor 5 finalisti în competiţia pentru functia hash NIST (BLAKE, Grøstl, JH, Keccak, Skein); atunci cand seria de numere rezultate intruneste anumite criterii, blocul este considerat a fi exploatat si este difuzat in reteaua care urmeaza sa fie adaugat la reteaua blockchain dupa ce a luat valoarea functiei hash. (Mineritul se poate face cu procesorul GPU, dar si cu alte dispozitive hardware)

Odata ce un bloc este extras, o recompensa care consta in token-uri 3DCoin este distribuita intre mineri (50%), operatori de Super noduri (45%) si rezervei de dezvoltare (5%). Aceasta este metoda unica de generare a token-urilor 3DCoin.

In cazuri foarte rare, mai multe blocuri sunt minate in acelasi timp, prezentand o situatie in care colegii au un ultim bloc diferit adaugat blocului lor, in acest caz se sincronizeaza pur si simplu cu cel mai bun lant majoritar. Atunci cand puterea de calcul creste in retea (rata de hashing), fie prin cresterea numarului de mineri, fie prin performanta lor hardware, trebuie sa se faca o compensare prin cresterea dificultatilor miniere, mentinand astfel o rata de productie buna a blocurilor si consensul pe un singur lant.

Super noduri

Detinatoul unui **nod,** il poate transforma intr-un **Super nod,** folosind **1.000** de token-uri 3DCoin, pe care le poate recupera oricand, acest lucru facand posibila contrinutia la diferite functii. Utilizatorul va primii premii pentru aceasta activitate, pentru a-l motiva sa ia cele mai bune decizii, deoarece va avea de castigat in mod direct de pe urma acestor decizii. Functiile acestea sunt:

- Votul pentru controlul continului.
- Participarea la serviciul de tranzactii instant.
- Gazduirea de evenimente de amestec al token-urilor.

Rezerva de dezvoltare

5% din recompensa pe bloc va fi alocata fondului de rezerva; acesta va plati pentru proiectele care obtin token-uri 3DCoin la finalul lunii. Plata din rezerva va fi folosita si pentru a recompensa dezvoltatorii si contribuitorii, de asemenea vor sprijini integrarea caselor de schimb importante si a furnizorilor de API-uri.

Operatorul super nodului va primi un vot, pe care il va folosi in favoarea propunerii pe care vrea sa o spijine si voturile for fi sustinute intr-o maniera corespunzatoare.

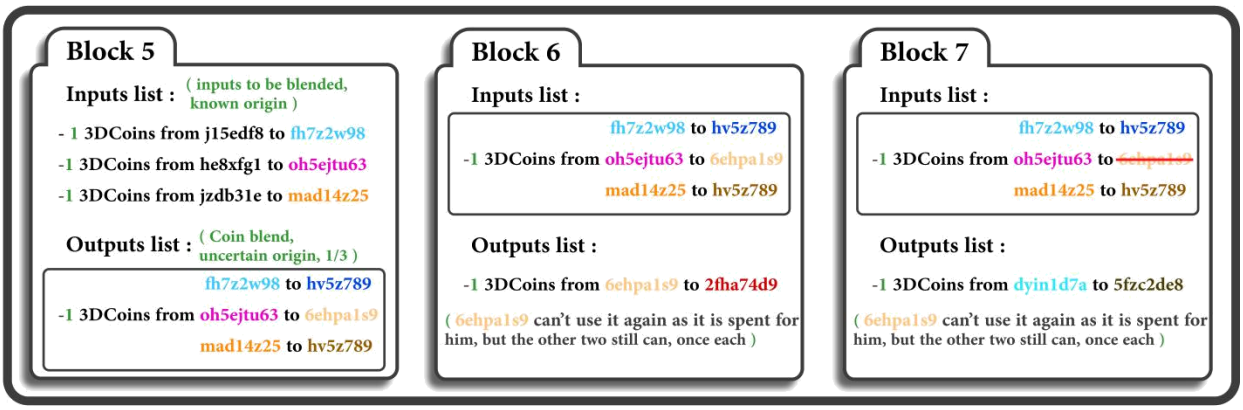
Amestecul monedelor

Cateva utilizari ale cheii publice dezvaluie identitatea detinatorului, ca o comanda fizica, in care cheia si adresa de livrare pot fi legate, sau ca plasarea unei chei intr-o semnatura pe forum pentru donatii. Pentru a reobtine anonimitatea fondurilor, va oferim serviciul de amestec al token-urilor.

Cererea de amestec incepe prin aplicatia portofel, unde utilizatorul selecteaza tranzactia pe care vrea sa o anonimizeze, iar portofelul o va fragmenta in denumirea standard (10, 1, 0.1, and 0.01), pentru a facilita operatiunea administrata de un super nod; apoi verifica lista existenta de super noduri si selecteaza aleator unul din ele, folosind o suma hash a unui bloc, pentru a maximiza gradul de randomizare.

Tranzactia este plasata intr-o coada de amestec, atunci cand sunt gasite 3 variante potrivite pentru o denumire standard; Super nodul lanseaza o alerta, ce semnaleaza ca sesiunea de amestec poate incepe catre cele 3 aplicatii portofel, iar sesiunea de amestec incepe in urma confirmarilor celor 3 utilizatori.

Fiecare din aceste 3 portofele trimite si datele de intrare ce trebuie mixate si o noua cheie publica, care va primi fondurile anonimizate. Apoi, super nodul va crea o tranzactie tripla ce va contine 3 date de intrare si cheile publice de primire a token-urilor. Tranzactia este trimisa catre cele 3 portofele, acestea verifica exactitatea datelor de intrare si a cheilor publice, semneaza tranzactia si o trimit inapoi la super nod. In acest moment, super nodul are o tranzactie tripla cu 3 semnaturi, dupa o ultima verificare finala, tranzactia este trimisa ca orice alta, urmand sa fie adaugata intr-un bloc minat si, apoi in reteaua blockchain.



Rezultatul: o tranzactie ce contine 3 date de intrare egale, care pot fi cheltuite, odata ce fiecare va primi o cheie publica. Acestea vor fi create pe loc, asa incat nimeni nu poate stii cui ii apartin, deoarece niciuna din cele 3 date de intrare nu se refera la o anumita cheie.

Tranzactii instant

Chiar daca tranzactiile dureaza cateva minute pentru a fi confirmate in bloc, nu este suficient de rapid pentru acest mediu, unde bunurile sunt destinate sa fie livrate instantaneu. Va vom prezenta mai jos un nou tip de tranzactie, cea instantanee:

Procesul este orchestrat de 10 super noduri selectate aleatoriu; acestea sunt schimbate de fiecare data cand un bloc este minat. Cand se trimite o solicitare de tranzactie instant, super nodurile apeleaza intreaga retea pentru a bloca intrarea care va fi tratata; orice tranzactie care o utilizeaza va fi respinsa. Odata ce intreaga retea este sincronizata pe dispozitivul de blocare, super nodurile vor verifica si apoi vor confirma tranzactia instantanee. Chiar daca nu sunt salvate pe bloc, in cele din urma si aceste tranzactii vor fi difuzate ca orice alta tranzactie si tratate ca atare.

Se poate pune urmatoarea intrebare: de ce nu toate tranzactiile sunt instantanee daca sunt atat de sigure? Este posibila optiunea de a efectua toate tranzactiile dvs. instantaneu in mod implicit, dar aceste tranzactii necesita mai multa munca in retea, costand astfel mai mult. De asemenea, instantaneitatea nu este necesara pentru toate operatiile, cateva minute de asteptare nu sunt asa o mare pierdere, avand in vedere ca in prezent lumea asteapta 2-3 zile pentru un produs comandat.

Gazduire descentralizata

Toate scripturile de aplicatii sunt codificate si stocate in Capsulele de date, eliminand necesitatea unui server central sau, cel putin, facandu-l optional. Spatiul Districts va fi impartit intre noduri, deoarece acestea nu numai ca gestioneaza mesajele si blocurile, ci si gazduiesc actiunile si evenimentele care au loc in Districts, economia de latime de banda se va face printr-o prioritate de incarcare bazata pe intervale; actiunile nu vor fi incarcate dincolo de o anumita distanta. Pentru jocuri, a fost elaborata o metoda peer-to-peer care combina modele descentralizate si distribuite, in loc sa comunice direct intre ele; colegii folosesc nodurile ca poduri pentru a obtine o mai buna routare si o sincronizare mai rapida.

Sub-Monede

Activele personalizate non-fungibile pot fi create cu aplicatia portofel; aceasta creare consta intr-o conversie reversibila de la 3DCoin, numele trebuie sa fie ales de catre utilizator, deoarece rata este intotdeauna 100 de sub-monede la 1 3DCoin, pot fi folosite sub-monede cum ar fi token-uri, actiuni, cupoane. De exemplu, 100 SC ar putea fi create pentru a reprezenta stocul unei societati (100%), si, apoi, distribuit intre actionari, apoi tranzactionat in mod liber.

In reteaua blockchain, sub-monedele sunt doar token-uri 3DCoin codate pentru a fi percepute diferit de catre **aplicatia portofel.** [5]

Asistenta adresei externe

Multe metode de criptografie sunt oferite utilizatorilor, inclusiv celor ale altor criptomonede; acest fapt inseamna ca reteaua noastra poate accepta orice cheie publica din orice alta criptomoneda, simplificand astfel gestionarea mai multor conturi. Puteti primi token-uri 3DCoin prin cheia veche, fara a fi nevoie sa creati un cont nou. Obiectivul nostru pe termen lung este generalizarea acestei utilizari intre toate criptomonedele, permitand oamenilor sa aleaga o cheie universala. Aceasta se va intampla numai atunci cand cele mai multe criptomonede vor conveni asupra unui algoritm comun de verificare a semnaturii.

Tranzactiile pot fi simple comenzi de transfer, dar protocolul nostru aloca o portiune importanta scripturilor din spatiul blocurilor, facand posibila implementarea unor functii precum ar fi tranzactiile conditionate, pe langa tranzactiile standard.

4. Tranzactiile conditionate

Tranzactiile pot fi programate pentru a fi primite numai daca sunt indeplinite anumite conditii, oferind un spectru larg de optiuni in ceea ce priveste operatiile automatizate. Conditiile mentionate sunt scrise in scriptul atasat tranzactiei.

Un instrument vizual simplu va fi disponibil in **aplicatia portofel** pentru a seta astfel de tranzactii; mesajul difuzat care rezulta contine scriptul de tranzactie si conditiile. Parametrii principali conditionali sunt timpul, cheia publica si parola. Cateva exemple de tranzactii conditionate:

1- **Exemplu abstract:**

Bob ii trimite token-uri 3DCoin lui **Alice**, **Alice** le poate folosi avia dupa 24 de ore, cu o anumita **Cheie publica,** folosind o anumita **parola**, iar daca banii nu sunt cheltuiti in 48 de ore, banii se intorc la **Bob**.

2- **Exemplul setarii de livrare**:

Alice ii trimite token-uri 3DCoin protejate cu **parola** lui **Bob, Bob** ii trimite un produs lui **Alice; Bob** va avea acces la token-uri abia dupa ce **Alice** va introduce **parola** in aplicatia mobila **3DCoin** ce ruleaza pe telefonul mobil al curierului. Codul:

Cod de iesire: <sig><pubKey><password>
Cod de intrare: <160>HASH <SavedPassHash> <1,2> EQUALVERIFY <1>DUP <160>HASH <pubKeyHash> <1,2>EQUALVERIFY <1,2>CHECKSIG

In stiva:

Operatiune	**Stiva**
	Goala
<sig><pubKey><password>	<sig><pubKey><password>
<160>HASH	<sig><pubKey> passHash>
<SavedPassHash>	<sig><pubKey><passHash><SavedPassHash>
<1,2>EQUALVERIFY	<sig><pubKey>
<1>DUP	<sig><pubKey><pubKey>
<160>HASH	<sig><pubKey><pubHashA>
<pubKeyHash>	<sig><pubKey><pubHashA><pubKeyHash>
<1,2>EQUALVERIFY	<sig><pubKey>
<1,2>CHECKSIG	TRUE

3- **Exemplul unui escrow securizat**: (generat automat de catre aplicatia portofel)

Bob ii trimite token-uri 3DCoin unui **escrow** (**J**ohn)- administrator financiar, **J**ohn ii poate trimite token-urile doar lui **A**lices prin intermediul **cheii publice** sau ii poate returna **cheii publice** al lui **B**obs, dar nu le poate folosi el, daca nu ajung la **A**lice intr-o **luna**, banii se intorc la **B**ob.

Definirea funcitilor:

DUP: Considera ca argument primul element din stiva, il elimina si apoi copiaza noul prim element din stiva.

CUT: Executa functia **DUP**, si elimina elementul initial.

IF: Verifica primul element din stive, daca este 0, il elimina si executa operatiile ELSE, iar daca nu este 0, executa operatiile IF.

HASH: Considera ca argument primul element din stiva, il elimina, citeste noul element prim din stiva, ii aplica o functie hash, il elimina din stiva si adauga in aceasta suma hash calculata.

EQUALVERIFY: Verifica egalitatea dintre primele 2 elemente ale stivei; daca sunt egale, codul continua, daca nu, codul este finalizat si tranzactia este refuzata, iar ambele elemente sunt eliminate din stiva.

CHECKTIME: Daca valoarea primului element din stiva este mai mica decat timul Unix actual, se adauga valoarea TRUE (adevarat) in stiva, iar daca este mai mare, se adauga valoarea FALSE (fals).

Definirea constantelor:

<Time>: Adauga termenul limita (Unix Time) definit de care Bob in stiva.

<pubKey>: Cheia publica a persoanei care initiaza tranzactia, a celuia care trimite token-uri.

<pubKeyTo>: Cheia publica a persoanei care trebuie sa primeasca token-urile 3DCoin.

<PubKeyHashA,B,J**>:** Adresele stocate ale lui Alice, Bob si John.

Output script: <pubKeyTo><sig><pubKey>
Input script: <Time>CHECKTIME IF <1>DUP <160>HASH <PubKeyHash**B**> <1,2>EQUALVERIFY ELSE <1>DUP <160>HASH <PubKeyHash**J**> <1,2> EQUALVERIFY ENDIF <3>CUT <160>HASH <PubKeyHash**A**> <PubKeyHash**B**> 3,1 | 2 EQUALVERIFY <1,2>CHECKSIG

Codul incepe prin a verifica termenul limita si persoana care initiaza tranzactia.

Daca conditiile sunt satisfacute, cel care primeste token-urile 3DCoin poate ori sa cheltuiasca suma direct, sau poate sa salveze tranzactia. In acest caz, va primi din partea tranzactiei conditionale, o tranzactie standard gratuita.

Cand este trimisa o tranzactie conditionala, este insotita intotdeauna si de un timp de intoarcere care poate fi schimbat, obiectivul fiind evitarea situatiilor in care token-urile sunt blocate, deoarece cel care primeste suma nu indeplineste cerintele corespunzatoare.

5. Aplicatiile descentralizate

Dapp-urile sunt cele care folosesc tehnologia blockchain. Partea vizuala este tinuta in biblioteca virtuala a clientului Districts, dar scriptul, care este generat de Districts Visual Studio, se afla in blockchain, intr-o Capsula de date, eliminand costurile de gazduire si scazand timpul necesar unei astfel de operatiuni. De exemplu, cand se utilizeaza un model 3D, pozitia si alte proprietati, vor merge in bloc, dar fisierul model sau textura vor fi incarcate de pe PC-ul utilizatorului unde este instalat clientul. Dapp-urile pot varia de la jocuri la platforme educationale sau magazine si showroom-uri, care vor vinde haine, case, produse alimentare sau produse virtuale: programe, servicii de gazduire; nu exista literalmente nicio limita cu privire la ceea ce pot fi Dapp-urile.

Proprietatea asupra Dapp-ului este definita intr-o tranzactie codificata, una care nu detine token-uri 3DCoin, ci se refera la Capsula de date in care este salvat scriptul Dapp.

Un Dapp poate fi utilizat in mod liber sau conditionat, dar numai proprietarul poate modifica codul sau. Scripturile vor fi codificate pentru a avea o dimensiune foarte mica, in timp ce vor fi specifice clientului, ceea ce inseamnă ca pot rula numai cu clientul Districts, asigurand o siguranta maxima, deoarece posibilele functii pe care le poate utiliza un script sunt bine definite si generate numai de DVS.

Orice modificare sau actualizare se va realiza printr-o tranzactie actualizata codificata, transmisa, apoi verificata de retea. Daca un script detine functii nerecunoscute, actualizarea este respinsa.

Pentru a ne sustine obiectivul de a face crearea aplicatiilor accesibila tuturor, am elaborat platforma **Districts Visual Studio**.

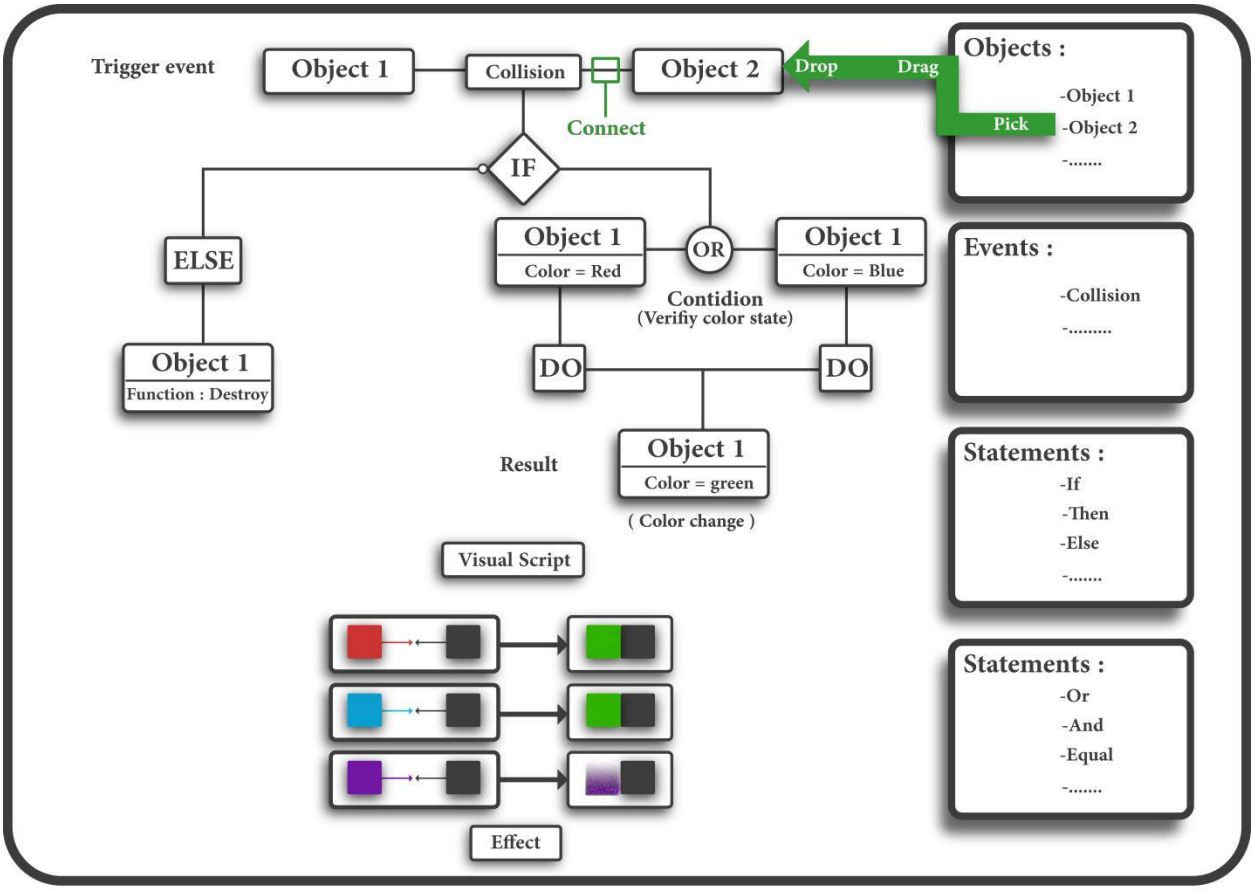
6. Districts Visual Studio

DVS permite tuturor sa creeze orice program fara a folosi cod; el prezinta o gama larga de functii, texturi, sunete sau modele 3D, avand o interfata intuitiva, care simplifica elaborarea Aplicatiilor. Utilizatorii vor avea parte de un mod VR care le va oferi abilitatea de a-si construi Dapp-urile, avand la dispozitie template-uri personalizabile.

Tutorialele care predau fiecare aspect al dezvoltarilor DVS pot fi gasite in zona de pornire a Districts sub forma de roboti interactivi, precum si clipuri video sau o sectiune dedicata forumului in care va avea loc un ajutor reciproc comunitar.

Alegeti (drag-drop) si conectati-va prin metoda de plasare a elementelor (modele 3d, butoane, iluminare ...), alocarea texturii, alocarea animatiei sau chiar scriptingul vizual, deoarece majoritatea creatiei va fi realizata de controlerele mouse-ului sau de VR. Modelarea terenurilor are un instrument specific care permite crearea de peisaje variate (zgomot de teren, relief, rampe, eroziune). Meniul proprietatilor poate fi deschis cu un clic. Interactiunile si declansatoarele sunt stabilite in harta interactiunilor, unde procesele sunt create ca arbori de conditii si rezultate, utilizatorul isi traseaza hartile si DVS il transforma intr-o aplicatie.

Exemplu vizual al hartii codului: Schimbarea culorii in cazul unei coliziuni

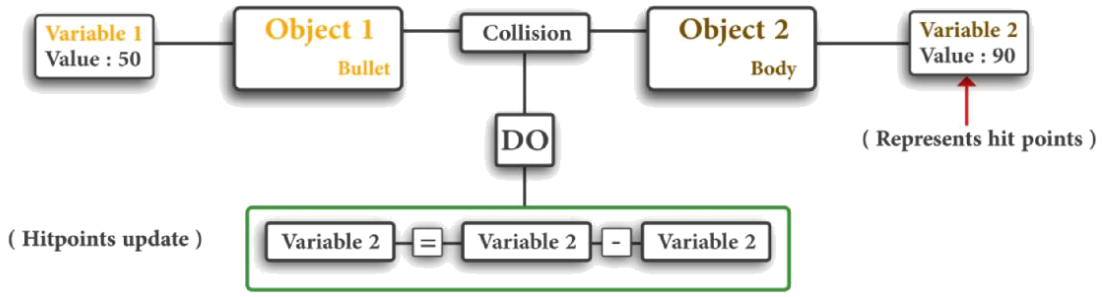


Reducerea deteriorarii armurii

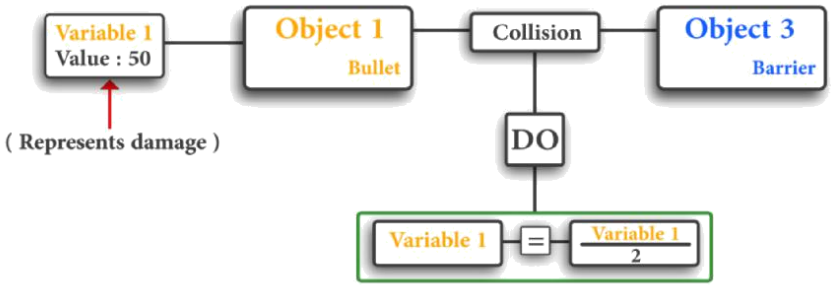
Functia de reducere a "punctelor de viata- HP":

Cand **glontul** atinge **corpul**; o noua valoare este atribuita punctelor de lovituri, scazand valoarea **Damage** (deteriorarii) din valoarea punctelor de viata (**HP)** .

HP reduction function

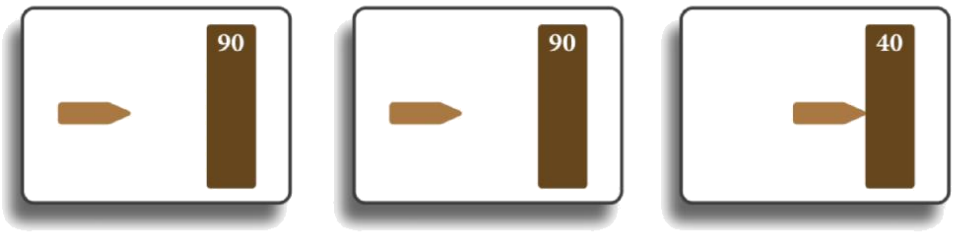


Bullet damage reduction function

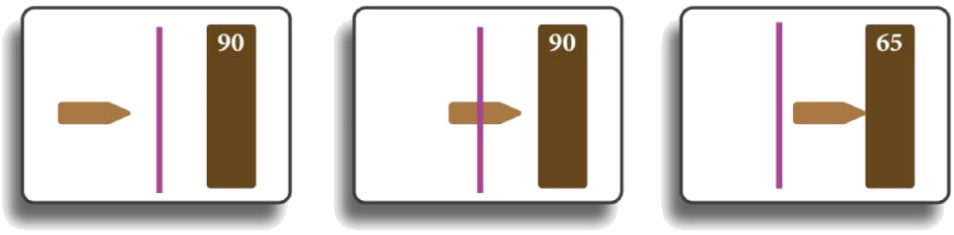


Visual Script

HP redcution only



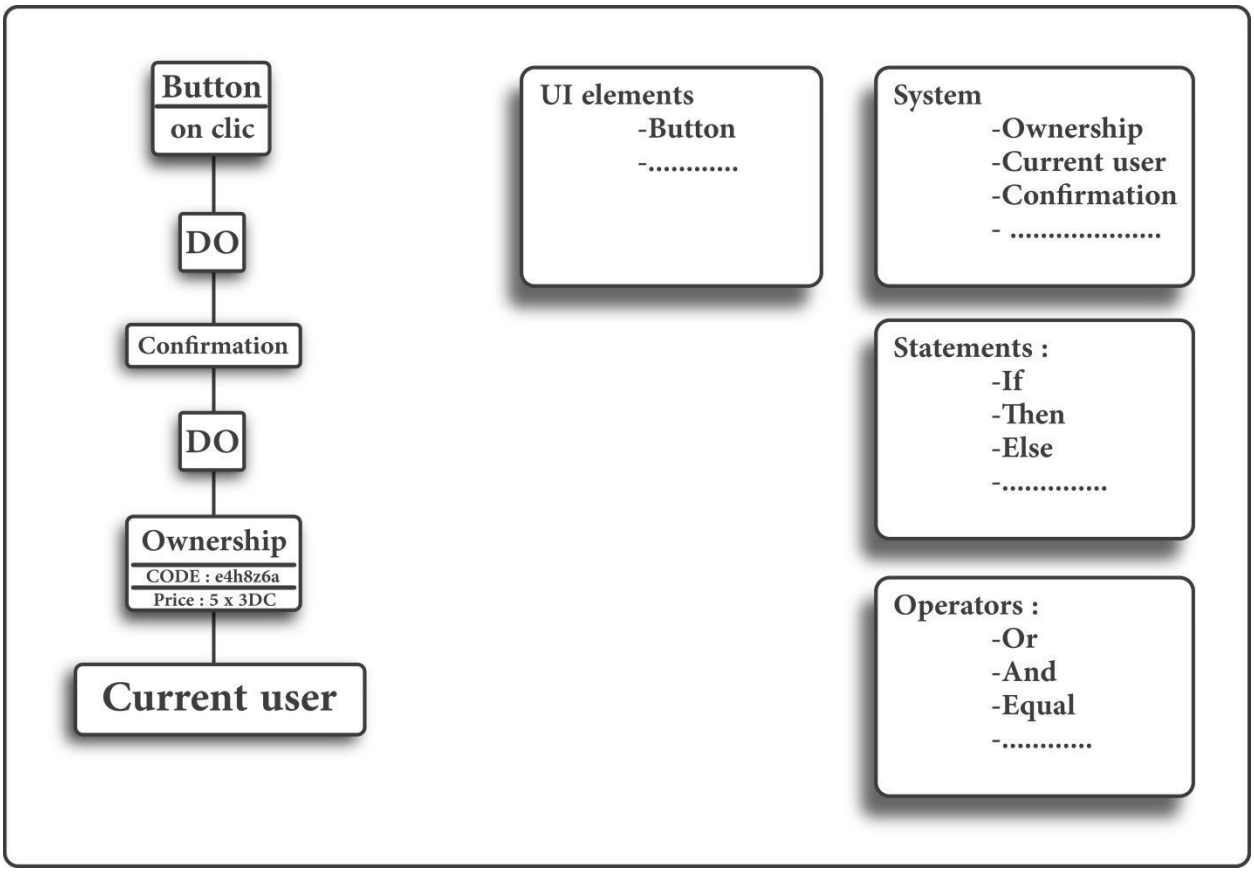
Bullet damage reduction, followed by HP reduction



Effect

Funtia de plata

Cand vorbim despre Dapps, dreptul de proprietate al obiectelor vandute, sau accesul la servicii este definit de o tranzactie codificata, de exemplu, cand este achizitionat dreptul de utilizare al unui serviciu sau produs, functia “Proprietate” creaza o tranzactie de plata care contine un cod spefici, aplicatia verifica prezenta acestei tranzactii in retea, de fiecare data cand o foloseste cineva. Crearea unei vanzari in mediul aplicatiei descentralizate este la fel de simpla ca orice alta functie:



Atunci cand se face clic pe butonul "Achizitie"- “Purchase”, se solicita o confirmare de la utilizator, cand face clic pe "Da", functia de proprietate creeaza si transmite automat o tranzactie de proprietate.

Inainte de lansare, utilizatorul poate testa Dapp-ul sau intr-un mod offline; odata testat si verificat; un script codificat este generat de DVS si gazduit intr-o Capsula de date. Pe langă aceasta, daca sunt incluse modele noi sau texturi, acestea vor fi trimise ca aditii la biblioteca Districts.

Continutul ilegal sau necorespunaător poate fi raportat de orice utilizator si apoi va fi restrictionat, in urma unui vot. Doar oamenii care ruleaza super noduri pot vota, vor face cea mai rațională alegere din cauza investitiei lor directe in sistem si a succesului sau. O parte din recompensa miniera a blocului va fi distribuita intre super noduri ca o stimulare in participarea la reglementare.

Odata ce aplicatia descentralizata este finalizata, o parcela de pamant trebuie sa fie achizitionata pentru a primi cladirea corespunzatoare, prin **token-ul de teren.**

7. Token-uri referitoare la teren

Acestea definesc proprietatea asupra unui teritoriu care va fi creat pentru a se construi cu ajutorul sau cladiri sau structuri. Parcelele sunt legate de aplicatiile descentralizate pe care le gazduiesc, ambele putand fi tranzactionate gratuit. Dreptul de proprietate asupra terenului va fi setat si salvat in aceeasi tranzactie ca Dapp-ul.

Utilizatorul va trebui sa selecteze propria parcela ori in districtele pre-partitionate ori pre-clasificate, sau intr-un district personalizat unde poate alege liber dimensiunea si locatia.

Primele 25 de token-uri de teren, care reprezinta primul inel de platforme, va apartine investitorilor de bloc, care le pot folosi sau tranzactiona cum le convine. Fiecare alta parcela poate fi achizitionata cu token-uri, ori din sistem, in cazul in care token-urile vor fi adaugate premiului de bloc, ori de la alti utilizatori.

8. Concluzie

Proiectul **Districts** ofera un cadru complet in care cele mai inalte asteptari ale consumatorilor vor fi satisfacute de o oferta incomparabila, din punct de vedere al calitatii si cantitatii. Creativitatea va fi pusa in aplicare si ideile nu vor fi niciodata limitate in domeniul imaginatiei, sa se exprime si sa se bucure de creatiile altora, intr-o piata cu adevarat libera condusa de utilizatorii sai.

Referinte:

[1] https://keepingstock.net/explaining-blockchain-how-proof-of-work-enables-trustless-consensus-2abed27f0845

[2] https://www.cryptocompare.com/coins/guides/how-does-a-hashing-algorithm-work/ (midified)

[3]https://en.bitcoin.it/wiki/Script

[4]https://github.com/BlockchainTechLLC/3dcoin/blob/master/src/script/interpreter.cpp#L688

[5] https://en.bitcoin.it/wiki/Colored_Coins