CatalansCoin

La criptomoneda social, catalana i lliure

Juny 2019 - 1a versió

Equip de desenvolupament:[t.me] @CatalanscoinDevelopers
TL:::Adaptacions + ampliació + : [t.me] @Pistatxin

Taula de continguts

1. Resum

"Announcing the first release of Bitcoin, a new electronic cash system that uses a peer-to-peer network to prevent double-spending. It's completely decentralized with no server or central authority.

See bitcoin.org for screenshots.

Download link:
http://downloads.sourceforge.net/bitcoin/bitcoin-0.1.0.rar"

Així començava el 8 de Gener de 2009 el post[i] que, signat amb el pseudònim de Satoshi Nakamoto[ii] revolucionaria els nous paradigmes d'internet i solucionaria un dels problemes que començaven a definir-se ja en aquell moment: identitat digital i diners electrònics.

El Bitcoin[iii] i la tecnologia que utilitza anomenada Blockchain[iv] avui són un clar referent tant en transaccions econòmiques com en nous desenvolupaments aplicats a la industria de tots els àmbits per identificar recursos, productes i processos logístics.

Només com a pinzellada de la magnitud que 10 anys després de la seva creació significa Bitcoin cal esmentar que a Juny de 2019 la capitalització en USD és de 140 mil milions. I el volum del mercat de les criptomonedes supera els 200 bilions de dòlars[v].

Amb aquestes dades i molt en contra del que voldrien els grans lobby econòmics i financers de tot el mon que a diari intenten, fabricant noticies falses, les criptomonedes i la tecnologia que representen són una forma clara de nous paradigmes en tots els àmbits de la nostre societat i d'un nou model de governança.

Les criptomonedes com el Bitcoin han dotat a l'individu d'una gran llibertat financera entre d'altres, ja que són la forma més completa de diners d'avui dia, gràcies a les seves propietats en seguretat, rapidesa, fiabilitat, fungibilitat, transparència, llibertat i propietat.

Creiem que aquesta tecnologia propiciarà una revolució i volem aprofitar la llibertat que se'ns ofereix, així un grup de persones hem creat el CatalansCoin una criptomoneda que ha de dotar Catalunya i al poble català d'una eina per avançar i adaptar-se als nous temps.

2. Introducció

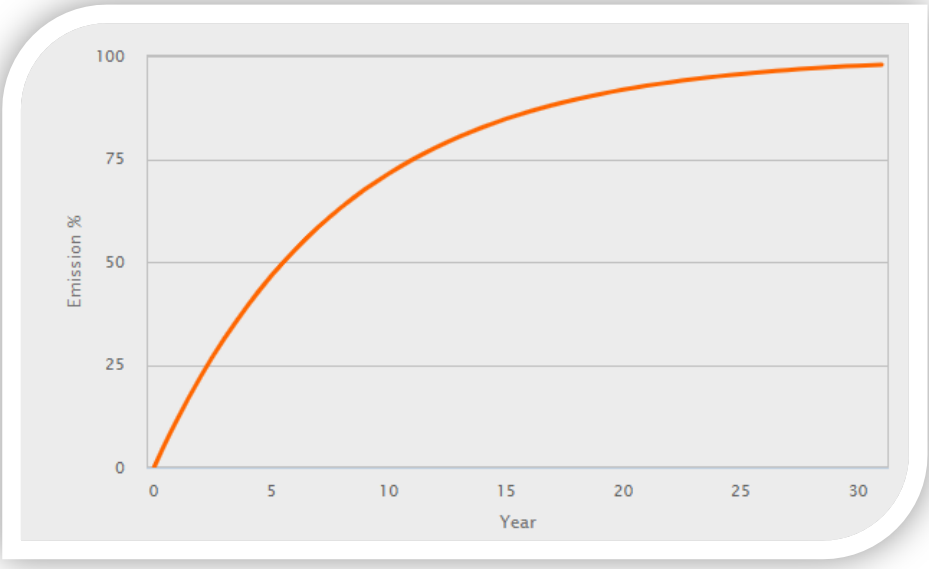
CatalansCoin és una moneda digital basada en TurtleCoin[vi]. Això vol dir que en la seva base és una moneda Cryptonote[vii], que inclou totes les característiques explicades en el whitepaper de Cryptonote, com ara:

- Fungibilitat. Totes les monedes són iguals i tenen el mateix valor gràcies a la dificultat de rastrejar d'aquestes.
- Algoritme de consens PoW[viii].
- Descentralització (una CPU, un vot).
- Emissió regular. Corba d'emissió decreixent constant sense halvings.

L'objectiu de CatalansCoin de crear la criptomoneda local més remarcable fins ara, centrada únicament per Catalunya i pels catalans, però amb llibertat de participació internacional. Per això hem definit les següents variables:

- Corba d'emissió lenta, similar a la del Bitcoin, de manera que la totalitat de les monedes trigarà més de 30 anys a ser emesa, donant temps a implementar les millores necessàries segons augmenta l'adopció.

- Un suplí total de 75 mil milions de monedes. Per calcular aquest número hem multiplicat la població total de Catalunya per 10000. Creiem que és un nombre raonable donada la gran quantitat d'usuaris que tenim com a objectiu, i la lenta corba d'emissió que ajudarà a anar guanyant adopció a poc a poc.
Continuant amb l'anterior punt, s'ha optat per una quantitat de dos decimals, respectant el sistema monetari més popular internacionalment dels cèntims.



3.Necessitats de Catalunya i objectius

3.1. Resistència a la censura de l'estat espanyol.

Els sistemes descentralitzats són coneguts per la seva resistència contra la censura. CatalansCoin es compromet a expandir les idees de la llibertat i construir una plataforma resistent que compleixi els següents objectius:

- Llibertat d'expressió. Possibilitat d'expressar-se i establir votacions de forma anònima i transparent sense ser oprimit per cap entitat.
- Memòria de Catalunya a Blockchain. Per augmentar la resistència contra la censura, la Blockchain de CatalansCoin podrà emmagatzemar textos de diferents tipus com ara:
- Tweets de personatges rellevants.
- Literatura catalana.
- Premsa catalana.

3.2. Llibertat monetària.

Les monedes centralitzades són controlades pels grans estats, inflades i depreciades deliberadament i usades per manipular a les comunitats subjacents sense possibilitat de resposta. Per evitar-ho CatalansCoin aconseguirà:

- Un repartiment de monedes just entre els catalans, que inclourà un canvi en l'algoritme de consens, mantenint la descentralització de la moneda.
- Acceptació de CatalansCoin en comerços, dotant a aquests amb les eines necessàries.
- Avenços en termes d'usabilitat, sense deixar de tenir una primera capa forta i descentralitzada.

3.3. Identitat, propietat i transparència.

Per dotar els catalans d'un sistema que verifiqui la seva identitat i protegeixi els seus drets i llibertats, es crearà una plataforma d'actius. Aquesta complirà objectius com ara:

- Sistema de verificació d'identitat. Gràcies al qual cada català podrà defensar, verificar i exercir els seus drets i llibertats com a català. Hi ha d'haver casos d'ús diversos com:
  - Llibertat d'expressió i de realitzar votacions.
  - Protecció i seguretat sense renunciar a la fungibilitat.
  - Permetre actualitzacions futures en l'algoritme de consens.
  - Gestió de beques, ajudes a famílies.

- Utilització a contractes intel·ligents.

4. Algoritme de consens

CatalansCoin com a moneda Cryptonote, i igual que Bitcoin, és una moneda en què el sistema de prevenció d'atacs i de repartiment de monedes està basat en una prova de treball. Per afegir un bloc a la cadena de blocs es necessita resoldre un problema de certa dificultat - en el qual s'inclou com a dada el hash de l'últim bloc - per força bruta. La cadena de blocs vàlida serà sempre la més llarga. A causa d'aquest cost econòmic d'introduir blocs, es crea un ecosistema en el qual si la majoria de miners són honestos, la cadena no podrà ser alterada.

No obstant això, aquest sistema té certes mancances que seran descrites a continuació.

4.1. Algoritme de prova de treball

L'algoritme de prova de treball de CatalansCoin és "Cryptonight-Catalans"[ix]. Una petita variació de Cryptonight V2 de monero, amb una modificació en la memòria necessària per crear un drap de Cryptonight. Gràcies a això, l'algoritme és molt més proper a la filosofia "one-CPU-one-vot" descrita en el whitepaper original de Bitcoin, podent-se realitzar sense grans desavantatges en qualsevol tipus de dispositiu que tingui una CPU.

Un altre punt positiu d'aquest algoritme és la resistència dels "circuits integrats d'aplicació específica" (ASICs), la qual cosa ajuda a tenir un repartiment de monedes i presa de decisions legítim per part dels usuaris. No obstant això, cal considerar que a causa del gran potencial de la moneda, així com la creixent versatilitat del maquinari en l'actualitat, tant ASICs com FPGAs seran desenvolupats per a aquest algoritme si no fem modificacions.

És per això que CryptoNight Catalans evolucionarà i s'actualitzarà per prevenir-ne mentre necessitem d'un algoritme de consens mixt per mantenir una Blockchain descentralitzada.

Hem trobat en aquest nou algoritme de treball la millor opció en l'actualitat per CatalansCoin. No obstant això segueixen existint diversos problemes com:

- Interès econòmic i polític de terceres parts en desprestigiar, revertir transaccions i censurar. (Atacs 51%).
- Manca d'interès i/o coneixements en l'usuari mitjà. Es crearan eines usables per conscienciar el usuari del significat i de la importància de "minar". Tanmateix és

evident que això no és suficient perquè l'usuari mitjà comenci a protegir la xarxa de CatalansCoin.
- Emissió de blocs irregular (pocs miners quan la dificultat està alta i molts quan està baixa).

4.2. Futur algoritme de consens

Després d'estudiar els diferents algoritmes de consens que hi ha a les blockchains de l'actualitat, hem arribat a la conclusió que el PoW (prova de treball) és el més estès, descentralitzat i segur. No obstant això, a causa de les mancances anteriorment esmentades, CatalansCoin implementarà canvis en l'algoritme de consens, conservant el PoW (a curt termini), però afegint més variables, com ara:

- Habilitat dels nodes de poder votar per la Blockchain correcta (protecció contra atacs 51%)
- Recompensar els nodes complets localitzats a Catalunya per contribuir a mantenir una xarxa segura sense necessitat de realitzar una prova de treball o mantenir una certa quantitat de monedes.
- Els nodes de Catalunya, al mateix temps, rebran una major recompensa en trobar una solució PoW sense afectar el suplí màxim.
- Per evitar l'explotació d'aquesta característica internacionalment, es reduirà la recompensa d'un node si troba molts blocs (pools)

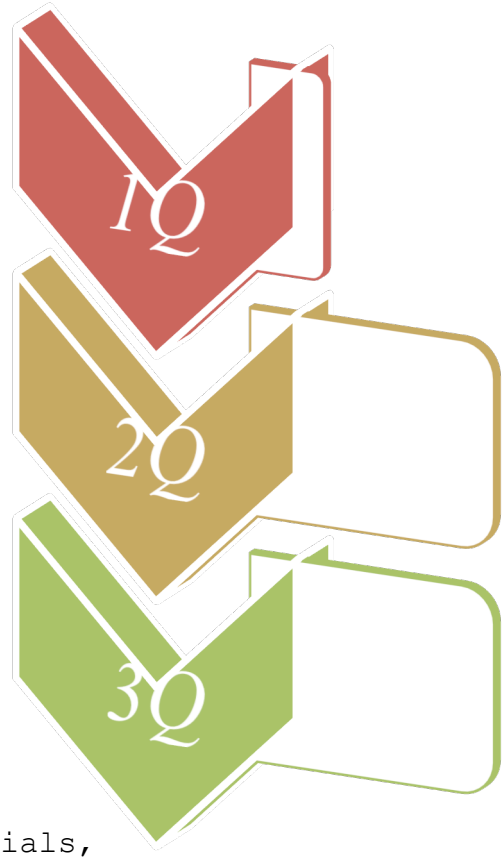
5. Roadmap

- Producció d'un nou lloc web, re disseny del roadmap i creació d'un whitepaper. (Q2 2019)

- Planificar bounties, incentivar la creació d'articles que parlin sobre CatalansCoin. (Q2 2019)

- Negociar el llistat en exchanges i DEX. (Q2 2019)

- Creació d'una organització externa no lucrativa i transparent, fundada per la comunitat (Q2 2019). Aquesta organització governada per la comunitat, tindrà objectius diversos, com ara:



    - Augmentar la freqüència de airdrops. Creació d'esdeveniments físics per donar a conèixer la moneda.

    - Incentivar el desenvolupament d'eines desitjades per la comunitat.

    - Donar suport al moviment independentista de Catalunya i defensar les llibertats dels catalans.

    - Incentivar la creació de nodes, treballar per crear una Blockchain segura i descentralitzada (Q2 2019)

    - Desenvolupar i planificar xarxes socials, esdeveniments físics, etc. Per conscienciar el món de la importància i necessitat històrica d'una Catalunya independent i sobre les aportacions llibertaris de la tecnologia de Blockchain. (Q3 2019)

    - Integració en dispositius xpos. Aconseguir comerços que acceptin CAT. (Q4 2019)

    - Integració en bitnovo o serveis semblants. (Q1 2020)

6. Enllaços

CLI wallet:
https://github.com/catalanscoin/catalanscoin/releases

GUI wallet:
https://github.com/catalanscoin/catalanscoinguiwallet/releases

Pool:
http://pool.catalanscoin.com/

Explorer:
http://explorer.catalanscoin.com/

Paper wallet:
http://catalanscoin.com/paper-wallet

CPU miner:
https://github.com/catalanscoin/catrig/releases

AMD miner:
https://github.com/catalanscoin/xmrigCC-amd/releases

7. Referencies i bibliografia

[i] https://www.metzdowd.com/pipermail/cryptography/2009-January/014994.html
[ii] https://ca.wikipedia.org/wiki/Satoshi_Nakamoto
[iii] https://ca.wikipedia.org/wiki/Bitcoin
[iv] https://ca.wikipedia.org/wiki/Blockchain
[v] https://www.blockchain.com/es/charts
[vi] https://docs.turtlecoin.lol/Getting-Started
[vii] https://cryptonote.org/whitepaper.pdf
[viii] https://ca.wikipedia.org/wiki/Prova_de_treball
[ix] https://github.com/catalanscoin/catalanscoin