



finestra

A black and white portrait of Bettina Warburg, a woman with long, wavy hair, looking directly at the camera with a slight smile.

Bettina Warburg

“Com la tecnologia de les cadenes de blocs
transformarà radicalment l'economia”

TED Summit celebrat a Banff el 28 de juny de 2016

Fotografia: blockchainworkshops.org

Bettina Warburg ha fet de la recerca entre política, economia i tecnologia la seva passió. Ho fa a través de la seva consultoria Animal Ventures, que assessora a governs, empreses, universitats i grups d'interès per desenvolupar *start-ups* en àmbits com la intel·ligència artificial, les cadenes de blocs o la indústria de l'internet de les coses. Les seves conferències apunten a un nou futur ple d'oportunitats i de reptes, però també d'interrogants, que com a societat caldrà fer-hi front.

Els economistes han estat estudiant el comportament humà durant centenars d'anys: com prenem decisions, com actuem de forma individual i en grup, com intercanviem valor... Han estudiat les institucions que faciliten el comerç com els sistemes legals, les corporacions o els mercats. Però hi ha una nova institució tecnològica que canviarà de dalt a baix la forma en què intercanviem valor: la tecnologia de les cadenes de blocs —o *blockchain* en anglès.

Bé, això és una afirmació molt contundent, però si us heu de quedar amb alguna cosa d'aquesta conferència, el que vull que recordeu és que, si bé la tecnologia de les cadenes de blocs és relativament nova, també és la continuació d'una història molt humana, i la història és la següent. Com a éssers humans, sempre busquem la manera de reduir les incerteses que tenim entre nosaltres per poder intercanviar valor.

Una de les primeres persones en explorar a fons la idea d'utilitzar institucions com a eina per reduir les nostres incerteses envers els altres en el camp de l'economia i ser capa-

ços de comerciar va ser el premi Nobel d'Economia Douglass North. Va morir a finals de 2015, però North va ser pioner en allò que anomenem la «nova economia institucional». I per «institucions» el que volia dir era senzillament regles formals, com ara una constitució, i restriccions informals, com ara els suborns. Aquestes institucions són en realitat l'oli que greixa els engranatges de l'economia i que permet que funcioni i ho hem pogut veure al llarg de la història de la humanitat.

Si ens remuntem a l'època en què érem economies de caçadors-recol·lectors, veurem que en realitat només comerciàvem dins de l'estructura del nostre propi poblat. Teníem algunes restriccions informals, però vam forçar el comerç mitjançant la violència o les repressions socials. A mesura que les nostres societats esdevenien més complexes i les rutes comercials cada cop arribaven més lluny, vam crear institucions més formals, com ara els bancs per la moneda, els governs, les corporacions... Aquestes institucions ens van ajudar a gestionar el comerç a mesura que creixia la incertesa i la complexitat i

Les cadenes de blocs redueixen la incertesa i, per tant, prometen transformar els nostres sistemes econòmics de forma radical

el nostre control personal disminuïa. Amb l'aparició d'Internet, vam posar aquestes institucions en línia. Vam crear plataformes de comerç com Amazon, eBay, Alibaba... institucions més ràpides que actuen com a intermediàries per facilitar l'activitat econòmica humana.

Tal com ho veia Douglass North, les institucions són una eina per reduir la incertesa de forma que puguem connectar i intercanviar tot tipus de valor en la societat, i crec que ara estem entrant en una nova evolució radical en la manera en què interactuem i comerciem, perquè per primer cop podem disminuir la incertesa no només amb institucions polítiques i econòmiques com bancs, corporacions i governs, sinó que ara també ho podem fer només amb tecnologia.

Així doncs, què és la tecnologia de les cadenes de blocs? Una cadena de blocs és una base de dades descentralitzada que emmagatzema un registre de béns i transaccions en una xarxa entre iguals (P2P). És bàsicament un registre públic de qui posseeix què i qui transacciona què. Aquestes operacions estan protegides

mitjançant criptografia i, al cap d'un temps, l'historial de transaccions queda tancat en blocs de dades que després són units entre si mitjançant xifrat i tot queda protegit criptogràficament. Això crea un registre immutable i infalsificable de tots els moviments que s'han efectuat en aquesta xarxa. Aquest registre es replica en tots i cadascun dels ordinadors que utilitzen la xarxa.

No és una app. No és una empresa. Crec que la descripció més aproximada seria dir que és alguna cosa com la Viquipèdia. A la Viquipèdia ho podem veure tot. És una obra col·lectiva que canvia i s'actualitza constantment. A la Viquipèdia també hi podem fer el seguiment dels canvis al llarg del temps, i podem crear les nostres pròpies «viquis», perquè, en el seu nucli, és tan sols una infraestructura de dades. Amb la Viquipèdia, doncs, tenim una plataforma oberta que emmagatzema paraules i imatges i els canvis en aquestes dades al llarg del temps. Una cadena de blocs, per la seva banda, la podem imaginar com una infraestructura oberta que emmagatzema molts tipus d'actius. Emmagatzema la història de la custòdia, la propietat

i la ubicació dels actius, com per exemple la moneda digital bitcoin i altres actius digitals com títols de propietat intel·lectual. També poden ser certificats, contractes, objectes del món real i, fins i tot, informació personal identificable. Evidentment en les cadenes de blocs hi intervenen molts altres factors tècnics, però bàsicament així és com funcionen. És el fet que siguin un registre públic que emmagatzema transaccions en una xarxa i que es repliquin en tota aquesta xarxa el que fa que siguin molt segures i difícils d'alterar.

Això ens porta al nostre tema de com les cadenes de blocs redueixen la incertesa i, per tant, com prometen transformar els nostres sistemes econòmics de forma radical. La incertesa és un aspecte molt important en l'economia; vull examinar tres formes d'incertesa a les quals ens enfrontem en gairebé totes les nostres transaccions diàries i en què les cadenes de blocs poden tenir un paper important. Ens enfrontem a incerteses com no saber amb qui estem tractant, no tenir visibilitat en una transacció, i no tenir a qui recórrer en cas que les coses vagin malament.

Les cadenes de blocs ens permeten crear una plataforma oberta i global on emmagatzemar qualsevol testimoni o prova sobre qualsevol persona provinent de qualsevol font

Vegem el primer exemple: no saber amb qui estem tractant. Posem per exemple que vull comprar un telèfon intel·ligent de segona mà a l'eBay. La primera cosa que faré serà intentar aconseguir informació sobre el venedor. És un usuari habitual? Té bons comentaris i bones puntuacions o no té ni tan sols perfil? Ressenyes, puntuacions, verificacions... Aquestes són les proves i els testimonis sobre les nostres identitats que recopilem com podem i que utilitzem per reduir la incertesa sobre les persones amb qui estem tractant. Però el problema és que estan molt fragmentades. Penseu en quants perfils teniu, vosaltres. Les cadenes de blocs ens permeten crear una plataforma oberta i global on emmagatzemar qualsevol testimoni o prova sobre qualsevol persona provinent de qualsevol font. Això ens permet crear una identitat portàtil controlada per l'usuari. Més que un perfil, significa que pots revelar de forma selectiva diferents atributs sobre tu que ajudin a facilitar el comerç o la interacció, com per exemple que un govern t'ha expedit un document d'identitat, o que ets major de 21 anys, revelant la prova criptogràfica que aquesta informa-

ció existeix i que està comprovada i «tancada». Disposar d'aquest tipus d'identitat portàtil tant en el món físic com en el món digital significa poder comerciar d'una manera totalment nova.

Bé, això era com les cadenes de blocs poden disminuir la incertesa sobre les persones amb qui estem tractant. La segona incertesa a la qual ens enfrontem sovint és que no hi hagi transparència en les nostres interaccions. Diguem que m'enviaran aquell telèfon intel·ligent per correu. M'agradaria que hi hagués una certa transparència; per exemple, voldria saber si el producte que he comprat és el mateix que el que m'arriba per correu, i si hi ha algun registre o constància de com ha arribat fins a mi. Això és aplicable no només als aparells electrònics, sinó també a molts altres tipus de béns i dades, com ara medicines, articles de luxe i qualsevol altre producte que no vulguem que sigui alterat.

El problema de moltes empreses, especialment les que fabriquen articles complexos com telèfons intel·ligents, és que es relacionen amb tots els seus proveïdors a través de

cadenes de subministrament horitzontals. Totes aquestes persones que intervenen en la fabricació d'un producte no tenen la mateixa base de dades. No utilitzen la mateixa infraestructura i per això resulta molt difícil veure com evoluciona un producte amb el temps de forma transparent.

Amb una cadena de blocs podem crear una realitat compartida amb moltes entitats en les quals potser no confiem. Amb això vull dir que tots aquests nodes de la xarxa no tindran per què conèixer-se o confiar els uns en els altres, perquè podran monitoritzar i validar la cadena per ells mateixos. Penseu de nou en la Viquipèdia. És una base de dades compartida, i malgrat tenir múltiples lectors i múltiples autors al mateix temps, només té una única veritat. Doncs bé, podem crear el mateix amb les cadenes de blocs. Podem crear una base de dades descentralitzada que tingui la mateixa eficiència que un monopoli però sense crear cap autoritat central. Així, tots aquests proveïdors i tot tipus d'empreses podrien interactuar utilitzant la mateixa base de dades sense haver de confiar necessàriament

Les nostres incerteses, més que frenar-nos ens impulsen; podem aprofitar tota incertesa col·lectiva i utilitzar-la per col·laborar i intercanviar més, més ràpid i de forma més oberta

els uns en els altres. La implicació per als consumidors és que podrà haver-hi molta més transparència. A mesura que un objecte del món real s'anés desplaçant, també podríem veure el seu certificat digital o la seva autenticació desplaçant-se a través de la cadena de blocs, afegint valor a mesura que avancés. Això representa tot un nou món pel que fa a la nostra visibilitat.

Bé, ja hem vist com les cadenes de blocs poden disminuir les nostres incerteses pel que fa a la identitat i com poden canviar el significat de «transparència» en el comerç complex i a llargues distàncies com en les cadenes de subministrament. L'última de les incerteses a les quals ens enfrontem sovint i que tenen un final més obert són els incompliments. Què passa si no m'envien telèfon intel·ligent? Podré recuperar els meus diners? Les cadenes de blocs ens permeten escriure codis — contractes vinculants entre persones — i garantir que es compleixin sense necessitat de cap tercera part que ho hagi de fer complir. Si tornem a l'exemple de telèfon intel·ligent, seria com un pagament en dipòsit: paguem el telèfon, però no desblo-

quegem els fons fins que no puguem verificar que s'han complert totes les condicions. Així, ens assegurem de rebre el telèfon.

Crec que això és una de les maneres més interessants i emocionants amb què les cadenes de blocs redueixen les nostres incerteses, perquè en certa mesura significa que podem fusionar institucions. Això vol dir que una bona part de l'activitat econòmica humana es pot automatitzar i quedar garantida amb fons, valors etcètera i podem concentrar la intervenció humana cap a les vores, és a dir, els llocs per on la informació passa del món real cap a les cadenes de blocs.

Crec que el que deixaria Douglass North més astorat sobre aquest ús de la tecnologia és que allò que fa que funcioni, allò que fa que les cadenes de blocs es mantinguin segures i verificades, és precisament la nostra desconfiança mútua. Així doncs, les nostres incerteses, més que frenar-nos i fer que necessitem institucions com bancs, governs o corporacions ens impulsen; podem aprofitar tota aquesta incertesa col·lectiva i utilitzar-la per col·laborar

i intercanviar més, més ràpid i de forma més oberta.

Bé, ara no vull que us endugueu la impressió que les cadenes de blocs són la solució a tot, per molt que els mitjans de comunicació hagin dit que acabaran amb la pobresa, els medicaments falsificats o que salvaran la selva amazònica. La veritat és que aquesta tecnologia encara és a les beceroles i encara haurem de veure molts experiments i probablement algun fracàs abans no puguem entendre realment tots els usos que pot tenir per a la nostra economia. Però hi ha moltíssima gent treballant-hi, des d'institucions financeres fins a empreses tecnològiques, passant per *start-ups* i universitats. I un dels motius és que no es tracta tan sols d'una evolució de l'economia, sinó que també és una innovació en el món de la ciència de la informàtica.

Les cadenes de blocs ens proporcionen la capacitat tècnica de crear un registre d'intercanvis entre persones, de canvis de moneda, de tot tipus de béns físics o digitals i, fins i tot, dels nostres atributs personals, d'una forma totalment nova. Així doncs,

Les cadenes de blocs ens proporcionen la capacitat tècnica de crear un registre d'intercanvis entre persones, de canvis de moneda, de tot tipus de béns físics o digitals i, fins i tot, dels nostres atributs personals, d'una forma totalment nova

en certa manera, es converteixen en una institució tecnològica que té molts dels avantatges de les institucions tradicionals que estem acostumats a utilitzar en la societat, però ho fan d'una forma descentralitzada. I ho fan convertint moltes de les nostres incerteses en certeses.

Així que crec que hem de començar a preparar-nos, perquè estem a punt de veure un món en què les institucions distribuïdes i autònomes tindran un paper molt important.

Moltes gràcies. ■