Co to jest krypto waluta? Pytanie coraz częściej zadawane w dzisiejszych czasach z powodu ich znaczenia na rynku. Zaczelo się to jako produkt poboczny w innej innowacji, jako produkt nie miał zostać walutą. Lecz w 2008 bitcoin został wypuszczony jako „Peer-to-Peer system platnosci electronicznej”. Nie potrzebowaly one serwera, ani centralnej administracji. Była to pierwsz udana proba od początku pomysłu, czyli od lat dziewiedziestiatych, przez cala dekade proby były podejmowane, lecz wszystkie skonczyly się niepowodzeniem. Dzieki pomysłowi Saotshi Nakamoto Bitcoin stal się dość popularna waluta. Lecz jeżeli zabierzemy caly marketing, jest to poporstu wartość w bazie danych, lecz jak popatrzymy na prawdziwa walute przetrzymywana w bankach jest to to samo.   
Jak to działa?

Tutaj nei ma ustalonej wartości, sama waluta nie ma swojego odpowiednika w przedmiotach materialnych, jest tam wiara w system, gdyż sa to tylko wartości w bazie danych, wielkim plusem takiego sposobu jest brak administracji oraz udziału państw. Jest przez to nie ograniczony prawami, nie ma tez kogos kto administruje danymi, każdy użytkownik posiada kopie wszystkich wartości każdego użytkownika. Dzieki temu poporstu ogłaszamy ze chcemy zrobić transfer z danego konta na inne konto podajac jego dane oraz wartrosc przeslanej waluty. Aby zapobiec podszywaniu się pod innych uzytkownikow, gdyż wszytkei numery sa publiczne, używane sa klucze które odpowiadają podpisa w checkach i wekslach. Pozwala ona innym użytkownika potwierdzić ze ta tranzakcja została wyslana przez wlasnie tego użytkownika. Sa one unikalne dla każdej transakcji wiec nie jest to system w którym latwo możemy podrobić czyjs podpis.

Wszystko opiera się na technologii zwanje blockchain, jest to rosnaca lista rekordow nazwanych blockami. Sa one polaczane prz pomocy cryptografi, oznacza ze każdy z nich zawiera cryptographic hash poprzedniego bloczka, znak czasu idate dranzakcji, najczęściej sa przedstawiane jako drzewo Merkle.  
Kryptograficzna funkcja hash, jest to specjalna klasa funkcji hash,, Jest to algorytm matematyczny który mapuje dane dowolnego rodzaju do bitowe string’u z ustalona dlugoscia zwanego hashehm. Jest stworzona by tworzyla funkcje jednostronna, jest to funkcja która latwo sconvertowa lecz niemozliwa to odwrócenia.

Jak to się odnosi do naszego tematu? W krypto walutach potwierdzenie jest czyms co pozwala na temu systemowi dzialac. Dopuki tranzakcja jest oczekujaca nie oznacza ona nic dla systemu, może ona zostać dowolnie zmieniona, lecz jeżeli zostanie potwierdzoan wszyscy w systemie będą wiedzieć ze została zrealizowana, oznacza to ze każdy użytkownik będzie widział zmiane jaka wprowadzila ona na nasze konto jak i na konto drugiej strony transakcji.   
Jeżeli nie mamy serwera, ani administracji jak możemy potwierdzać nasze tranzakcje? Czy każdy będzie musial uzwiezyc nam na slowo? Problem ten jest rozwiązany przez kopaczy którzy w naszym systemie. Dekoduja oni tranzakcje tak, aby zweryfikować ich uczciwość. Po potwiedzeniu tranzakcja kazda czesc wezlu musi dodac ja do swojej bazy danych. Wtedy dopiero staje się ona czescia łańcucha blokowego.

Po wykonainu tej pracy kopacze dostają zaplate w formie tokenu odpowiedniej kryptowaluty na której rzecz pracują, np. bitcoin, electrum.

Kopaczem kryptowaluty może być każdy. Przez brak centralnej jednostki zarzadzajace nie ma srodkow ani osob które moglyby to zlecac. Aby nie spowodować katastrofy która by powstala przez podrabianie kluczy przy pomocy tysięcy urzadzen, tworca zadecydowal ze kazda tranzakcja laczy się z opciazeniami na naszym komputerze. W jaki sposób to osiagnal? Postawil zasade która musi być spelniona aby tranzakcja mogla zostać zrealizowana. Żeby to osiagnac musza oni wygenerowac hash dzięki któremu można polaczcy nowy block z poprzednimi w lancuchu. Nazwal to Proof-of-Work. W przypadku bitcoin’a najpopularniejszej kryptowaluty jest to algorytm nazwany SHA 256 Hash.   
Polega to na kodowaniu tekstu tak aby nikt bez sekretnego kodu nie mogl go odczytac. Po znalezieniu rozwiązania kopacz może stworzyć blok i dodac go do lancucha blkowego. Jako nagroda za wykonanie tej pracy dostaje on na swoje konto prederminowana liczbe kryptowaluty. Jest to jedyny sposób na utworzenie ważnego Bitcoina. Trudnosc tych kodow jest zwiekszana z iloscia komputerow w całej sieci kopaczy, zapobiega to tworzeniu nieskończonej ilości waluty. Dzieki takim działania zapobiegawczym w danym momencie można wytworzyć tylko okreslona liczbe kryptowaluty. Jest to zasada która nei może zostać zlamana przez nikogo.

Dlaczego ludzie inwestują w krypto waluty?

Jest to najlepszy przykład ze ludzie nie potrzebują państwa aby mieć walute. Sa one zbudowane na cryptografi przez co nie musimy ufac zadnej partii rzadzacej lub innym osoba, lecz matematyce. Zawieraja tez wiele potrzebnych i ważnych elementow waluty.   
Piewrwszym sa właściwości tranzakcyjne gdzie wyroznaimy cztery najważniejsze.  
Nieodwracalnosc, po potwierdzeniu nie da się cofnac transakcji jak to jest możliwe w przypadku banku lub innych instytucjach. Jeżeli stracimy je w jakiś stopniu nie możemy ich cofnac, jest to problematyczne jeżeli zostanie nam wykradzione dane logowania. Wiec niestety to rozwiązanie posiada plus jak i minusy.

Anonimowosc, ani tranzakcja, ani konto nie jest powiazane do czegos co ma odpowiednik w naszym siwecie, nie jest podpisane do sooby tak jak to bywa w bankach, a wartości na nim nie odpowiadaj niczym fizycznym jak np rezerwa zlota. Zazwyczaj możemy przeanalizować ze tranzakcja się odbyla nie zawsze mozmey przypisac to do ludzi którzy dokonali tych transakcji. Jest to przydatne dla ludzi którym panastwo zakazuje kupowania lub sprzedaży niektórych produktów. Lecz tak jak w poprzednim przykładzie jest to miecz obusieczny gdyż może zostać wykozystany np. rpzez terroystow do zakupow broni.

Szybkosc i ogolnosiwatowsc, tranzakcje sa prawie natychmiastowo rozporwadzane bo sieci, ich potwierdzenei zajmuje więcej czasu ale tez nei jest to zazwyczaj czas dłuższy niż czas potwieredznia przelewu bankowego. Nie zaleza tez one od przynaznosci do kraju lub miejsca zamieszkania, sa tak samo szybko rozpatrzywane bez względu na lokacje.

Bezpieczenstwo  
  
  
<https://blockgeeks.com/guides/what-is-cryptocurrency/#What_Are_Miners_Doing>  
<https://cryptocurrencyfacts.com/how-does-cryptocurrency-work-2/>