

Wojciech Nowakowski, prof

## Dziś internet można mieć tylko dla siebie

Rewolucja „prywatny pieniądz w internecie” zaczęła się 31 października 2008 roku, kiedy to do dziś nieznanemu nikomu Satoshi Nakamoto opublikował na jednym z serwisów artykuł pt. *Bitcoin: A Peer-to-Peer Electronic Cash System*. Nie doczekał się wtedy znaczącej reakcji środowiska, więc po pół roku wpisał się na portal internetowych entuzjastów bezpośrednich kontaktów w sieci P2P (ang. peer-to-peer, każdy z każdym):

### Bitcoin open source implementation of P2P currency

Posted by Satoshi Nakamoto on February 11, 2009 at 22:27

I've developed a new open source P2P e-cash system called Bitcoin. It's completely decentralized, with no central server or trusted parties, because everything is based on crypto proof instead of trust. Give it a try, or take a look at the screenshots and design...

W istocie był to pierwszy dostrzegalny sygnał o powstaniu zdecentralizowanej wirtualnej waluty kryptograficznej nazwanej wtedy i do dziś nazywanej bitcoin. W tej pierwszej publikacji Nakamoto przedstawił koncepcję emisji wirtualnego pieniądza, zabezpieczenia tej emisji, kryptograficznego rejestrowania transakcji oraz kontroli wiarygodności obrotu. Do matematycznej koncepcji tego pieniądza wykorzystano istniejące i opisane już wcześniej narzędzia kryptograficzne, z których najważniejszym był tzw. *łańcuch bloków* (blockchain), czyli zaszyfrowany zapis transakcji tworzący *de facto* odporną na fałszerstwa księgę handlową. Nakamoto wykorzystał także inne znane już wcześniej procedury kryptograficzne, na przykład *dowód pracy* (Proof of Work), narzędzia kontroli emisji, czy też *funkcję skrótu* (hash). Wszystko po to, by uniemożliwić oszustwa, zarówno emisyjne jak i księgowo, i zabezpieczyć zdefiniowaną walutę przed dewaluacją i zhakowaniem.

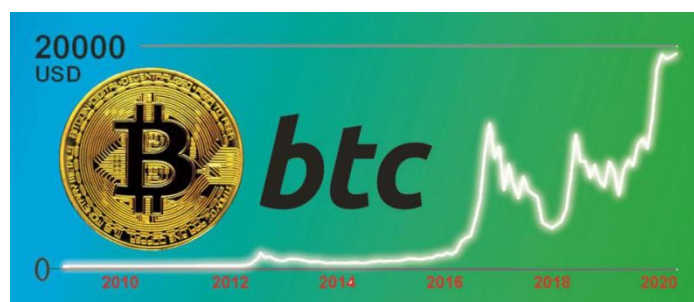
Wirtualne waluty były już w internecie definiowane wcześniej, na przykład w postaci żetonów do gier, lecz nigdy nie miały wartości publicznej i nie były też systemowo zabezpieczone przed kradzieżą. Nie było to po prostu potrzebne.

Pojawienie się tak dobrze zabezpieczonego pieniądza, zapewniającego do dziś wiarygodność transakcji było i jest zdumiewające. W końcu była to bezpieczna aplikacja internetowa, wprowadzona jako protest wobec dominacji rządowych walut państwowych. Co więcej, podmioty obracające tą nową walutą z założenia miały być równorzędne i niejawnie, identyfikowane jedynie pseudonimem, a wszystkie operacje natychmiast były publiczne.

Co ciekawe, fakt zdefiniowania takiej nowego finansowego bytu nie stał się wydarzeniem. Potraktowano go jako drobiazg bez znaczenia. A przecież powstała pierwsza suwerenna waluta świata. Waluta, która po pewnym czasie stała się powszechnym, międzynarodowym środkiem płatniczym internetu.

Bitcoin wystartował od założonego kursu o wartości wymiennej 1 USD. Dopiero jednak po roku 2015, gdy kryzysy gospodarcze i giełdowe stały się częste i bardziej dotkliwe, dostrzeżono go jako walutę ratunkową. A ponieważ nie było regulatora, wtedy już kurs tego pieniądza szalał, a wykres wartości był prawie jak przekrój szczytowych partii Himalajów. Średnia wieloletnia tego kursu natomiast stale rosła.

Od 1 \$ w 2010 roku, do 20000 \$ teraz. Dziś złotówkowy kurs bicoina stabilizuje się na poziomie 75 tys. PLN, a cały wolumen tej waluty wynosi 1,4 bln PLN. Bitcoin y warte są więc 6 krotnie więcej niż wszystkie polskie złotówki w obiegu.



Dla informatyka najbardziej zdumiewające jest to, że kod programu definiującego walutę bitcoin jest otwarty i dostępny w sieci każdemu. Ale czymś zupełnie innym jest tę walutę mieć, niż mieć kod definiujący tej waluty. Wykorzystując to znane oprogramowanie, każdy może taką nową swoją wirtualną walutę kreować. I tak robią. Dziś tych nowo zdefiniowanych walut jest już prawie dwa tysiące. Zdefiniowanie wirtualnej waluty w sieci bowiem nie kosztuje nic. Dopiero gdy znajdują się chętni by kupić za prawdziwe fiducyjne pieniądze jednostki nowej pieniędzy, to kryptowaluta ta zagości na rynku. Ci, którzy kupują jednostki tych nowo powołanych do życia kryptowalut liczą oczywiście na wzrost wartości zakupionych jednostek. Jest to więc mechanizm trywialny, podobny do gry giełdowej.

### Ethereum

Koncepcja Bitcoina, tej pierwszej kryptowaluty świata znalazła wielu entuzjastów, ale też i pojawili się wizjonerzy, którzy dostrzegli znacznie większy potencjał merytoryczny pomysłu. Jednym z nich był Vitalik Buterin, entuzjasta informatyki od dziecka, a potem twórca waluty i technologii Ethereum.



Witalij Buterik. Klatka z filmu *Vitalik Buterin On Creating One Of The World's Largest Cryptocurrencies*. Źródło: [youtube.com/watch?v=fi0ORZR4A88](https://youtube.com/watch?v=fi0ORZR4A88)

Urodził się w 1994 roku w Kołomnie, 140-tysięcznym mieście nad Oką, w pobliżu Moskwy. Gdy miał 5 lat jego rodzice, informatycy, postanowili wyemigrować za pracę

do Kanady. Tu Vitalik skończył szkoły, a nawet zaczął studiować informatykę. Studia te jednak szybko porzucił, by zajmować się tylko informatyką.

Gdy Buterin po raz pierwszy zetknął się w 2011 roku z bitcoinem, zignorował go. Mówił potem – *myślałem, że koncepcja bitcoina nie ma żadnej wartości, więc spisałem to na straty*. Potem jednak śledził ten projekt, a nawet zarabiał na nim pisząc artykuły do *Bitcoin Weekly*. Za każdy publikowany tekst płacono mu 5 bitcoinów, wartych wtedy niecałe 4 USD. *To była moja pierwsza prawdziwa praca. Dostawałem za nią prawie półtora dolara za godzinę!* – mówił potem w wywiadach. Dostrzegł jednak, że wykorzystanie technologii Bitcoin tylko jako pieniądza jest niesłuszne, bo technologia ta ma wielki potencjał w wielu dziedzinach gospodarki, również poza finansami.

Z pomocą dwóch kolegów zaczął więc urzeczywistniać swój pomysł. Napisali już nie jedna tylko aplikację, ale całe kryptograficzne środowisko informatyczne o nazwie *Ethereum*, które miało umożliwić każdemu tworzenie aplikacji w różnych dziedzinach, a następnie udostępniać je innym za wynagrodzeniem. Powołano przy tym środek płatniczy, kryptowalutę o nazwie *ether*.

W taki sposób narzędzia i procedury, po raz pierwszy użyte do zdefiniowania waluty bitcoin zostały potem użyte do wielu, bardzo wielu różnych dziedzin. Platforma Ethereum umożliwia teraz nie tylko formalne uporządkowanie i decentralizację wielu dziedzin finansów, w tym umów zawieranych w protokołach komputerowych (tzw. *smart contracts*), umów *crowdfundingowych* i w ogóle operacji inwestycyjnych, ale też zupełnie innych rodzajów działalności. Na przykład głosowania i wyborów, zarządzania firmą, czy zawierania umów, w tym również aktów notarialnych obrotu nieruchomościami. Tym samym powstało sieciowe środowisko internetowe, dostępne on-line, z tysiącami aplikacji w technologii łańcucha bloków. Poszerzyło to obszar zastosowań tej technologii na światy poza finansowe.

Okazało się bowiem, że każdy, nawet średnio zaawansowany w programowaniu użytkownik sieci może w środowisku Ethereum tworzyć atrakcyjne aplikacje znakowane kodem wpisanym do łańcucha bloków. Aplikacje proste lub bardziej wyrafinowane, a nawet zaawansowane i rozbudowane. Aplikacje te dostępne wszystkim w sieci za opłatą w kryptowalucie. Można nawet nimi handlować – kupować lub odsprzedawać innemu użytkownikowi. Nie może natomiast ich uruchomić, ukraść, zniszczyć, ani skopiować nikt poza właścicielem.

Innymi słowy w Ethereum, a potem także na innych, powstałych później platformach, powstał duży i dobrze funkcjonujący, głównie na smartfonach, mobilny, chmurowy świat usług i programów użytkowych z kontrolowaną własnością i dostępem. Można powiedzieć, że **wszystko mamy już w dłoni!**

Dopiero teraz, po latach wątpliwej już od dawna wolności w internecie twórczość i własność jest skutecznie zabezpieczona i nie wymaga pracy specjalistów i ponoszenia dużych kosztów. Stało się tak dzięki kryptograficznej przestrzeni łańcuchów bloków. I to bez ponoszenia dużych kosztów związanych z zachowaniem bezpieczeństwa, poufności, co w „zwykłej” rzeczywistości, na przykład usługach bankowych, medycznych czy wojsku jest standardem. Tam też korzystają z kryptografii, ale z kosztownych, specjalnych procedur i specjalnych urządzeń.

### **DeFi i DApps, czyli cyfrowy bazar**

Tak właśnie, wdzięcznie, zostały nazwane kryptoświaty programów, aplikacji i

procedur powstałych w opisanym technologii łańcucha bloków. To setki tysięcy już najrozmaitszych programów użytkowych. Świat finansów, kolekcjonerstwa, mody, muzyki, filmów, cyfrowych dzieł sztuki i gier komputerowych. Cały ten cyfrowy контент jest legalny i licencjonowany i zarejestrowany w sensie własności. W zwykłym internecie jest to nieosiągalne. Tu można kupować sobie oprogramowanie, obrazy, filmy czy utwory muzyczne, które stają się tylko moje i nikt nie ma do nich praw. Tu można też kupić sobie wirtualne zwierzątko, tylko moje, jedyne na świecie. To wszystko można też sprzedawać.

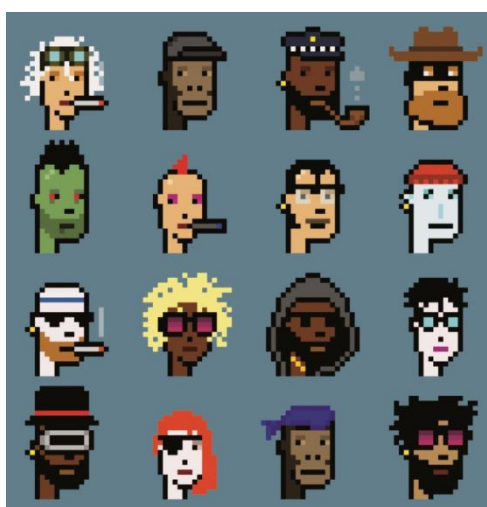
Aplikacje zdecentralizowane mają sens jedynie na platformach kryptowalutowych, bo tu dostępny jest jawny i prosty system obrotu i płatności. W kryptowalutach oczywiście, ale te przecież mogą być natychmiast wymieniane na prawdziwe pieniądze w każdej walucie świata, bo aplikacjami sieci są również kantory.

**DeFi** czyli *Decentralized Finance* to aplikacje, które oferują kredyty, pożyczki i prywatne płatności nie wymagając rejestracji danych osobowych i sprawdzania tożsamości. Są tu również aplikacje spekulacyjne do zabawy tzw. *instrumentami pochodnymi*. Można też tu ubezpieczać się od ryzyka i zarabiać na odsetkach, grać na loteriach i zdobywać finansowanie społecznościowe (crowdfunding). Wszystko to bez peselu, nazwiska, pośredników i kontroli wiarygodności finansowej!

**DApps** natomiast, czyli *Decentralized Applications* to tysiące aplikacji o szerokim spektrum zastosowań. Wiele tych aplikacji oferuje wyszukiwanie i wymianę różnych kryptoaktywów. Są też takie, z zupełnie innych światów: sport, rynek cyfrowych dzieł sztuki współczesnej (tu ceny nierzadko osiągają dziesiątki tysięcy USD, muzyka, towary i przedmioty kolekcjonerskie.

Przykładem ciekawej i popularnej aplikacji kolekcjonerskiej jest na przykład *Cryptopunk*. Tu handluje się małymi 32x32 pikselowymi ikonkami twarzy punków stworzonymi cyfrowo przez dwóch grafików. Jest ich dokładnie 10000 i nie ma dwóch takich samych. Zapisane są w łańcuchu bloków.

Na początku, po stworzeniu tych cyfrowych minio obrazków ich twórcy rozdali je za darmo chętnym. Teraz można je kupować, licytować i oferować na rynku wtórnym, również w łańcuchu bloków.



Cryptopunks. To coś takiego, jak kolekcjonowanie jedynych okazów czegokolwiek

Projekt ten zrobił światową karierę. Zainspirował nawet współczesny ruch CryptoArt. O Cryptopunks pisano między innymi w Financial Times, Paris Review, Christie's of London, New York Times. i wielu innych. Na przełomie 2018 i 2019, przez 6 miesięcy prezentowano te ikonki w Karlsruhe, w ZKM Center for Art and Media w ramach wystawy Open Codes Exhibition.

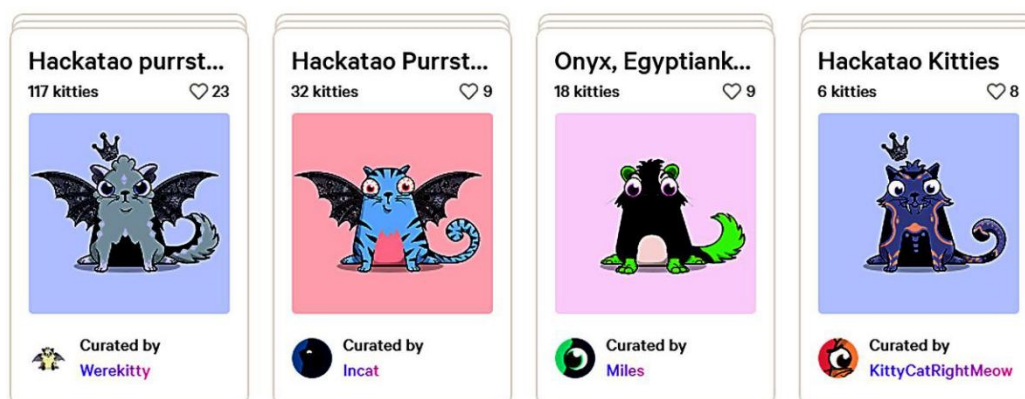
### CryptoKitties

Bardzo liczną grupą zdecentralizowanych aplikacji stanowią gry zakodowane i działające w łańcuchu bloków. Są zindywidualizowane i płatne. Każdy właściciel może przebieg gry kształtować jak chce. Już jedna z pierwszych na platformie Ethereum gra *CryptoKitties* (kryptokotki) firmy Axiom Zen stała się sensacją 2017 roku. Gra ta, oferuje po prostu zakupienie do osobistego udomowienia wirtualnego kota i jego hodowanie, nawet z rozwijaniem jego rodu. Do wyboru jest wirtualnych stworzeń, różnych kotów po prostu, nawiasem mówiąc graficznie ubogich.



## Start Your Digital Cat Collection

In CryptoKitties you can breed and adopt Kitties of all colours and shapes. Create Collections of your favourite cats and share them with our breeding community.



Jeden z ekranów gry Cryptokitties. Wybieramy sobie kotka, bu go pokochać.

Źródło: cryptokitties.co

Każdy kot jest inny. Niekopiowalny i niepodrabialny. Po zakupie kot stanowi własność inwestora, a jego wartość na rynku może rosnąć lub maleć. Wirtualne koty są zdolne do rozmnażania się. Potomstwo uzyskuje unikalny numer oraz nowy 256-bitowy odrębny genom z DNA. Koty-rodzice mogą przekazywać potomstwu do 12 cech, w tym kształt mordki, futro, kształt i kolor oczu, barwy podstawowe i akcentów, ale też charakter, np. dzikość. Wszystkie te zwierzęta są różne, zarówno wizualnie jak i charakterologicznie, także pod względem zachowania.

Teraz każdy może mieć kota! Dawniej też tak było, ale w realu, co teraz uważa się za przeżytek. Robią co chcą i wymykają się z domu, nie wiadomo gdzie i po co.

Teraz jest naprawdę *cool*. Gracze, a właściwie hodowcy wirtualnych kotów, to osoby obu płci pracujące głównie w korporacjach. Oni lubią koty, właśnie wirtualne, bo są czyste i nie trzeba po nich sprzątać.

.....

Nasuwa się pytanie: co dzieje się z naszym światem? Czy może po zapewnieniu sobie podstawowych potrzeb – fizycznego i intelektualnego bytu życie staje się zbyt puste, więc ratujemy się jak kto może? A może widząc to sama Natura daje nam popalić koronawirusem?