

# Architektura Kryptowalut

## Studium Bitcoina i Ethereum

Wojciech Korzeniowski  
Instytut Informatyki  
Wydział Elektroniki i Technik Informacyjnych  
Politechnika Warszawska

**Abstract—Opis koncepcji i mechanizmów wykorzystanych przy tworzeniu kryptowalut.**

### I. WSTĘP

Niniejszy artykuł przedstawia jakie problemy z pieniędzmi istnieją w dzisiejszym świecie i w jaki sposób pojawienie się kryptowalut może pomóc je rozwiązać. Następnie skupimy się na matematycznych conceptach które zostały wykorzystane przy projektowaniu kryptowalut oraz samą architekturę kryptowalut. Opisane zostanie czym jest Blockchain, co oznacza kopanie bloków a także to w jaki sposób zapewniane jest bezpieczeństwo oraz czym jest fork w kontekście Blockchainu. Pod koniec opiszę co nowego wprowadza Ethereum w stosunku do Bitcoina.

#### A. Historia waluty

Od zarania dziejów na świecie istniał handel. Zanim jednak powstały waluty, ludzie wymieniali się między sobą różnymi dobrami w sposób bezpośredni. Jeden z problemów który występuje podczas takiej wymiany jest problem z wydaniem reszty. Przykładowo, jeżeli ktoś kto hodował świnię i potrzebował kostkę masła, musiał wymienić całą świnię na dużą ilość masła. Ewentualnie mógł podzielić świnię i zostać z resztą świni co mogło powodować problem z jej przechowaniem. Rozwiązaniem tego problemu okazały się waluty. Hodowca mógł sprzedać swoją świnię w zamian za określoną ilość danej waluty a następnie część przeznaczyć na zakup masła. Inny problem który istnieje w świecie bez walut to problem z oszacowaniem wartości jednych dóbr w stosunku do innych. Zdecydowanie łatwiej jest sprowadzić wartość dóbr do wspólnej waluty co pozwala na łatwiejsze określenie w jakim stosunku powinna zostać dokonana wymiana jednego dobra z innym.

#### B. Rola banków

Jeżeli posiadamy pieniądze, ale nie chcemy być odpowiedzialni za ich przechowywanie możemy skorzystać z usług Banku. Podstawową operacją jaką możemy wykonać w Banku jest możliwość zdeponowania oraz pobrania wcześniej zdeponowanych środków. Kolejną z operacji jest wykonanie transferu środków z jednego konta na inne konto. Taka operacja umożliwia transfer środków innej osobie bez konieczności bezpośredniego przekazania pieniędzy w postaci monet czy banknotów. W takiej sytuacji Bank poświadcza że

właściciel konta przekazał swoje środki innej osobie dzięki czemu ta może je dalej przekazać. Taka rola sprawia że Banki są jedną z instytucji zaufania publicznego. Znaczący to między innymi to że społeczeństwo wierzy iż w każdej chwili może odebrać powierzone Bankowi pieniądze co nie jak pokazuje historia nie zawsze jest prawdą. Przykładem posłuży sytuacja Grecji z 2015 roku gdzie w wyniku kryzysu finansowego greckie Banki zostały zamknięte a wypłaty z bankomatów ograniczone do 60 euro na dzień.[1]

Fakt iż Bank jest odpowiedzialny za weryfikację czy dana osoba posiada odpowiednią ilość środków do wykonania transferu wymusza prowadzenie rejestru. W rejestrze znajdują się informacje przypisane do danego konta, historia wszystkich transferów oraz wynikająca z nich liczba zgromadzonych na koncie środków. Na banku spoczywa odpowiedzialność aby zawartość rejestru nie wpadła w niepowołane ręce oraz to aby rejestr nie przepała co spowodowałoby utratę zgromadzonych przez klientów środków gdyż tylko on jest dokumentem poświadczającym stan konta.

1) Subsubsection Heading Here: Subsubsection text here.

### II. CONCLUSION

The conclusion goes here.

### ACKNOWLEDGMENT

The authors would like to thank...

### REFERENCES

- [1] PolskieRadio.pl. (2015) Grecja: bankomaty zaczęły ponownie działać. nie ma limitu wypłat dla zagranicznych turystów. [Online]. Available: <https://www.polskieradio.pl/42/273/Artykul/1468946>