



Science Article
Oleh Danchivskyi

Oleh Danchivskyi

Zastosowanie blockchain w zabezpieczeniu transakcji internetowych

Artykuł naukowy

Rzeszów, 2023

Spis treści

1.	Wstęp.....	3
1.1.	Definicja blockchain.....	3
1.2.	Znaczenie bezpieczeństwa w transakcjach internetowych.....	3
2.	Geneza i historia blockchain	4
2.1.	Powstanie i rozwój blockchain.....	4
2.2.	Kluczowe momenty i milestones.....	4
3.	Architektura blockchain i jej zastosowanie w zabezpieczeniu transakcji	4
3.1.	Jak działa blockchain.....	4
3.2.	Zasady działania blockchain w zabezpieczeniu transakcji.....	5
3.3.	Przykłady zastosowania blockchain w zabezpieczeniu transakcji	5
4.	Zalety i wady blockchain w zabezpieczeniu transakcji.....	5
4.1.	Bezpieczeństwo i niezawodność blockchain.....	5
4.2.	Wydajność i efektywność.....	5
4.3.	Ograniczenia i potencjalne ryzyka związane z blockchain	6
5.	Przyszłość blockchain w zabezpieczeniu transakcji.....	6
5.1.	Trendy i prognozy	6
5.2.	Potencjalne zastosowania blockchain w zabezpieczeniu transakcji.....	6
5.3.	Możliwe wyzwania i bariery w dalszym rozwoju.....	6
6.	Praktyczne zastosowanie blockchain w zabezpieczeniu transakcji internetowych.	7
6.1.	Transakcje online jako potencjalne zagrożenie.	7
6.2.	Blockchain jako sposób na zwiększenie bezpieczeństwa i niezawodności transakcji online.	7
6.3.	W jaki sposób można zastosować blockchain w zabezpieczeniu transakcji online.	7
6.4.	Przykłady zastosowań blockchain w zabezpieczeniu transakcji online, takie jak:.....	8
6.4.1.	Bezpieczne przesyłanie i przechowywanie informacji o transakcji.	8
6.4.2.	Zabezpieczenie przed kradzieżą danych i oszustwami.....	8
6.4.3.	Zabezpieczenie przed nieautoryzowanym dostępem do informacji o transakcji.	8
6.4.4.	Zabezpieczenie przed fałszywymi transakcjami o podszywaniem się.	8
6.4.5.	Weryfikacja i uwierzytelnianie tożsamości użytkownika przed dokonaniem transakcji.	9
6.5.	Praktyczne zastosowanie blockchain w zabezpieczeniu transakcji.....	9
7.	Zakończenie.....	10
7.1.	Podsumowanie kluczowych informacji.....	10
7.2.	Wnioski i rekomendacje.....	10
8.	Literatura	11

1. Wstęp

Blockchain jest coraz częściej wykorzystywanym narzędziem w branży finansowej, które pozwala na bezpieczne przeprowadzanie transakcji internetowych. W ostatnich latach zauważalny jest wzrost zainteresowania blockchainem jako sposobem na zwiększenie bezpieczeństwa danych i zapewnienie przejrzystości transakcji. W artykule omówimy znaczenie bezpieczeństwa w transakcjach internetowych i w jaki sposób blockchain jest w stanie je zabezpieczać.

1.1. Definicja blockchain

Blockchain to rozproszona baza danych, która składa się z bloków, które zawierają informacje o transakcjach. Bloki są łączone w jedną, niezmienną i rozproszoną sieć, która jest udostępniana wszystkim użytkownikom. Każdy nowy blok jest zabezpieczony za pomocą skomplikowanego algorytmu kryptograficznego, co zapewnia bezpieczeństwo danych. Blockchain jest bezpieczny, ponieważ każdy blok jest zabezpieczony i powiązany z poprzednim, co zapobiega jakimkolwiek zmianom w danych.

1.2. Znaczenie bezpieczeństwa w transakcjach internetowych

Bezpieczeństwo danych jest kluczowe w dzisiejszym świecie, w którym coraz więcej transakcji jest przeprowadzanych przez Internet. Niestety, tradycyjne systemy bankowe i finansowe są często narażone na cyberataki i nie są w pełni zabezpieczone przed nieautoryzowanym dostępem. W takich sytuacjach, blockchain może zapewnić dodatkową ochronę, ponieważ jego niezawodny i rozproszony charakter zabezpiecza dane przed nieautoryzowanym dostępem. Co więcej, blockchain pozwala na śledzenie każdej transakcji, co zapewnia przejrzystość i umożliwia szybką i skuteczną detekcję ewentualnych nieprawidłowości. W ten sposób, blockchain jest w stanie zapewnić dodatkowy poziom bezpieczeństwa w transakcjach internetowych, co jest szczególnie ważne w branży finansowej, gdzie każda nieautoryzowana transakcja może prowadzić do poważnych strat finansowych.

W kontekście bezpieczeństwa, blockchain jest również atrakcyjny dla przedsiębiorstw, ponieważ pozwala na przechowywanie i udostępnianie danych w sposób bezpieczny i zabezpieczony przed nieautoryzowanym dostępem. W ten sposób, blockchain jest w stanie zapewnić dodatkowy poziom ochrony danych osobowych i finansowych, co jest szczególnie ważne w dobie rosnącej liczby cyberataków.

Podsumowując, blockchain jest ważnym narzędziem w zabezpieczaniu transakcji internetowych i może zapewnić dodatkowy poziom bezpieczeństwa danych i transakcji. Jego rozproszona i niezawodna budowa pozwala na zabezpieczenie danych przed nieautoryzowanym dostępem i umożliwia śledzenie każdej transakcji, co zapewnia przejrzystość i bezpieczeństwo w branży finansowej i poza nią.

2. Geneza i historia blockchain

Blockchain to technologia oparta na koncepcji rejestru cyfrowego, która po raz pierwszy została opracowana w 2008 roku przez Satoshi Nakamoto, anonimowego twórcę i autora koncepcji kryptowaluty Bitcoin. Od tego czasu, blockchain rozwinął się i znalazł zastosowanie w wielu różnych dziedzinach, w tym w zabezpieczeniu transakcji internetowych. W niniejszym rozdziale przedstawiona zostanie historia i geneza powstania blockchain oraz najważniejsze momenty i milstone w jego rozwoju.

2.1. Powstanie i rozwój blockchain

Blockchain powstał jako część projektu o nazwie Bitcoin, opublikowanego w 2008 roku. Projekt ten zakładał stworzenie nowej formy cyfrowej waluty, która byłaby pozbawiona centralnej jednostki kontroli i której transakcje byłyby zabezpieczone za pomocą zdecentralizowanej i zabezpieczonej technologii blockchain.

Od tamtego czasu, blockchain ewoluował i stał się jednym z najważniejszych trendów w dziedzinie technologii informacyjnych. Wiele firm i organizacji zaczęło dostrzegać potencjał blockchain i wykorzystywać go do różnych celów, w tym do zabezpieczenia transakcji internetowych, zarządzania danymi i zasobami, udostępniania informacji i tworzenia nowych modeli biznesowych.

2.2. Kluczowe momenty i milestones

Niektóre z kluczowych momentów i milestones w historii blockchain to:

- Publikacja whitepaper Bitcoin w 2008 roku, który zapoczątkował powstanie blockchain i cyfrowej waluty Bitcoin.
- Wprowadzenie platformy Ethereum w 2015 roku, która umożliwiła tworzenie i uruchamianie aplikacji opartych na blockchain.
- Wzrost popularności kryptowalut w 2017 roku, co doprowadziło do zwiększenia zainteresowania blockchain i jego potencjału w różnych dziedzinach.
- Wprowadzenie regulacji i standardów dotyczących blockchain, które zaczęły powstawać w ostatnich latach, co umożliwia bezpieczne i zgodne z prawem wykorzystanie tej technologii.

3. Architektura blockchain i jej zastosowanie w zabezpieczeniu transakcji

W tym punkcie skupimy się na analizie architektury blockchain i jej zastosowaniu w zabezpieczeniu transakcji internetowych. Omówimy, jak działa blockchain, jakie zasady działania stanowią jego siłę i jakie są przykłady zastosowań tej technologii w zabezpieczeniu transakcji. Celem tego punktu jest zrozumienie mechanizmów, które sprawiają, że blockchain jest skutecznym narzędziem do zabezpieczenia transakcji.

3.1. Jak działa blockchain

Blockchain jest rozproszoną bazą danych, składającą się z wielu bloków połączonych w łańcuch. Każdy blok zawiera informację o transakcji i jest łączony z poprzednim blokiem przez funkcję skrótu. Funkcja ta gwarantuje, że każdy blok jest

jednoznacznie powiązany z poprzednim i następnym blokiem, co zapewnia integralność i nie zapisywalność danych w bazie.

3.2. Zasady działania blockchain w zabezpieczeniu transakcji

Blockchain wykorzystuje kryptografię do zabezpieczenia transakcji i utrzymania integralności danych. Każda transakcja jest zatwierdzana przez sieć użytkowników, a następnie zapisywana w bloku. Ten proces powoduje, że każda transakcja jest nieodwracalna i niepodlegająca edycji. Dzięki temu blockchain zapewnia bezpieczeństwo i prywatność danych oraz transakcji, co jest kluczowe w zabezpieczeniu transakcji internetowych.

3.3. Przykłady zastosowania blockchain w zabezpieczeniu transakcji

Blockchain jest wykorzystywany w wielu różnych dziedzinach, w tym w bankowości, handlu elektronicznym i ubezpieczeniach. Na przykład, w bankowości blockchain jest wykorzystywany do zapewnienia bezpieczeństwa i prywatności transakcji finansowych. W handlu elektronicznym blockchain jest wykorzystywany do zabezpieczenia danych i transakcji związanych z e-commerce. W ubezpieczeniach blockchain jest wykorzystywany do zapewnienia, że wszystkie transakcje związane z ubezpieczeniem są bezpieczne i niepodlegające edycji.

4. Zalety i wady blockchain w zabezpieczeniu transakcji

Ten rozdział poświęcony jest analizie zalet i wad blockchaina jako narzędzia do zabezpieczania transakcji internetowych. W ramach tego punktu omówione zostaną kluczowe aspekty bezpieczeństwa i niezawodności blockchaina, jego wydajności i efektywności, a także potencjalne ograniczenia i ryzyka z nim związane. Celem tego rozdziału jest zaprezentowanie pełnego obrazu możliwości i ograniczeń blockchaina w kontekście jego zastosowania w zabezpieczeniu transakcji internetowych.

4.1. Bezpieczeństwo i niezawodność blockchain

Jedną z kluczowych zalet blockchaina jest jego bezpieczeństwo i niezawodność. Blockchain jest zdecentralizowany, co oznacza, że nie ma jednego punktu kontroli, co znacznie utrudnia przeprowadzenie ataku hakerskiego. Ponadto, każdy blok w łańcuchu jest skryptowo powiązany z poprzednim blokiem, co oznacza, że każda zmiana w jednym bloku wprowadzona przez hakera jest natychmiast wykrywana i odrzucana.

4.2. Wydajność i efektywność

Blockchain jest również bardzo wydajny i efektywny, ponieważ wszystkie transakcje są przetwarzane równocześnie przez wiele komputerów, a nie tylko jeden centralny serwer. W rezultacie, blockchain jest w stanie przetwarzać duże ilości transakcji w krótkim czasie, co znacznie przyspiesza proces transakcyjny.

4.3. Ograniczenia i potencjalne ryzyka związane z blockchain

Choć blockchain oferuje wiele korzyści w zakresie bezpieczeństwa i wydajności, nie jest bez wad. W szczególności, blockchain jest nadal na początkowym etapie rozwoju i nie jest jeszcze powszechnie stosowany. Dlatego też, brak doświadczenia i wiedzy dotyczącej jego stosowania może prowadzić do błędów i potencjalnych ryzyk. Ponadto, ze względu na brak regulacji i standardów, może dojść do nieuczciwego lub nielegalnego wykorzystania blockchained. Warto więc dokładnie przeanalizować wszystkie aspekty stosowania blockchained i podejmować świadome i odpowiedzialne decyzje związane z jego zastosowaniem.

5. Przyszłość blockchain w zabezpieczeniu transakcji

Blockchain jest coraz częściej wykorzystywany do zabezpieczenia transakcji internetowych i jego popularność wciąż rośnie. W nadchodzących latach, jego rozwój i zastosowanie jest prognozowane jako jedno z kluczowych wydarzeń w świecie technologii i finansów. W tej sekcji będzie omówione kilka trendów i prognoz dotyczących przyszłości blockchain w zabezpieczeniu transakcji.

5.1. Trendy i prognozy

W ostatnich latach zauważalny jest wzrost zainteresowania blockchainem i jego wprowadzenie do różnych gałęzi przemysłu. Jego popularność wynika z jego unikalnych właściwości, takich jak bezpieczeństwo, niezawodność i efektywność. Prognozy mówią o dalszym rozwoju tej technologii i jej zastosowania w coraz większej liczbie branż.

5.2. Potencjalne zastosowania blockchain w zabezpieczeniu transakcji

Blockchain może być wykorzystywany do zabezpieczania różnych rodzajów transakcji, w tym transakcji finansowych, medycznych i logistycznych. Jego zastosowanie jest szczególnie atrakcyjne w przypadku transakcji, które wymagają wysokiego poziomu bezpieczeństwa i niezawodności, takich jak transfer pieniędzy i przetwarzanie danych osobowych.

5.3. Możliwe wyzwania i bariery w dalszym rozwoju

W ciągu najbliższych kilku lat, możemy spodziewać się dalszego rozwoju blockchain jako narzędzia do zabezpieczenia transakcji w Internecie. Mimo to, nadal istnieją wyzwania i bariery, które mogą uniemożliwić jego pełne wykorzystanie i rozwój. Jednym z głównych wyzwań jest brak zaufania do technologii, z powodu jej związku z kryptowalutami i różnego rodzaju nielegalnymi działaniami. Dodatkowo, dalszy rozwój blockchain będzie wymagać znacznych nakładów inwestycyjnych, aby zapewnić odpowiednią infrastrukturę i wsparcie.

Inną barierą może być opór ze strony rządów i regulujących organizacji, które mają obawy co do bezpieczeństwa i prywatności danych przetwarzanych w blockchain. Wiele państw wprowadziło już regulacje dotyczące kryptowalut i blockchain, ale ich stosowanie i skuteczność nadal pozostaje kontrowersyjna.

Pomimo tych wyzwań, wiele firm i organizacji dostrzega potencjał blockchain i inwestuje w jego rozwój. Dzięki temu, możliwe jest, że w przyszłości blockchain stanie się jeszcze bardziej powszechnym i skutecznym narzędziem do zabezpieczenia transakcji w Internecie.

6. Praktyczne zastosowanie blockchain w zabezpieczeniu transakcji internetowych.

Ten punkt skupia się na praktycznym zastosowaniu technologii blockchain w zabezpieczeniu transakcji internetowych. W ostatnich latach blockchain zyskał popularność jako bezpieczny i niezawodny sposób na przeprowadzenie transakcji online, zwłaszcza w kontekście finansów i walut kryptograficznych. W tym punkcie omówione zostaną zagrożenia związane z transakcjami online oraz sposoby, w jakie blockchain może pomóc w zabezpieczeniu transakcji przed takimi zagrożeniami. Przedstawione zostaną również przykłady konkretnych zastosowań blockchain w celu zapewnienia bezpieczeństwa i niezawodności transakcji internetowych.

6.1. Transakcje online jako potencjalne zagrożenie.

Transakcje online stanowią coraz większe zagrożenie dla bezpieczeństwa danych i informacji o transakcji. Hakerzy i cyberprzestępcy są coraz bardziej zdeterminowani, aby uzyskać dostęp do wrażliwych informacji i pieniędzy. Konwencjonalne metody zabezpieczania transakcji online takie jak hasła i szyfrowanie danych stają się coraz bardziej nieefektywne, ponieważ hakerzy są w stanie uzyskać dostęp do nich za pomocą coraz bardziej zaawansowanych technik.

6.2. Blockchain jako sposób na zwiększenie bezpieczeństwa i niezawodności transakcji online.

Blockchain może być użyty jako narzędzie do zwiększenia bezpieczeństwa i niezawodności transakcji online. Jego zdecentralizowana struktura pozwala na uwierzytelnianie i weryfikację transakcji bez potrzeby korzystania z centralnego punktu, co zwiększa bezpieczeństwo i niezawodność. Ponadto, blockchain jest oparty na matematycznych algorytmach i kryptografii, co dodatkowo zwiększa bezpieczeństwo transakcji.

6.3. W jaki sposób można zastosować blockchain w zabezpieczeniu transakcji online.

Istnieje kilka sposobów, w jakie blockchain może być zastosowany do zabezpieczenia transakcji online. Przykłady to:

- Uwierzytelnianie tożsamości użytkownika przed dokonaniem transakcji
- Bezpieczne przesyłanie i przechowywanie informacji o transakcji

- Zabezpieczenie przed kradzieżą danych i oszustwami
- Zabezpieczenie przed nieautoryzowanym dostępem do informacji o transakcji
- Zabezpieczenie przed fałszywymi transakcjami i podszywaniem się

6.4. Przykłady zastosowań blockchain w zabezpieczeniu transakcji online, takie jak:

Ten podpunkt skupia się na przykładach zastosowań blockchain w zabezpieczeniu transakcji online. W tym kontekście blockchain postrzegany jest jako narzędzie, które może zwiększyć bezpieczeństwo i niezawodność transakcji online poprzez wprowadzenie rozproszonego systemu rejestracji transakcji. W punkcie tym zostaną omówione różne przykłady zastosowań blockchain, które pomagają zabezpieczyć transakcje online przed różnymi zagrożeniami, takimi jak kradzież danych, oszustwa, nieautoryzowany dostęp i fałszywe transakcje.

6.4.1. Bezpieczne przesyłanie i przechowywanie informacji o transakcji.

Jest to jedna z kluczowych zalet stosowania blockchain w transakcjach online jest bezpieczne i niezawodne przesyłanie i przechowywanie informacji o transakcji. Dzięki temu, że informacje te są zapisywane w sieci i dostępne dla wszystkich użytkowników, jest możliwe uniemożliwienie ich modyfikacji czy usunięcia przez osoby niepowołane.

6.4.2. Zabezpieczenie przed kradzieżą danych i oszustwami.

Blockchain zapewnia także zabezpieczenie przed kradzieżą danych i oszustwami. Dzięki temu, że informacje o transakcji są zapisywane w sieci i dostępne dla wszystkich użytkowników, jest trudne do wykonania przez cyberprzestępców.

6.4.3. Zabezpieczenie przed nieautoryzowanym dostępem do informacji o transakcji.

Blockchain umożliwia także zabezpieczenie przed nieautoryzowanym dostępem do informacji o transakcji. Dzięki temu, że informacje te są zaszyfrowane i dostępne tylko dla zatwierdzonych użytkowników, jest możliwe uniemożliwienie ich ujawnienia osobom trzecim.

6.4.4. Zabezpieczenie przed fałszywymi transakcjami o podszywaniem się.

Blockchain pozwala także na zabezpieczenie przed fałszywymi transakcjami i podszywaniem się. Dzięki temu, że informacje o transakcji są zapisywane w sieci i niepodatne na modyfikacje, jest trudne do wykonania przez cyberprzestępców.

6.4.5. Weryfikacja i uwierzytelnianie tożsamości użytkownika przed dokonaniem transakcji.

Weryfikacja i uwierzytelnianie tożsamości użytkownika przed transakcją to ważny aspekt zabezpieczenia online, który można zrealizować za pomocą blockchain. Uwierzytelnienie odbywa się za pomocą unikatowych kluczy i haseł, skanowania biometrycznego lub weryfikacji na podstawie danych demograficznych. To zapobiega nieautoryzowanym transakcjom i jest szybkie, wygodne i bezpieczne dla użytkownika.

6.5. Praktyczne zastosowanie blockchain w zabezpieczeniu transakcji

Przykładowy kod wykorzystujący blockchain w zabezpieczeniu transakcji można zapisać w języku programowania Solidity, który jest używany do tworzenia inteligentnych kontraktów w sieci Ethereum. Poniżej przedstawiam prosty przykład kontraktu, który umożliwia dwóm użytkownikom wymianę waluty za pomocą blockchain:

```
pragma solidity ^0.4.24;

contract SecureExchange {
    address public user1;
    address public user2;
    mapping (address => uint) public balances;

    event Transfer(address from, address to, uint amount);

    constructor() public {
        user1 = msg.sender;
    }

    function setReceiver(address receiver) public {
        require(msg.sender == user1, "Only user1 can set the receiver.");
        user2 = receiver;
    }

    function deposit() public payable {
        balances[msg.sender] += msg.value;
    }

    function withdraw(uint amount) public {
        require(balances[msg.sender] >= amount, "Insufficient balance.");
        balances[msg.sender] -= amount;
        msg.sender.transfer(amount);
        emit Transfer(msg.sender, address(this), amount);
    }
}
```

```

function exchange(uint amount) public {
    require(msg.sender == user1 || msg.sender == user2,
"Unauthorized user.");
    require(balances[msg.sender] >= amount, "Insufficient
balance.");
    balances[user1] += amount;
    balances[user2] -= amount;
    emit Transfer(msg.sender, msg.sender == user1 ? user2 :
user1, amount);
}
}

```

W tym przykładzie kontrakt umożliwia użytkownikom przesyłanie i wymianę środków z wykorzystaniem blockchain. Kontrakt utrzymuje informacje o adresach użytkowników oraz ich saldach. Użytkownicy mogą wpłacać środki na swoje konto, wypłacać je lub wymieniać z innym użytkownikiem.

W kontrakcie wykorzystano również zdarzenia, które pozwalają na śledzenie przepływu środków w sieci Ethereum. Zdarzenie Transfer jest emitowane za każdym razem, gdy użytkownik wykonuje wpłatę, wypłatę lub wymianę. Dzięki temu zdarzeniu można łatwo śledzić historię transakcji w sieci.

Przykład ten jest bardzo prosty i ma charakter edukacyjny. W rzeczywistych aplikacjach blockchain, takich jak kryptowaluty czy platformy ICO, kontrakty są bardziej skomplikowane i wymagają bardziej zaawansowanego kodowania.

7. Zakończenie

Ten punkt ma na celu podsumowanie wszystkich ważnych informacji i wniosków, które zostały przedstawione wcześniej. W tym rozdziale będzie przedstawione w skrócie wszystko, co zostało opisane wcześniej, a także ewentualne rekomendacje dotyczące dalszego rozwoju i zastosowania blockchain w zabezpieczeniu transakcji.

7.1. Podsumowanie kluczowych informacji

Blockchain jest technologią, która pojawiła się w 2008 roku i od tego czasu cieszy się stale rosnącą popularnością. Jest to rozproszona i zdecentralizowana baza danych, która umożliwia bezpieczne i zaufane przeprowadzanie transakcji. W odróżnieniu od klasycznych systemów, w których transakcje są kontrolowane przez pojedyncze jednostki, blockchain zapewnia bezpieczne i niezawodne środowisko, w którym transakcje są kontrolowane przez sieć uczestników.

7.2. Wnioski i rekomendacje

Blockchain jest uważany za jedną z najważniejszych i najbardziej przełomowych technologii ostatnich lat. Ma on ogromny potencjał, aby zmienić sposób, w jaki wiele branż i sektorów działa. W szczególności w zakresie bezpieczeństwa transakcji,

blockchain jest uważany za jeden z najbardziej obiecujących i skutecznych rozwiązań. Warto jednak pamiętać, że jak każda technologia, blockchain również ma swoje wady i ograniczenia, a jego dalszy rozwój i zastosowanie będzie wymagać rozwiązania szeregu wyzwań i barier.

Ogólnie rzecz biorąc, zalecamy zainteresowanie się blockchain i jego możliwościami, a także śledzenie najnowszych trendów i rozwoju tej technologii. Może ona mieć kluczowe znaczenie dla przyszłości bezpieczeństwa transakcji w Internecie.

8. Literatura

- [1] Andreas M. Antonopoulos. (2014). Mastering Bitcoin: Unlocking Digital Cryptocurrencies. O'Reilly Media, Inc.
- [2] Don Tapscott, Alex Tapscott. (2016). Blockchain Revolution: How the Technology Behind Bitcoin Is Changing Money, Business, and the World. Penguin.
- [3] Tiana Laurence. (2018). Blockchain for Dummies. John Wiley & Sons.
- [4] Daniel Drescher. (2017). Blockchain Basics: A Non-Technical Introduction in 25 Steps. Apress.
- [5] Narula, N., Bonneau, J., Felten, E., Miller, A., & Goldfeder, S. (2016). Bitcoin and Cryptocurrency Technologies: A Comprehensive Introduction. Princeton University Press.
- [6] Szabo, N. (1997). Formalizing and Securing Relationships on Public Networks. First Monday, 2(9).
- [7] Nakamoto, S. (2008). Bitcoin: A Peer-to-Peer Electronic Cash System. <https://bitcoin.org/bitcoin.pdf>