INCARE
INTERNATIONAL JOURNAL OF EDUCATIONAL RESOURCES
Volume 02, Number 02 August 2021

IMPLEMENTASI BLOCKCHAIN DALAM APLIKASI PEMILU

Yulfitno Wingga Pratama[1], Denny Kurniadi[2]
Universitas Negeri Padang (UNP), Indonesia
email: yulfitno@gmail.com

Abstract

Elections are a democratic activity in Indonesia which are carried out every five years to elect leaders, but in the process of manual election calculations, the results are leaked and can cause data security problems. Through this research, we can provide solutions by implementing blockchain technology in election applications that will provide security for election results data stored on the blockchain. Blockchain technology is a chain of data blocks that are connected to each other by peer to peer. This application uses the Solidity programming language and uses a local ethereum blockchain database (Ganache). The method used in making this application is the waterfall method with Unified Modeling Language (UML) modeling where the visual modeling method is in object-oriented system design. From the results of testing the blockchain system for this application, it is found that blockchain can help secure election results very securely, where every result data will be stored in every block in a decentralized blockchain network.

Keywords: *Election, Blockchain, Ganache (Local Ethereum Blockchain)*

Accepted:	Reviewed:	Published:
July 15 2021	July 22 2021	August 30 2021

A. Pendahuluan

Pemilihan umum berkala merupakan prasyarat bagi suatu bentuk pemerintahan yang demokratis, karena pemilihan umum merupakan cara untuk melaksanakan kedaulatan rakyat yang diselenggarakan secara langsung, umum, rahasia, jujur, dan adil dalam Negara Kesatuan Republik Indonesia (NKRI) untuk memimpin suatu negara. pemerintahan yang didukung oleh demokrasi pancasila dan UUD 1945. Manipulasi suara sering terjadi pada akhir pemilu, seperti segel safety box rusak atau hasil pemilu rusak karena perselisihan antar Pasangan Calon (Paslon). Salah satu cara mengatasi permasalahan pemilu konvensional adalah dengan menerapkan sistem pemilu elektronik. Dengan menggunakan teknologi blockchain, setiap transaksi yang terjadi akan dienkripsi menggunakan Secure Hash Algorithm 256 (SHA-256) dan akan membuat semacam rantai blok dan

mengirimkannya ke semua jaringan yang terhubung peer-to-peer sehingga semua dapat memvalidasi masing-masing transaksi (Schneier, 1996).

Blockchain adalah teknologi *cryptocurrency* dari *bitcoin*, teknologi ini ditemukan oleh "Satoshi Nakamoto" pada tahun 2008. Saat ini, *blockchain* telah diimplementasikan dalam banyak hal, termasuk identitas digital, pemungutan suara digital, dan notaris yang terdesentralisasi. Secara sederhana, blockchain dapat digambarkan sebagai database terdesentralisasi, tanpa kepercayaan antar *node* dalam jaringan *peer-to-peer* (Ellervee, 2017). *Blockchain* menggunakan banyak fungsi *hash* dalam prosesnya. *Hash* membantu blockchain untuk mendeteksi jika ada data yang diubah karena kesalahan jaringan. Dari *hash* yang sudah digunakan di *blockchain*, *has*h selalu berukuran sama, dua *string* yang identik akan menghasilkan *hash* yang sama, dua *string* yang berbeda akan menghasilkan *hash* yang berbeda dan membuat string yang cocok dengan *hash* yang diberikan sangat sulit.

Perancangan aplikasi ini menggunakan bahasa pemrograman Solidity untuk membuat kontrak dengan blockchain Ethereum. Soliditas adalah bahasa tingkat tinggi yang digunakan untuk mengimplementasikan kontrak pintar (Mohanta dkk., 2018). Bahasa Soliditas ditulis dalam file .sol, dan soliditas sangat mirip dengan sintaksis javascriptnya, diketik secara statis, mendukung pewarisan dan polimorfisme, serta tipe dan pustaka kompleks yang ditentukan pengguna. Kontrak cerdas adalah prosedur tertanam yang disimpan dengan data yang ditindaklanjuti. Men-debug kontrak pintar adalah tugas yang sangat sulit karena setelah digunakan, kode tidak dapat diakses kembali dan pemeriksaan atribut sederhana tidak mudah dilakukan karena data dikodekan (Bragagnolo dkk., 2018).

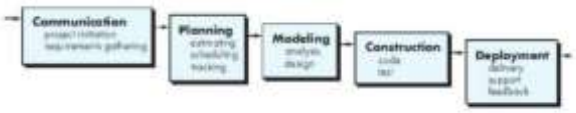
Perancangan aplikasi ini diharapkan dapat mengatasi proses penghitungan hasil akhir penghitungan suara di TPS oleh panitia KPU (Dagher dkk., 2018). Dengan menerapkan *blockchain* dan memanfaatkan setiap node yang terhubung ke jaringan yang sama, hasil pemilihan akhir akan terlihat sama untuk semua pihak yang terhubung ke jaringan.

B. Metode Penelitian

1. Metode *Waterfall*

Menurut Pressman (2015:42), model *waterfall* adalah model klasik yang bersifat sistematis, berurutan dalam membangun *software.* Nama model ini sebenanrnya adalah "*Linear Sequential Model*". Model ini sering disebut juga dengan "*classic life cycle*" atau metode waterfall. Model ini termasuk ke dalam model generic pada rekayasa perangkat lunak dan pertama kali diperkenalka oleh Winston Royce sekitar tahun 1970 dan merupakan model yang paling banyak di

pakai dalam *Software Engineering* (SE). Berikut merupakan fase-fase dalam model waterfall menurut Pressman :



Gambar.1 Model waterfall menurut pressman

Dalam perancangan ini menggunakan Teknik sebagai berikut :

a. Planning
   Tahapan perencanaan yang menjelaskan tentang teknis, sumber daya dan hasil dari prodek yang ingin dihasilkan
b. Modelling
   Tahapan ini adalah tahap perancangan dan pemodelan arsitektur yang berfokus pada perancangan struktur data, arsitektur software, tampilan interface dan algoritma program.
c. Construction
   Tahapam ini merupakan proses penerjemahan bentuk desain menjadi kode atau bentuk yang dapat dibaca oleh mesin. Setelah pengkodean selesai dilakukan pengujian terhadap sistem dan kode yang sudah dibuat.
d. Deployment
   Tahapan ini merupakan tahapa implementasi software ke penelitian yang dilakukan

2. Analisis Sistem

Menurut (Yogiyanto, 1995) analisis sistem adalah penguraian dari suatu sistem informasi yang utuh kedalam bagian-bagian komponennya dengan maksud untuk mengidentifikasi dan mengevaluasi permasalahan, kesempatan , hambatan yang terjadi sesuai kebutuhan yang diharapakan sehingga dapat diusulkan perbaikan. Tujuan dari analisis sistem ini untuk mempersiapkan hal-hal yang perlu dikembangkan dalam perancangan suatu sistem informasi, serta maenganalisis permasalahan, kebutuhan, dan kelemahan oleh pemakai sistem untuk dapat memberikan solusi ke dalam unsur-unsur yang terlibat yaitu :

a. Analisis Proses Bisnis

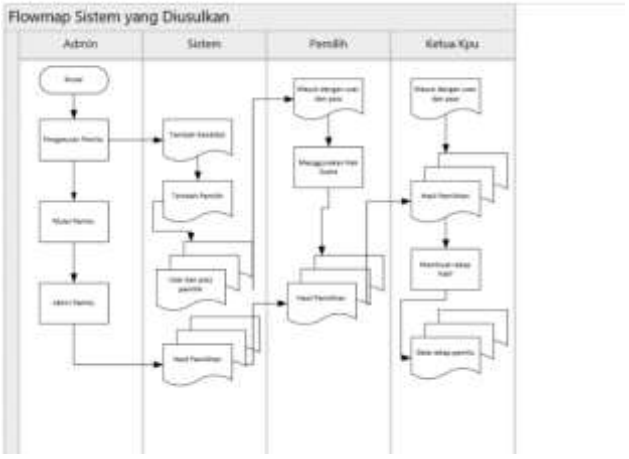
Proses bisnis (*business process*) dapat didefinisikan sebagai kumpulan aktivitas atau pekerjaan terstruktur yang saling terkait untuk menyelesaikan suatu masalah tertentu atau yang menghasilkan produk dan atau layanan tertentu (Weske, 2007).

Tabel 1. Analisis Proses Bisnis

No	*Proses bisnis*	*Aktivitas*
1	Pengelolaan Pemilihan	• Admin atau staff terkait mengisi data yang diperlukan untuk pelaksanaan pemilu • Admin atau staff terkait membuat akun • Admin atau staff terkait memulai pemilihan umum • Admin atau staff terkait mengakhiri pemilihan umum
2	Pengelolaan pemilih	• Pemilih mndaftar di sistem dengan alamat, nama dan no ktp • Admin atau staff terkait menerima dan memverifikasi data dari pemilih
3	Proses voting	• Data pemilih yang telah diverifikasi oleh admin dan bisa langsung menggunakan hak suara
4	Proses Hasil Pemilu	• Setiap vote dari pemilih akan langsung masuk kedatabase blockchain dan akan membuat blockc setiap data yang masuknya • Rekap hasil akan ditampilkan setelah waktu pemilu habis dan di akhiri oleh admin

b. Flowmap Sistem Yang diusulkan

Menurut (Meza Silvana, Dkk, 2015) flowmap merupakan penggambaran secara grafik dari Langkah-langkah dan urutan-urutan prosedur dari suatu program. Flowmap sistem yang diusulkan ini berisi tentang alur aplikasi dari beberapa actor mulai dari mulai sampai akhir proses aplikasi.



Gambar 2*. Flowmap* Sistem yang diusulkan

Flowmap sistem dijelaskan tahap berjalan nya sistem dimulai dengan admin yang mengatur segala hal tentang pemilihan mulai dari penambahan kandidat , tambah akun pemilh, memulai dan mengakhiri pemilu. Pemilih yang telah

mendapatkan *username* dan *password* akan bisa menggunakan hak suara. Ketika pemilihan berakhir semua *user* akan bisa mengakses hasil dari pemilihan.

c. Analisis Kebutuhan

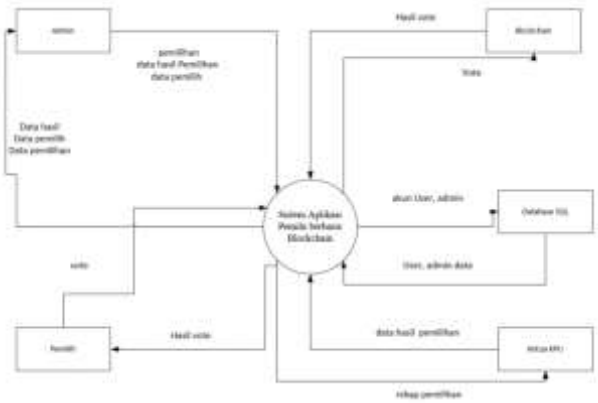
analisis kebutuhan merupakan suatu proses yang sistematis dalam menentukan kebutuhan dalam menjalankan aplikasi (Briggs, 1991). ada dua kebutuhan perangkat keras dan perangkat lunak. Kebutuhan untuk perangkat keras adalah spesifikasi perangkat keras yang digunakan untuk menjalankan aplikasi ini yaitu : min cpu (intel core i3/amd A5), disk (10GB), ram (4GB), monitor (14 inch) dan input (keyboard dan mouse). Untuk perangkat lunak yaitu : sistem operasi (win 7/win 10), database (ganache), web server (web3.js), framework (truffle) dan aplikasi pendukung (metamask dan google).

2. Perancangan Sistem

Menurut (Kenneth dan Jane , 2006 : G12) perancangan sistem adalah kegiatan dalam merancang dan menetukan cara mengolah sistem informasi dari hasil Analisa sehingga sistem tersebut sesuai dengan requirement

1) Context Diagram

Context diagram merupakan diagram pertama dalam rangkaian data flow diagram yang menggambarkan entitas yang berhubungan dengan sistem (jogiyanto , 2005) .

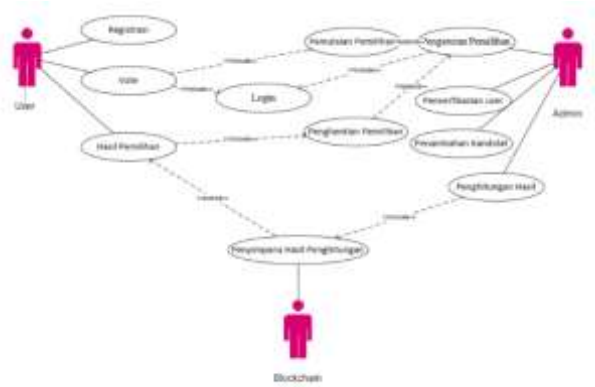


Gambar 3. Context Diagram

Context diagram diatas terlihat ada 5 terminator dalam aplikasi ini adalah: admin, pemilih, *database sql*, ketua kpu dan *blockchain*. Data admin dan pemilih akan disimpan di sql dan data hasil pemilih akan disimpan di *blockchain*.

2) *Use Case* Diagram

Menurut Sukamto dan Shalahuddin (2014: 155) *use case* diagram merupakan pemodelan untuk sistem yang akan dibuat .*Use case* diagram menjelaskan bahwa alur dari suatu kegiatan yang mencapai tujuan tertentu. Pada *use case* dibawah ini dijelaskan pada gambar bahwa yang punya akun hanya dapat memvoting sekali

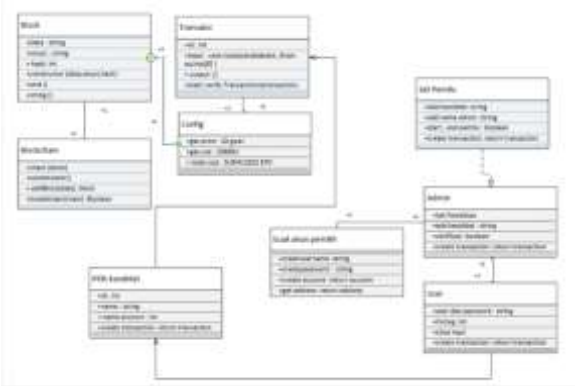


Gambar 4. *Use Case Diagram*

Use case dijelaskan admin memiliki fungsi mengatur pemilihan, mengatur pemilih dan hasil pemilihan. Setelah user registrasi akan diverifikasi oleh admin dan user baru bisa melakukan hasil *voting*, hasil *voting* akan masuk ke *blockchain*.

3) Class Diagram

Menurut Sri Mulyani (2016: 247) mendefinisikan adalah diagram yang digunakan untuk mempresentasikan kelas, komponen-komponen kelas dan hubungan antar masing-masing kelas. Menunjukkan hubungan antar class dalam sistem yang sedang dibangun dan bagaimana diagram tersebut saling berkolaborasi untuk mencapai suatu tujuan.

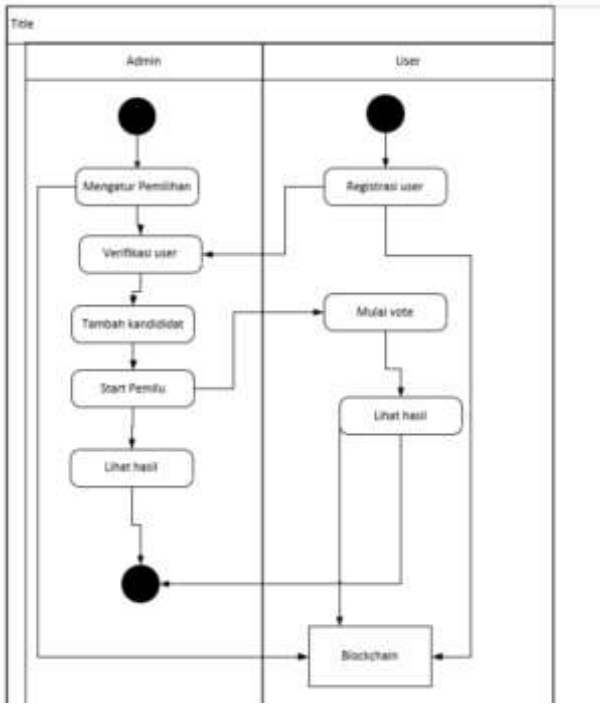


Gambar 5. *Class Diagram*

Class diagram diatas menunjukkan *class diagram* pada transaksi *blockchain* dan sudah ditambah dengan implementasi sistem yang dibuat

4) Activity Diagram

Menurut Sukamto dan Shalahuddinn (2014 : 161) adalah menggambarkan aliran kerja dari sebuah sistem pada perangkat lunak. Teknik mendeskripsikan logika *procedural*, proses bisnis dan aliran kerja dalam banyak kasus.

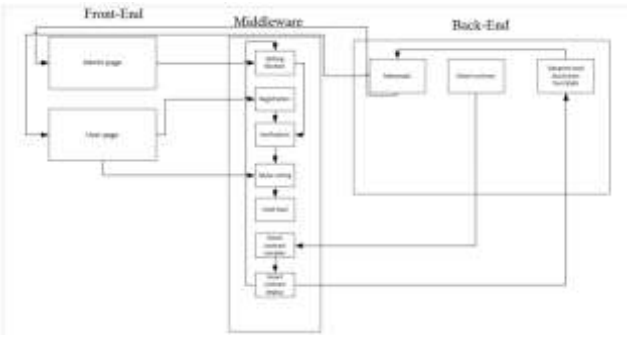


Gambar 6. *Activity Diagram*

Activity diagram dari admin mengatur pemilihan kemudian menambah kandidat kemudian menjalankan pemilu dan kemudian user melakukan registrasi setelah itu admin akan memverifikasi data user dan data user baru bisa melakukan *voting* dari hasil pemilu akan tersimpan di jaringan *blockchain*.

5) Perancangan Arsitektur Sistem

Arsitektur sistem adalah model konseptual yang mendefinisikan struktur, perilaku dan pandangan dari suatu sistem, deskripsi arsitektur adalah deskripsi formal dan representasi dari suatu sistem yang digunakan untuk mendukung penjelasan tentang struktur sistem (Nugroho, 2005). Dalam perancangan arsitektur sistem ini terdapat beberapa bagian yaitu front-end, middleware dan backend



Gambar 7. Arsitektur Perancangan Sistem

ada beberapa bagian dari arsitektur sistem yaitu sebagai berikut :

- *User page (front-end)* Menurut Career Foundry, frontend adalah bagian yang bertugas menghubungkan sebuah situs atau aplikasi pengguna. Pada frontend aplikasi ini menampilkan nama kandidat *vote*, info akun dan *button vote* dan halaman admin serta registrasi dan *setting* pemilihan
- *Middleware* , pada bagian ini merupakan bagian tengah yang menghubungkan komponen *front-end dengan komponen lain nya*
- *Back-end*, merupakan bagian belakang dari sebuah web. Backend sistem yang menggunakan *local host blockchain port 8545*, metamask penghubung *smart contract* dengan *browser*.

6) Analisis Kebutuhan Blockchain

Perancangan sistem dengan *blockchain* ada beberapa bahan pendukung yang akan bisa membuat *blockchain* berjalan disistem yang ada sebagai berikut :

- *Ethereum,* dengan *Ethereum blockchain* dapat diprogram membuat aplikasi desentralisasi sesuai kebutuhan pengguna
- *Smart contract*, sebuah pernjanjian yang diubah dalam bentuk digital sehingga penjanjian sulit dilakukan (Atzei dkk., 2017).
- *Address,* untuk membuat identitas unik dalam *etherum blockchain* (Liu & Wang, 2017)
- *Node.Js*, alat open source yang digunakan untuk menulis kontrak *solidity* langsung dari browser.
- *Solidity*, Bahasa pemrograman objek untuk menulis *smart contract blockchain* (Dannen, 2017).
- *Metamask,* Aplikasi *browser* yang memudahkan untuk berinteraksi dengan web berbasis *Ethereum*.
- Sublime text 3 sebagai teks editor.

7) Rancangan Antar Muka Aplikasi

Perancangan antar muka aplikasi ini terdapat dua halaman yang ada yaitu halaman *admin* dan halaman user (pemilih). Untuk rancangan antar muka aplikasi ini menggunakan model *react.js* yang juga digunakan dalam pembuatan *UI Facebook* dan *Instagram* . Ada beberapa halaman *interface* yang akan dibahas sebagai berikut :

a) Desain Halaman Admin

Pada halaman admin berisi data admin dan pengaturan pemilihan

b) Desain Halaman Tambah Kandidat

Halaman tambah kandidat calon oleh admin

c) Desain Halaman Registrasi User

Halaman regitrasi pemilih berdasarkan alamat akun ether

d) Desain Halaman Verifikasi User

Halaman verifikasi pemilih oleh admin

e) Desain Halaman Voting

Halaman voting calon kandidat oleh pemilih

f) Desain Tampilan Halaman Hasil

Halaman hasil baik pemilih maupun admin sistem bisa melihat hasil ketika pemilihan berakhir

C. Hasil dan Pembahasan

1. Hasil Pembuatan

Pembuatan Aplikasi pemilu ini dengan implementasi *blockchain* ini memiliki tujuan untuk mengamankan data hasil pemilihan umum sehingga data

hasil yang rentan akan kecurangan akan tersimpan di setiap *block* di dalam jaringan *blockchain* secara *peer-to-peer* (Davis, 2018).

2. Implementasi Sistem

Tahap implementasi merupakan kegiatan pembuatan sistem atau aplikasi dengan menggunakan bantuan perangkat lunak maupun perangkat keras sesuai dengan analisis dan perancangan untuk menghasilkan suatu sistem yang bekerja. Sistem ini diimplementasikan menggunakan *solidity v5.0* untuk pengolahan kode program (*back-end*), *javacript Sintax Ekstensiom (JSX)* sebagai pengolah *user interface (front-end).*

3. Pengujian Sistem Berdasarkan Aspek Dasar Blockchain

Tahap pengujian ini didasarkan sifat dasar *blockchain* yaitu sebagai berikut:

a. Immutability

Adalah sifat dimana data input yang masuk ke dalam sistem *blockchain* tidak dapat dirubah atau dihapus (Narayanan dkk., 2016)

Seperti yang terlihat pada gambar diatas terdapat beberapa detil komponen transaksi blockchain yaitu Hash, Nonce, blockHash, blockNumber, Transaction Index, value dan v,r,s. ada 7 layer keamanan dalam suatu block dan membutuhkan waktu dan resources yang tepat untuk membuka dan merubah data dalam kemamanan 7 tingkat layer tersebut bisa di pertanggungjawabkan sifat immutability nya.

b. Transparansi

Adalah sifat *blockchain* dimana setiap perubahan data yang terjadi dalam sistem berbasis *blockchain* dapat dilihat oleh seluruh partisipan yang terlibat (Xinyi dkk., 2018). Setiap *vote* yang dilakukan makan pada *blockchain* akan terbentuk *block* baru seperti berikut

c. Terdesentralisasi

Pada sifat ini data yang terdistribusi kepada setiap partisipan yang terlibat sehingga semua partisipan mempunyai data Salinan yang sama (Zheng dkk., 2017). Pada kasus ini perancangan aplikasi ini semua jenis user akan dapat mengakses data hasil pemilihan sehingga bisa disebut terdesentralisasi

D. Simpulan

Berdasarkan perancangan yang telah dilakukan, beberapa poin kesimpulan sebagai berikut :

1. Perancangan ini dilakukan dengan mendefinisikan *asset participant* dan *transaction* yang terlibat dalam sistem database yang dibangun. Dengan hasil berupa jaringan *local blockchain* port 8545 dengan *local host metamask* port yang sama
2. Hasil fungsionalitas aplikasi sekitar 90% dari keseluruhan analisis fungsionalitas

Daftar Rujukan

Atzei, N., Bartoletti, M., & Cimoli, T. (2017). A survey of attacks on ethereum smart contracts (sok). *International conference on principles of security and trust*, 164–186.

Bragagnolo, S., Rocha, H., Denker, M., & Ducasse, S. (2018). SmartInspect: solidity smart contract inspector. *2018 International workshop on blockchain oriented software engineering (IWBOSE)*, 9–18.

Briggs, L. J. (1991). *Instructional design: Principles and applications*. Educational Technology.

Dagher, G. G., Marella, P. B., Milojkovic, M., & Mohler, J. (2018). *Broncovote: Secure voting system using ethereum's blockchain*.

Dannen, C. (2017). *Introducing Ethereum and solidity* (Vol. 318). Springer.

Davis, J. (2018). Peer to peer insurance on an Ethereum blockchain. *Dynamis*

Whitepaper. Retrieved February 18th f.

Ellervee, A. (2017). A reference model for Blockchain-based distributed ledger technology. *Unpublished master's thesis), University of Tartu*.

Liu, Y., & Wang, Q. (2017). An E-voting Protocol Based on Blockchain. *IACR Cryptol. ePrint Arch.*, *2017*, 1043.

Mohanta, B. K., Panda, S. S., & Jena, D. (2018). An overview of smart contract and use cases in blockchain technology. *2018 9th International Conference on Computing, Communication and Networking Technologies (ICCCNT)*, 1–4.

Narayanan, A., Bonneau, J., Felten, E., Miller, A., & Goldfeder, S. (2016). *Bitcoin and cryptocurrency technologies: a comprehensive introduction*. Princeton University Press.

Nugroho, A. (2005). *Analisis dan Perancangan Sistem Informasi dengan Metodologi Berorientasi Objek. Edisi Revisi*.

Schneier, B. (1996). *Applied Cryptography Second Edition: protocols, algorithms, and source code in CJ Wiley & Sons*. Inc.

Xinyi, Y., Yi, Z., & He, Y. (2018). Technical characteristics and model of blockchain. *2018 10th international Conference on communication Software and networks (ICCSN)*, 562–566.

Zheng, Z., Xie, S., Dai, H., Chen, X., & Wang, H. (2017). An overview of blockchain technology: Architecture, consensus, and future trends. *2017 IEEE international congress on big data (BigData congress)*, 557–564.