A permissioned blockchain prototype facilitating banking record interoperability

University of Essex

Anrich Potgieter

November 10, 2022

Declaration

Test text

Abstract

Acknowledgements

Contents

Chapter 1

Introduction

Chapter 2

Background Literature

2.1 Defining Blockchain Technology

2.1.1 Background

Blockchain technology reaches back far further than the inception of Bitcoin, and we can see some of the first implementations appearing in 1998. In a 1998 white paper titled bmoney, we see some of the earliest building blocks of cryptocurrencies and the adoption of blockchain technologies (Dai 1998). Wei Dai outlines some cornerstone concepts that would later inspire Satoshi Nakamoto to create Bitcoin. Wei begins to outline a form of Zero Knowledge proof where two parties involved in an exchange or transaction use pseudonyms in the form of public keys to identify themselves within the context of a transaction (*Zero-Knowledge Proofs — Ethereum.Org* 2022). Furthermore, Wei begins laying the foundation of cryptographically complex puzzles that are solved to determine the value of the currency transferred. The concepts mentioned above would eventually lead to one of the crucial components of blockchains known as proof of work.

Further to the cryptographic puzzles introduced by Wei Dai in 2002, we see the emergence of a white paper by Adam Back titled hashcash (Back 2002). Back, originally envisioned these concepts to solve denial of service attacks on email servers where communication over these email protocols would come at a greater cost of computational power. Later Back realised that this denial of service concept would effectively translate into a proof-of-work function where this function would create a token representing the computational complexity required to solve the hash.

As seen above, proof-of-work is an essential cornerstone of blockchain technology and is historically significant to one of the most important blockchains in history, bitcoin. 2004 was potentially the most crucial year in the history of blockchain technology; in a white paper titled RPOW - Reusable Proofs of Work by Hal Finny, we observe a piece of client software that creates an RPOW token cryptographically signed by the client's private key (Finney 2022). The token mentioned before is stored on a secure server that identifies the stored token ownership by the private key. If the private key owner wishes to transfer this token to another user, they sign a transfer order which is stored as a public key; the server then assigns the transferred token to the new owner's private key.

In 2008 we observed a culmination of various concepts seen within the cryptography development space with the emergence of the infamous blockchain, Bitcoin. In the white paper by Satoshi Nakamoto, the fundamental components of blockchain technology appear in a concise collection of computing concepts that facilitate a blockchain where a user can store electronic cash without a third-party financial institution (Nakamoto 2008). The Bitcoin whitepaper introduces the fundamental components of a blockchain with an overview of how these components work together. The fundamental components or concepts outlined are transactions, timestamp server, proof-of-work, networks (Nodes), incentives and payment verification. The concepts mentioned above provided a foundation for future blockchain development and research directions.

In 2014 sometime after the initial release of Bitcoin, a white paper by Vitalik Buterin surfaced titled Ethereum, where Buterin outlined a vision for the future of blockchain development (Vitalik 2014). Buterin proposed the expansion of the fundamental components of Bitcoin to create a development environment facilitating the creation of "consensus-based applications". Furthermore, Buterin surmises a new addition to the standard blockchain: the smart contract. The aforementioned smart contract is defined as a "computerised transaction protocol" that defines a series of contractual conditions once met, a transaction is complete (Yaga et al. 2018). The invention of smart contacts has significantly repositioned blockchain technology to solve various complex trust-based scenarios in many industries.

The concepts outlined before are essential concepts required to create a blockchain. (Di Pierro 2017) states that blockchains solve the problem of establishing trust in a "distributed system". Furthermore, (Yaga et al. 2018) outlines that blockchains provide reliable trust mechanisms using a "tamper resistant digital ledger." The ledger relies on a peer-to-peer network with a series of

nodes which synchronously replicate data across the network to ensure data availability across the network (Butijn, Tamburri, and Heuvel 2020). Hashing network time stamps into a continuous chain of ”hash-based proof-of-work” blocks ensure the reliability of the data, furthermore it would be impossible to make changes to data without asking nodes in the network to re-do the proof of work.

In the sections below, we will explore the components and concepts of blockchain technology to reveal future development opportunities and use cases for blockchains in banking organisations.

2.1.2 Types of Blockchains

Blockchains typically fall into three succinct categories, permissionless, permissioned and consortium. Historically permissionless blockchains are most prevalent; however, permissioned blockchains have come to the forefront as the need for blockchain technology has emerged in various industries with different use cases (Yaga et al. 2018). A further extension of private or permissioned blockchains is consortium blockchains where authenticated participants are decided by a consortium or organisation (Leible et al. 2019).

Permissionless

Permissionless blockchains are those in which any individual can participate in the network by reading and writing to it without authorisation (Yaga et al. 2018). Bitcoin is the first example of a permissionless blockchain; however, when Nakamoto created Bitcoin, standardised terms for blockchain types were not yet in use. In the Bitcoin whitepaper, Nakamoto addresses the privacy of traditional banking systems where a trusted third party verifies transactions using information about each party to complete the transaction (Nakamoto 2008). Nakamoto proposes an alternative where the identity of a network participant identifies itself using a public key rather than identifiable information, as seen in traditional banking systems.

Permissioned

Permissioned blockchains also known as private blockchains rely on a third party to select participants or nodes in the network (Imteaj, Hadi Amini, and Pardalos 2021).(Yaga et al. 2018)

states that permissioned blockchains provide ”finer-grained” permission controls for blockchain use cases where organisations require access control, limiting network participation by authenticating a node. Furthermore, (Leible et al. 2019) outlines that permissioned blockchains extend further than a means of authentication on the network. Leible states that the categorisation of blockchain types also extends to the governance and consensus mechanisms; additionally, in permissioned blockchains, node participation is not equal. All nodes in the network are often a collection of nodes within an organisation which is in contrast to permissionless blockchains such as Bitcoin, where participation is unlimited and anonymous. Leible further outlines the categorisation of user types or participants in a blockchain network; users are defined as ”user” and ”committee user”. The users or nodes in the network as the name of the blockchain implies can perform certain restricted actions on the blockchain (Butijn, Tamburri, and Heuvel 2020) (Rajasekaran, Azees, and Al-Turjman 2022).

Consortium

Consortium blockchains are an extension of permissioned blockchains where nodes and participants are required to authenticate on the network, although consortiums allow nodes from external organisations to participate in the network (Butijn, Tamburri, and Heuvel 2020). Furthermore, a consortium blockchain facilitates distributed validation where the consortium identifies nodes to verify transactions. This is particularly useful for organisations to agree upon effective data-sharing governance upheld by the blockchain (Imteaj, Hadi Amini, and Pardalos 2021). Consortiums are further categorised by node participation if the authenticated nodes on the network do not change, this is known as a ”static consortium”, whereas if nodes change over time the consortium is known as an ”agile consortium” (Ruoti et al. 2019).

2.1.3 Blockchain Components

In this section, we will investigate the critical components that make up a blockchain. Blockchain technology leverages various computer science disciplines however, a majority of the foundational concepts rely on cryptography.

Cryptographic Hash Functions

Cryptography forms the foundation of blockchain technology and facilitates a means to define the rules of the blockchain so that transactions are tamper-proof and auditable (Narayanan et al. 2016). (Narayanan et al. 2016) defines a hash function as a mathematical function with a series of properties:

- an input can be a string of any length
- typically outputs a fixed length of 256 bits
- the output of a hashed string is ”efficiently computable”

In the context of a blockchain, a hash function must be cryptographically secure, i.e a cryptographic hash function. A cryptographic hash function has three properties ”collision resistance, hiding and puzzle friendliness” (Narayanan et al. 2016). Below is a further exploration of the aforementioned properties.

Property 1: Collision Resistance A cryptographic hash function must be collision resistant to ensure the function is secure. A cryptographic collision is one where two unique inputs produce the same output (Narayanan et al. 2016). For example, an insecure hash function may generate an identical hash where the same characters are in a different order (Nakov 2018). To prevent a collision we require a collision detection algorithm, however, the probability of discovering a collision is astronomically small when using a cryptographic hash function such as SHA-256, in this case, due to computational cost, we place our trust in the complexity of the hash function and assume that a collision is unlikely.

Property 2: Hiding The hiding property of a cryptographic hash function supposes that it is impossible to calculate the input of the hash function given the hash output (Narayanan et al. 2016). In a blockchain, we make use of a commitment scheme to achieve the hiding property. A commitment uses two algorithmic methods, one called the commitment and verification, the commitment takes an input message and a secret unique random number (nonce) and outputs a commitment hash. The commitment hash is verified by the verification method where the method receives the commitment, message and nonce and will return true if ”com = = commit(msg, nonce)” (Narayanan

et al. 2016). The hiding property is fulfilled when given the commitment it is improbable to find the message.

Property 3: Puzzle Friendliness (Narayanan et al. 2016) states A puzzle-friendly hash function is difficult to solve using a strategy, rather the puzzle is solved through brute force. To define a puzzle we use the expression "$H(id \mid\mid x) \in Y$":

- H is the hash function
- id is the id of the puzzle
- Y is a target set, i.e the difficulty of the puzzle area that is searched.

Hash Pointers and Data Structures

Digital Signatures

Transactions

Asymmetric-Key Cryptography

Addresses

Ledgers

Blocks

Chaining Blocks

2.1.4 Consensus

Proof of Work (PoW)

Proof of Stake (PoS)

Delegated Proof of Stake (DPoS)

Proof of Elapsed Time (PoET)

Practical Byzantine Fault Tolerance (PBFT)

2.1.5 Smart Contracts

2.2 Organisational Interoperability

2.3 Facilitating Interoperability using Blockchain Technology

2.4 Blockchain Technology in Banking Organisations

2.4.1 Permissioned Blockchain Networks

2.5 Blockchain Data Storage and Retrieval

Chapter 3

Research Methodology

Chapter 4

Ethical and Professional Considerations

Chapter 5

Evaluation

Chapter 6

Learning

Chapter 7

Conclusion

Bibliography

Back, Adam (2002). “Hashcash - A Denial of Service Counter-Measure”. In: p. 10.

Butijn, Bert-Jan, Damian A. Tamburri, and Willem-Jan van den Heuvel (June 17, 2020). “Blockchains: A Systematic Multivocal Literature Review”. In: *ACM Computing Surveys* 53.3, 61:1–61:37. ISSN: 0360-0300. DOI: 10.1145/3369052. URL: http://doi.org/10.1145/3369052 (visited on 07/27/2022).

Dai, Wei (1998). *Bmoney*. URL: http://www.weidai.com/bmoney.txt (visited on 08/18/2022).

Di Pierro, Massimo (2017). “What Is the Blockchain?” In: *Computing in Science & Engineering* 19.5, pp. 92–95. ISSN: 1558-366X. DOI: 10.1109/MCSE.2017.3421554.

Finney, Hal (2022). *RPOW - Reusable Proofs of Work*. URL: https://nakamotoinstitute.org/finney/rpow/index.html (visited on 08/18/2022).

Imteaj, Ahmed, M. Hadi Amini, and Panos M. Pardalos (2021). “Introduction to Blockchain Technology”. In: *Foundations of Blockchain: Theory and Applications*. Ed. by Ahmed Imteaj, M. Hadi Amini, and Panos M. Pardalos. SpringerBriefs in Computer Science. Cham: Springer International Publishing, pp. 3–13. ISBN: 978-3-030-75025-1. DOI: 10.1007/978-3-030-75025-1_1. URL: https://doi.org/10.1007/978-3-030-75025-1_1 (visited on 07/29/2022).

Leible, Stephan et al. (2019). “A Review on Blockchain Technology and Blockchain Projects Fostering Open Science”. In: *Frontiers in Blockchain* 2. ISSN: 2624-7852. URL: https://www.frontiersin.org/article/10.3389/fbloc.2019.00016 (visited on 04/12/2022).

Nakamoto, Satoshi (2008). “Bitcoin: A Peer-to-Peer Electronic Cash System”. In: p. 11.

Nakov, Svetlin (2018). "Practical Cryptography for Developers". In: *Crypto Hashes and Collisions · Practical Cryptography for Developers*. URL: https://wizardforcel.gitbooks.io/practical-cryptography-for-developers-book/content/cryptographic-hash-functions/crypto-hashes-and-collisions.html (visited on 11/09/2022).

Narayanan, Arvind et al. (July 19, 2016). *Bitcoin and Cryptocurrency Technologies: A Comprehensive Introduction*. Illustrated edition. Princeton: Princeton University Press. 336 pp. ISBN: 978-0-691-17169-2.

Rajasekaran, Arun Sekar, Maria Azees, and Fadi Al-Turjman (Aug. 1, 2022). "A Comprehensive Survey on Blockchain Technology". In: *Sustainable Energy Technologies and Assessments* 52, p. 102039. ISSN: 2213-1388. DOI: 10.1016/j.seta.2022.102039. URL: https://www.sciencedirect.com/science/article/pii/S2213138822000911 (visited on 07/29/2022).

Ruoti, Scott et al. (Dec. 20, 2019). "Blockchain Technology: What Is It Good For?" In: *Communications of the ACM* 63.1, pp. 46–53. ISSN: 0001-0782. DOI: 10.1145/3369752. URL: http://doi.org/10.1145/3369752 (visited on 07/27/2022).

Vitalik, Buterin (2014). *Ethereum Whitepaper*. ethereum.org. URL: https://ethereum.org/en/whitepaper (visited on 08/05/2022).

Yaga, Dylan et al. (Oct. 2018). *Blockchain Technology Overview*. NIST IR 8202. Gaithersburg, MD: National Institute of Standards and Technology, NIST IR 8202. DOI: 10.6028/NIST.IR.8202. URL: https://nvlpubs.nist.gov/nistpubs/ir/2018/NIST.IR.8202.pdf (visited on 08/05/2022).

Zero-Knowledge Proofs — Ethereum.Org (2022). URL: https://ethereum.org/en/zero-knowledge-proofs/ (visited on 10/11/2022).

Appendix A

Appendices