A permissioned blockchain prototype facilitating banking record interoperability

University of Essex

Anrich Potgieter

October 23, 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 available across the network (Butijn, Tamburri, and Heuvel 2020).

2.1.2 Types of Blockchains

Permissionless

Permissioned

Consortium

2.1.3 Blockchain Components

Cryptographic Hash Functions

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

Chapter 3

Ethical and Professinoal Considerations

Chapter 4

Evaluation

Chapter 5

Learning

Chapter 6

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).

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

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

Appendicies