Chapter 4
Appendable-Block Blockchains: Overview, Applications, and Challenges

Regio A. Michelin
https://orcid.org/0000-0002-6758-1466
Cybersecurity CRC, Australia & University of New South Wales, Australia

Roben Castagna Lunardi
Federal Institute of Education, Science and Technology of Rio Grande do Sul (IFRS), Brazil

Henry Cabral Nunes
Pontifical Catholic University of Rio Grande do Sul, Brazil

Volkan Dedeoglu
CSIRO, Australia

Charles V. Neu
University of Santa Cruz do Sul, Brazil

Avelino Francisco Zorzo
Pontifical Catholic University of Rio Grande do Sul, Brazil

Salil S. Kanhere
https://orcid.org/0000-0002-1835-3475
University of New South Wales, Australia

ABSTRACT

Blockchain has emerged as a technology that can change the way people and systems interact, providing mechanisms that ensure integrity and ownership of the data produced without reliance on a trusted third-party. Appendable-block blockchain is a novel instantiation that suits for solutions that require a high transaction throughput. Appendable-block blockchains focus on data produced by nodes instead of a relation (transaction) between two entities. This new kind of blockchain can improve how data are stored and managed in distributed systems. This chapter introduces the notion of appendable-block blockchain and exemplifies its applicability in multiple practical domains. Additionally, the authors provide a discussion on the security aspects of this new blockchain. Finally, the chapter presents current issues and possible future directions for appendable-block blockchains.

DOI: 10.4018/978-1-7998-5839-3.ch004

INTRODUCTION

In recent years, blockchain technology has been used in different types of applications to solve, naturally, problems related to, for example, resilience, distributed processing, integrity and non-repudiation of produced information. Furthermore, different types of blockchain have also been developed to solve those problems using novel architectures, data structures, consensus algorithms or even the possibility to execute Turing machine code. Data blocks, for example, can be organised as the traditional Bitcoin block, using a Directed-Acyclic Graph, or using an appendable-block data structure.

The appendable-block capability, for example, changes the way that transactions are combined into a block. Our proposed blockchain architecture follows the traditional block definition in terms of splitting it in two different parts: (*i*) block header: this part contains the immutable information in the block. (*ii*) block payload: where the transactions are stored. However, in our architecture, the payload arranges the transactions using a linked list structure, and it defines a set of rules that enables an entity to send transactions to the block where the entity public key is stored.

The block header contains the required information to validate transactions ownership, and uniquely identify the block. It is composed of the block owner public key, sequential number identifier in the blockchain, previous block header hash, timestamp when the block was created, access policies, and expiration time.

The block payload can only contain transactions produced from the entity that holds the private key used to sign the transactions. The validation to append a new transaction, requires that the transaction must be signed by the entity private key, and the block expiration time was not reached. The signature is validated using the public key, stored in the block header, and thus the transaction is appended at the end of the payload section. Using a similar idea from traditional blockchain, where the first block points to the genesis block, and thus the following blocks are linked together, in the appendable-block blockchain the first transaction contains the block header hash data, and the following transactions are linked with the previous transaction's hash. This data structure enables the proposed blockchain to reduce the data fragmentation, as the transactions are grouped in blocks according to the entity that produces it.

This blockchain model was designed to support constrained entities producing information. These entities are arranged in a multi-layer architecture, according to their capabilities and purpose on the solution.

The rest of this chapter will present the different architectures that can be used to organize the appendable-block blockchain; a discussion on the different types of block data structures and explain the one used in the appendable-block blockchain; how consensus algorithms and smart contracts are used; and, finally, different applications that use appendable-block blockchain are presented.

ARCHITECTURES

Initially, as presented by Bitcoin (Nakamoto, 2008), blockchain was designed to operate over a completely distributed architecture, where all nodes can (also known as full nodes) have the same role in the management and in the operation of the blockchain. However, due to the characteristics of many applications, some proposals discussed the usage of blockchain in a more controlled environment. For example, for international bank transfers, Ripple (Armknecht *et al*., 2015) proposed an architecture composed of different roles, where clients connect through servers. Clients mean light-nodes that control a key pair and request transactions. Servers can be different kinds of nodes: a proposer (who will try to insert a new