DEPARTMENT OF COMPUTER SCIENCE

FACULTY OF NATURAL SCIENCE

A TERM PAPER

ON

**BLOCKCHAIN TECHNOLOGY**

BY

MUHAMMAD ABDULHAMID KPANJE

U18/FNS/CSC/1075

STEPHEN SILAS ATABA

U18/FNS/CSC/1078

TO

MR SHEHU LIMAN

Contents

[CHAPTER 1 4](#_Toc136731694)

[OVERVIEW OF BLOCKCHAIN TECHNOLOGY, HISTORY AND METHODOLOGY 4](#_Toc136731695)

[1.0 Introduction 4](#_Toc136731696)

[1.1 Background and History 5](#_Toc136731697)

[CHAPTER 2 6](#_Toc136731698)

[BLOCKCHAIN CATEGORAZATION 6](#_Toc136731699)

[2.0 INTRODUCTION 6](#_Toc136731700)

[2.1 Permissionless 6](#_Toc136731701)

[2.2 Permissioned: 7](#_Toc136731702)

[CHAPTER 3 9](#_Toc136731703)

[BLOCKCHAIN COMPONENTS 9](#_Toc136731704)

[3.0 introduction: 9](#_Toc136731705)

[3.1 Cryptographic Hash Functions 9](#_Toc136731706)

[3.2 Transactions 10](#_Toc136731707)

[3.3 Asymmetric-Key Cryptography 12](#_Toc136731708)

[3.4 Addresses and Address Derivation 13](#_Toc136731709)

[3.5 Ledgers 13](#_Toc136731710)

[3.6 Blocks 14](#_Toc136731711)

[CHAPTER 4 15](#_Toc136731712)

[SMART CONTRACT 15](#_Toc136731713)

[4.0 INTRODUCTION: 15](#_Toc136731714)

[CHAPTER 5 16](#_Toc136731715)

[CONCLUSION AND REFERENCE 16](#_Toc136731716)

[5.0CONCLUSION 16](#_Toc136731717)

[5.1 REFERENCE: 16](#_Toc136731718)

# CHAPTER 1

# OVERVIEW OF BLOCKCHAIN TECHNOLOGY, HISTORY AND METHODOLOGY

## 1.0 Introduction

Blockchains are tamper evident and tamper resistant digital ledgers implemented in a distributed fashion (i.e., without a central repository) and usually without a central authority (i.e., a bank, company or government). At their basic level, they enable a community of users to record transactions in a shared ledger within that community, such that under normal operation of the blockchain network no transaction can be changed once published. In 2008, the blockchain idea was combined with several other technologies and computing concepts to create modern cryptocurrencies: electronic cash protected through cryptographic mechanisms instead of a central repository or authority.

This technology became widely known in 2009 with the launch of the Bitcoin network, the first of many modern cryptocurrencies. In Bitcoin, and similar systems, the transfer of digital information that represents electronic cash takes place in a distributed system. Bitcoin users can digitally sign and transfer their rights to that information to another user and the Bitcoin blockchain records this transfer publicly, allowing all participants of the network to independently verify the validity of the transactions.

The Bitcoin blockchain is independently maintained and managed by a distributed group of participants. This, along with cryptographic mechanisms, makes the blockchain resilient to attempts to alter the ledger later (modifying blocks or forging transactions). Blockchain technology has enabled the development of many cryptocurrency systems such as Bitcoin and Ethereum1 . Because of this, blockchain technology is often viewed as bound to Bitcoin or possibly cryptocurrency solutions in general. However, the technology is available for a broader variety of applications and is being investigated for a variety of sectors

The numerous components of blockchain technology along with its reliance on cryptographic primitives and distributed systems can make it challenging to understand. However, each component can be described simply and used as a building block to understand the larger complex system. Blockchains can be informally defined as:

Blockchains are distributed digital ledgers of cryptographically signed transactions that are grouped into blocks. Each block is cryptographically linked to the previous one (making it tamper evident) after validation and undergoing a consensus decision. As new blocks are added, older blocks become more difficult to modify (creating tamper resistance). New blocks are replicated across copies of the ledger within the network, and any conflicts are resolved automatically using established rules.

## 1.1 Background and History

The core ideas behind blockchain technology emerged in the late 1980s and early 1990s. In 1989, Leslie Lamport developed the Paxos protocol, and in 1990 submitted the paper The PartTime Parliament [2] to ACM Transactions on Computer Systems; the paper was finally published in a 1998 issue. The paper describes a consensus model for reaching agreement on a result in a network of computers where the computers or network itself may be unreliable. In 1991, a signed chain of information was used as an electronic ledger for digitally signing documents in a way that could easily show none of the signed documents in the collection had been changed [3]. These concepts were combined and applied to electronic cash in 2008 and described in the paper, Bitcoin: A Peer to Peer Electronic Cash System [4], which was published pseudonymously by Satoshi Nakamoto, and then later in 2009 with the establishment of the Bitcoin cryptocurrency blockchain network. Nakamoto’s paper contained the blueprint that most modern cryptocurrency schemes follow (although with variations and modifications). Bitcoin was just the first of many blockchain applications.

Many electronic cash schemes existed prior to Bitcoin (e.g., ecash and NetCash), but none of them achieved widespread use. The use of a blockchain enabled Bitcoin to be implemented in a distributed fashion such that no single user controlled the electronic cash and no single point of failure existed; this promoted its use. Its primary benefit was to enable direct transactions between users without the need for a trusted third party. It also enabled the issuance of new cryptocurrency in a defined manner to those users who manage to publish new blocks and maintain copies of the ledger; such users are called miners in Bitcoin. The automated payment of the miners enabled distributed administration of the system without the need to organize. By using a blockchain and consensus-based maintenance, a self-policing mechanism was created that ensured that only valid transactions and blocks were added to the blockchain

Many electronic cash schemes existed prior to Bitcoin (e.g., ecash and NetCash), but none of them achieved widespread use. The use of a blockchain enabled Bitcoin to be implemented in a distributed fashion such that no single user controlled the electronic cash and no single point of failure existed; this promoted its use. Its primary benefit was to enable direct transactions between users without the need for a trusted third party. It also enabled the issuance of new cryptocurrency in a defined manner to those users who manage to publish new blocks and maintain copies of the ledger; such users are called miners in Bitcoin. The automated payment of the miners enabled distributed administration of the system without the need to organize. By using a blockchain and consensus-based maintenance, a self-policing mechanism was created that ensured that only valid transactions and blocks were added to the blockchain

Since Bitcoin was pseudonymous, it was essential to have mechanisms to create trust in an environment where users could not be easily identified. Prior to the use of blockchain technology, this trust was typically delivered through intermediaries trusted by both parties. Without trusted intermediaries, the needed trust within a blockchain network is enabled by four key characteristics of blockchain technology, described below:

• Ledger – the technology uses an append only ledger to provide full transactional history. Unlike traditional databases, transactions and values in a blockchain are not overridden.

• Secure – blockchains are cryptographically secure, ensuring that the data contained within the ledger has not been tampered with, and that the data within the ledger is attestable.

• Shared – the ledger is shared amongst multiple participants. This provides transparency across the node participants in the blockchain network.

• Distributed – the blockchain can be distributed. This allows for scaling the number of nodes of a blockchain network to make it more resilient to attacks by bad actors. By increasing the number of nodes, the ability for a bad actor to impact the consensus protocol used by the blockchain is reduced.

# CHAPTER 2

# BLOCKCHAIN CATEGORAZATION

## 2.0 INTRODUCTION

Blockchain networks can be categorized based on their permission model, which determines who can maintain them (e.g., publish blocks). If anyone can publish a new block, it is permissionless. If only particular users can publish blocks, it is permissioned. In simple terms, a permissioned blockchain network is like a corporate intranet that is controlled, while a permissionless blockchain network is like the public internet, where anyone can participate. Permissioned blockchain networks are often deployed for a group of organizations and individuals, typically referred to as a consortium. This distinction is necessary to understand as it impacts some of the blockchain components discussed later in this document.

## 2.1 Permissionless

Permissionless blockchain networks are decentralized ledger platforms open to anyone publishing blocks, without needing permission from any authority. Permissionless blockchain platforms are often open source software, freely available to anyone who wishes to download them. Since anyone has the right to publish blocks, this results in the property that anyone can read the blockchain as well as issue transactions on the blockchain (through including those transactions within published blocks). Any blockchain network user within a permissionless blockchain network can read and write to the ledger. Since permissionless blockchain networks are open to all to participate, malicious users may attempt to publish blocks in a way that subverts the system (discussed in detail later). To prevent this, permissionless blockchain networks often utilize a multiparty agreement or ‘consensus’ system (see Section 4) that requires users to expend or maintain resources when attempting to publish blocks. This prevents malicious users from easily subverting the system. Examples of such consensus models include proof of work (see Section 4.1) and proof of stake (see Section 4.2) methods. The consensus systems in permissionless blockchain networks usually promote non-malicious behavior through rewarding the publishers of protocol-conforming blocks with a native cryptocurrency.

## 2.2 Permissioned:

Permissioned blockchain networks are ones where users publishing blocks must be authorized by some authority (be it centralized or decentralized). Since only authorized users are maintaining the blockchain, it is possible to restrict read access and to restrict who can issue transactions. Permissioned blockchain networks may thus allow anyone to read the blockchain or they may restrict read access to authorized individuals. They also may allow anyone to submit transactions to be included in the blockchain or, again, they may restrict this access only to authorized individuals. Permissioned blockchain networks may be instantiated and maintained using open source or closed source software.

Permissioned blockchain networks can have the same traceability of digital assets as they pass through the blockchain, as well as the same distributed, resilient, and redundant data storage system as a permissionless blockchain networks. They also use consensus models for publishing blocks, but these methods often do not require the expense or maintenance of resources (as is the case with current permissionless blockchain networks). This is because the establishment of one’s identity is required to participate as a member of the permissioned blockchain network; those maintaining the blockchain have a level of trust with each other, since they were all

NISTIR 8202 BLOCKCHAIN TECHNOLOGY OVERVIEW

6

This publication is available free of charge from: https://doi.org/10.6028/NIST.IR.8202

authorized to publish blocks and since their authorization can be revoked if they misbehave. Consensus models in permissioned blockchain networks are then usually faster and less computationally expensive.

Permissioned blockchain networks may also be used by organizations that need to more tightly control and protect their blockchain. However, if a single entity controls who can publish blocks, the users of the blockchain will need to have trust in that entity. Permissioned blockchain networks may also be used by organizations that wish to work together but may not fully trust one another. They can establish a permissioned blockchain network and invite business partners to record their transactions on a shared distributed ledger. These organizations can determine the consensus model to be used, based on how much they trust one another. Beyond trust, permissioned blockchain networks provide transparency and insight that may help better inform business decisions and hold misbehaving parties accountable. This can explicitly include auditing and oversight entities making audits a constant occurrence versus a periodic event.

Some permissioned blockchain networks support the ability to selectively reveal transaction information based on a blockchain network users identity or credentials. With this feature, some degree of privacy in transactions may be obtained. For example, it could be that the blockchain records that a transaction between two blockchain network users took place, but the actual contents of transactions is only accessible to the involved parties.

Some permissioned blockchain networks require all users to be authorized to send and receive transactions (they are not anonymous, or even pseudo-anonymous). In such systems parties work together to achieve a shared business process with natural disincentives to commit fraud or otherwise behave as a bad actor (since they can be identified). If bad behavior were to occur, it is well known where the organizations are incorporated, what legal remedies are available and how to pursue those remedies in the relevant judicial system

# CHAPTER 3

# BLOCKCHAIN COMPONENTS

## 3.0 introduction:

Blockchain technology can seem complex; however, it can be simplified by examining each component individually. At a high level, blockchain technology utilizes well-known computer science mechanisms and cryptographic primitives (cryptographic hash functions, digital signatures, asymmetric-key cryptography) mixed with record keeping concepts (such as append only ledgers). This section discusses each individual main component: cryptographic hash functions, transactions, asymmetric-key cryptography, addresses, ledgers, blocks, and how blocks are chained together.

## 3.1 Cryptographic Hash Functions

An important component of blockchain technology is the use of cryptographic hash functions for many operations. Hashing is a method of applying a cryptographic hash function to data, which calculates a relatively unique output (called a message digest, or just digest) for an input of nearly any size (e.g., a file, text, or image). It allows individuals to independently take input data, hash that data, and derive the same result – proving that there was no change in the data. Even the smallest change to the input (e.g., changing a single bit) will result in a completely different output digest. Table 1 shows simple examples of this.

Cryptographic hash functions have these important security properties:

1. They are preimage resistant. This means that they are one-way; it is computationally infeasible to compute the correct input value given some output value (e.g., given a digest, find x such that hash(x) = digest).

2. They are second preimage resistant. This means one cannot find an input that hashes to a specific output. More specifically, cryptographic hash functions are designed so that given a specific input, it is computationally infeasible to find a second input which produces the same output (e.g., given x, find y such that hash(x) = hash(y)). The only approach available is to exhaustively search the input space, but this is computationally infeasible to do with any chance of success.

3. They are collision resistant. This means that one cannot find two inputs that hash to the same output. More specifically, it is computationally infeasible to find any two inputs that produce the same digest (e.g., find an x and y which hash(x) = hash(y)).

A specific cryptographic hash function used in many blockchain implementations is the Secure Hash Algorithm (SHA) with an output size of 256 bits (SHA-256). Many computers support this algorithm in hardware, making it fast to compute. SHA-256 has an output of 32 bytes (1 byte = 8 bits, 32 bytes = 256 bits), generally displayed as a 64-character hexadecimal string (see Table 1 below).

This means that there are 2256 ≈ 1077, or 115,792,089,237,316,195,423,570,985,008,687,907,853,269,984,665,640,564,039,457,584,007,913,129,639,936 possible digest values. The algorithm for SHA-256, as well as others, is specified in Federal Information Processing Standard (FIPS) 180-4 [5]. The NIST Secure Hashing website [6] contains FIPS specifications for all NIST-approved hashing algorithms.

## 3.2 Transactions

A *transaction* represents an interaction between parties. With cryptocurrencies, for example, a transaction represents a transfer of the cryptocurrency between blockchain network users. For business-to-business scenarios, a transaction could be a way of recording activities occurring on digital or physical assets. Figure 1 shows a notional example of a cryptocurrency transaction. Each block in a blockchain can contain zero or more transactions. For some blockchain implementations, a constant supply of new blocks (even with zero transactions) is critical to maintain the security of the blockchain network; by having a constant supply of new blocks being published, it prevents malicious users from ever “catching up” and manufacturing a longer, altered blockchain (see Section 4.7).

The data which comprises a transaction can be different for every blockchain implementation, however the mechanism for transacting is largely the same. A blockchain network user sends information to the blockchain network. The information sent may include the sender’s address (or another relevant identifier), sender’s public key, a digital signature, transaction inputs and transaction outputs

A single cryptocurrency transaction typically requires at least the following information, but can contain more:

• **Inputs** – The inputs are usually a list of the digital assets to be transferred. A transaction will reference the source of the digital asset (providing provenance) – either the previous transaction where it was given to the sender, or for the case of new digital assets, the origin event. Since the input to the transaction is a reference to past events, the digital assets do not change. In the case of cryptocurrencies this means that value cannot be added or removed from existing digital assets. Instead, a single digital asset can be split into multiple new digital assets (each with lesser value) or multiple digital assets can be combined to form fewer new digital assets (with a correspondingly greater value). The splitting or joining of assets will be specified within the transaction output.

The sender must also provide proof that they have access to the referenced inputs, generally by digitally signing the transaction – proving access to the private key.

• **Outputs** – The outputs are usually the accounts that will be the recipients of the digital assets along with how much digital asset they will receive. Each output specifies the number of digital assets to be transferred to the new owner(s), the identifier of the new owner(s), and a set of conditions the new owners must meet to spend that value. If the digital assets provided are more than required, the extra funds must be explicitly sent back to the sender (this is a mechanism to “make change”).

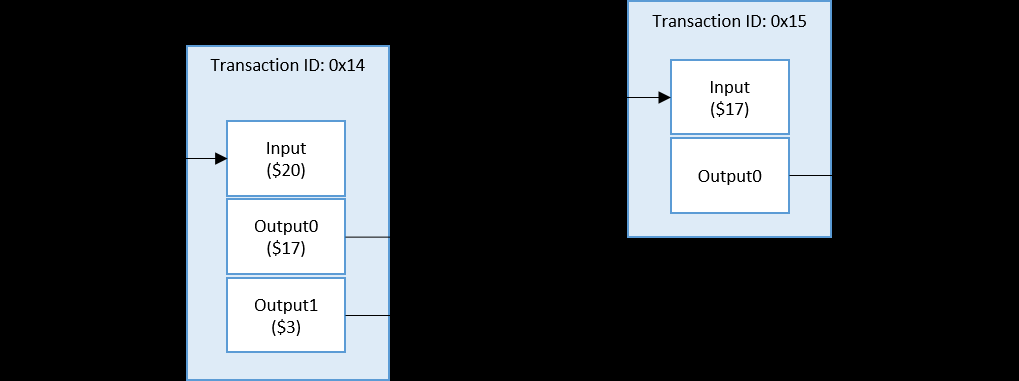


Figure 3.1 - Example Cryptocurrency Transaction

## 3.3 Asymmetric-Key Cryptography

Blockchain technology uses asymmetric-key cryptography4 (also referred to as public key cryptography). Asymmetric-key cryptography uses a pair of keys: a public key and a private key that are mathematically related to each other. The public key is made public without reducing the security of the process, but the private key must remain secret if the data is to retain its cryptographic protection. Even though there is a relationship between the two keys, the private key cannot efficiently be determined based on knowledge of the public key. One can encrypt with a private key and then decrypt with the public key. Alternately, one can encrypt with a public key and then decrypt with a private key.

Asymmetric-key cryptography enables a trust relationship between users who do not know or trust one another, by providing a mechanism to verify the integrity and authenticity of transactions while at the same time allowing transactions to remain public. To do this, the transactions are ‘digitally signed’. This means that a private key is used to encrypt a transaction such that anyone with the public key can decrypt it. Since the public key is freely available, encrypting the transaction with the private key proves that the signer of the transaction has access to the private key. Alternately, one can encrypt data with a user’s public key such that only users with access to the private key can decrypt it. A drawback is that asymmetric-key cryptography is often slow to compute.

## 3.4 Addresses and Address Derivation

Some blockchain networks make use of an *address*, which is a short, alphanumeric string of characters derived from the blockchain network user’s public key using a cryptographic hash function, along with some additional data (e.g., version number, checksums). Most blockchain implementations make use of addresses as the “to” and “from” endpoints in a transaction. Addresses are shorter than the public keys and are not secret. One method to generate an address is to create a public key, applying a cryptographic hash function to it, and converting the hash to text:

public key cryptographic hash function address

Each blockchain implementation may implement a different method to derive an address. For permissionless blockchain networks, which allow anonymous account creation, a blockchain network user can generate as many asymmetric-key pairs, and therefore addresses as desired, allowing for a varying degree of pseudo-anonymity. Addresses may act as the public-facing identifier in a blockchain network for a user, and oftentimes an address will be converted into a QR code (Quick Response Code, a 2-dimensional bar code which can contain arbitrary data) for easier use with mobile devices.



## 3.5 Ledgers

A *ledger* is a collection of transactions. Throughout history, pen and paper ledgers have been used to keep track of the exchange of goods and services. In modern times, ledgers have been stored digitally, often in large databases owned and operated by a centralized trusted third party (i.e., the owner of the ledger) on behalf of a community of users. These ledgers with centralized ownership can be implemented in a centralized or distributed fashion (i.e., just one server or a coordinating cluster of servers).

There is growing interest in exploring having distributed ownership of the ledger. Blockchain technology enables such an approach using both distributed ownership as well as a distributed physical architecture. The distributed physical architecture of blockchain networks often involve a much larger set of computers than is typical for centrally managed distributed physical architecture. The growing interest in distributed ownership of ledgers is due to possible trust, security, and reliability concerns related to ledgers with centralized ownership:

## 3.6 Blocks

Blockchain network users submit candidate transactions to the blockchain network via software (desktop applications, smartphone applications, digital wallets, web services, etc.). The software sends these transactions to a node or nodes within the blockchain network. The chosen nodes may be non-publishing full nodes as well as publishing nodes. The submitted transactions are then propagated to the other nodes in the network, but this by itself does not place the transaction in the blockchain. For many blockchain implementations, once a pending transaction has been distributed to nodes, it must then wait in a queue until it is added to the blockchain by a publishing node.

Transactions are added to the blockchain when a publishing node publishes a block. A *block* contains a block header and block data. The block header contains metadata for this block. The block data contains a list of validated and authentic transactions which have been submitted to the blockchain network. Validity and authenticity is ensured by checking that the transaction is correctly formatted and that the providers of digital assets in each transaction (listed in the transaction’s ‘input’ values) have each cryptographically signed the transaction. This verifies that the providers of digital assets for a transaction had access to the private key which could sign over the available digital assets. The other full nodes will check the validity and authenticity of all transactions in a published block and will not accept a block if it contains invalid transactions.

# CHAPTER 4

# SMART CONTRACT

## 4.0 INTRODUCTION:

The term smart contract dates to 1994, defined by Nick Szabo as “a computerized transaction protocol that executes the terms of a contract. The general objectives of smart contract design are to satisfy common contractual conditions (such as payment terms, liens, confidentiality, and even enforcement), minimize exceptions both malicious and accidental, and minimize the need for trusted intermediaries.” [17]. Smart contracts extend and leverage blockchain technology. A smart contract is a collection of code and data (sometimes referred to as functions and state) that is deployed using cryptographically signed transactions on the blockchain network (e.g., Ethereum’s smart contracts, Hyperledger Fabric’s chaincode). The smart contract is executed by nodes within the blockchain network; all nodes that execute the smart contract must derive the same results from the execution, and the results of execution are recorded on the blockchain. Blockchain network users can create transactions which send data to public functions offered by a smart contract. The smart contract executes the appropriate method with the user provided data to perform a service. The code, being on the blockchain, is also tamper evident and tamper resistant and therefore can be used (among other purposes) as a trusted third party. A smart contract can perform calculations, store information, expose properties to reflect a publicly exposed state and, if appropriate, automatically send funds to other accounts. It does not necessarily even have to perform a financial function. For example, the authors of this document have created an Ethereum smart contract that publicly generate trustworthy random numbers [18]. It is important to note that not every blockchain can run smart contracts. The smart contract code can represent a multi-party transaction, typically in the context of a business process. In a multi-party scenario, the benefit is that this can provide attestable data and transparency that can foster trust, provide insight that can enable better business decisions, reduce costs from reconciliation that exists in traditional business to business applications, and reduce the time to complete a transaction.

# CHAPTER 5

# CONCLUSION AND REFERENCE

5.0CONCLUSION:

There is a tendency to overhype and overuse most nascent technology. Many projects will attempt to incorporate the technology, even if it is unnecessary. This stems from the technology being relatively new and not well understood, the technology being surrounded by misconceptions, and the fear of missing out. Blockchain technology has not been immune. This section highlights some of the limitations and misconceptions of blockchain technology.

## 5.1 REFERENCE:

[1] Clarke, A.C., “Hazards of Prophecy: The Failure of Imagination,” from Profiles of the Future: An Inquiry into the Limits of the Possible, 1962.

[2] Lamport, Leslie. “The Part-Time Parliament.” ACM Transactions on Computer Systems, vol. 16, no. 2, Jan. 1998, pp. 133–169., <https://dl.acm.org/citation.cfm?doid=279227.279229>.

[3] Narayanan, A., Bonneau, J., Felten, E., Miller, A., and Goldfede, S., Bitcoin and Cryptocurrency Technologies: A Comprehensive Introduction, Princeton University Press, 2016.

[4] Nakamoto, S., “Bitcoin: A Peer-to-Peer Electronic Cash System,” 2008. https://bitcoin.org/bitcoin.pdf [5] National Institute of Standards and Technology, Secure Hash Standard (SHS), Federal Information Processing Standards (FIPS) Publication 180-4, August 2015. <https://doi.org/10.6028/NIST.FIPS.180-4>

[6] National Institute of Standards and Technology (NIST), Secure Hashing website, <https://csrc.nist.gov/projects/hash-functions>

[7] “Hash per Second.” Bitcoin Wiki, <http://en.bitcoin.it/wiki/Hash_per_second>.

[8] National Institute of Standards and Technology, SHA-3 Standard: PermutationBased Hash and Extendable-Output Functions, Federal Information Processing Standards (FIPS) Publication 202, August 2015. <https://doi.org/10.6028/NIST.FIPS.202>

[9] National Institute of Standards and Technology (NIST), Digital Signature Standard, Federal Information Processing Standards (FIPS) Publication 186-4, July 2013. <https://doi.org/10.6028/NIST.FIPS.186-4>

[10] “LDAP.com.” LDAP.com, <https://www.ldap.com>.