Πανεπιστημιο Πελοποννησου

Σχολη Μηχανικων

Τμημα Ηλεκτρολογων Μηχανικων και Μηχανικων Υπολογιστων

ΔΙΠΛΩΜΑΤΙΚΗ ΕΡΓΑΣΙΑ

¨Η ΑΣΦΑΛΕΙΑ ΤΩΝ ΥΠΟΛΟΓΙΣΤΩΝ (CYBERSECURITY) ΜΕ ΤΗΝ ΤΕΧΝΟΛΟΓΙΑ BLOCKCHAIN ΣΕ ΕΦΑΡΜΟΓΕΣ ΤΟΥ ΜΕΛΛΟΝΤΟΣ¨

ΑΝΔΡΟΥΤΣΟΠΟΥΛΟΥ ΠΑΝΑΓΙΩΤΑ

ΕΠΙΒΛΕΠΩΝ: ΔΡΟΣΟΠΟΥΛΟΣ ΑΝΑΣΤΑΣΙΟΣ

ΠΑΤΡΑ, 2023

Πίνακας περιεχομένων

Πρόλογος

Το Blockchain, το θεμέλιο του Bitcoin, έχει λάβει εκτεταμένη προσοχή πρόσφατα. Το Blockchain χρησιμεύει ως ένα αμετάβλητο βιβλίο που επιτρέπει τις συναλλαγές να πραγματοποιούνται με decentralized τρόπο. Εμφανίζονται εφαρμογές που βασίζονται σε blockchain, που καλύπτουν πολυάριθμους τομείς συμπεριλαμβανομένων των χρηματοπιστωτικών υπηρεσιών, του συστήματος φήμης και του Internet of Things (IoT) κ.ο.κ. Ωστόσο, υπάρχουν ακόμα πολλές προκλήσεις της τεχνολογίας blockchain, όπως η επεκτασιμότητα και τα προβλήματα ασφάλειας που περιμένουν να ξεπεραστούν. Αυτή η εργασία παρουσιάζει μια ολοκληρωμένη επισκόπηση της τεχνολογίας blockchain. Παρέχουμε πρώτα μια επισκόπηση της αρχιτεκτονικής blockchain και συγκρίνουμε μερικούς τυπικούς συναινετικούς αλγόριθμους που χρησιμοποιούνται σε διαφορετικά blockchains. Επιπλέον, παρατίθενται εν συντομία τεχνικές προκλήσεις και πρόσφατες εξελίξεις. Διατυπώνουμε επίσης πιθανές μελλοντικές τάσεις για το blockchain.

Περίληψη

Το Bitcoin έχει προταθεί ως ασφαλές καταφύγιο για τα παραδοσιακά περιουσιακά στοιχεία για πολλούς λόγους, συμπεριλαμβανομένης της ανεξαρτησίας από τη νομισματική πολιτική, ενός ρόλου ως αποθέματος αξίας και περιορισμένης συσχέτισης με τα παραδοσιακά περιουσιακά στοιχεία. Ενώ πολλά από αυτά τα επιχειρήματα είναι επιτακτικά, οι εμπειρικές δοκιμές των ιδιοτήτων ασφαλούς καταφυγίου του Bitcoin στερούνται κεντρικής συνιστώσας, μιας σοβαρής κρίσης των χρηματοπιστωτικών αγορών[1]. Σε αυτό το έγγραφο, παρέχουμε μια πρώτη εκτίμηση των ιδιοτήτων ασφαλούς καταφυγίου του Bitcoin κατά τη διάρκεια μιας περιόδου σημαντικής αναταραχής στις χρηματοπιστωτικές αγορές, στην εποχή του Covid-19.

Το δίκτυο Bitcoin διατηρεί ένα κατανεμημένο δημόσιο βιβλίο που καταγράφει την ιδιοκτησία όλου του bitcoin, το εγγενές ψηφιακό διακριτικό περιουσιακών στοιχείων του δικτύου. Οι νέες συναλλαγές ομαδοποιούνται σε "μπλοκ" και προστίθενται διαδοχικά στη συνεχιζόμενη αλυσίδα μπλοκ του δικτύου - εξ ου και ο όρος "blockchain". Το blockchain Bitcoin περιέχει κάθε μπλοκ από την αρχή, εκτεινόμενο μέχρι το πρώτο μπλοκ γνωστό ως " Genesis Block "[2].

Πανομοιότυπα αντίγραφα του blockchain φιλοξενούνται σε υπολογιστές σε όλο τον κόσμο που τρέχουν το λογισμικό Bitcoin. Αυτοί οι υπολογιστές ονομάζονται " κόμβοι ". Αυτός ο σχεδιασμός διασφαλίζει ότι καμία μεμονωμένη οντότητα δεν ελέγχει το blockchain ή το πρωτόκολλο που το διέπει. Η κατανεμημένη φύση του Bitcoin το καθιστά decentralizedκαι ανθεκτικό στο να ελέγχεται (ή να κλείνει) από οποιαδήποτε κυβέρνηση ή κεντρική αρχή. Θεωρητικά, όλοι οι κόμβοι που διατηρούν ένα πλήρες αντίγραφο του blockchain - γνωστό ως "πλήρεις κόμβοι" - θα πρέπει να καταστραφούν για να διαγραφεί το blockchain Bitcoin[2].

Οι κόμβοι που είναι γνωστοί ως "ανθρακωρύχοι" εξυπηρετούν τον σκοπό της επικύρωσης των συναλλαγών Bitcoin και της ασφάλειας του βιβλίου blockchain. Στο παραδοσιακό τραπεζικό σύστημα, όταν στέλνετε χρήματα από τον τραπεζικό σας λογαριασμό σε άλλον τραπεζικό λογαριασμό, οι τράπεζες λειτουργούν ως έμπιστοι μεσάζοντες, αφαιρώντας κεφάλαια από έναν λογαριασμό και προσθέτοντάς τους σε έναν άλλο[3]. Με το Bitcoin, οι κεντρικοί μεσάζοντες αντικαθίστανται από ένα αξιόπιστο δίκτυο ανθρακωρύχων.

Οι ανθρακωρύχοι ανταγωνίζονται για την επίλυση ενός παζλ απόδειξης εργασίας, με ένταση υπολογισμού. Ο "νικητής" ανθρακωρύχος ανταμείβεται με έναν ορισμένο αριθμό bitcoin (συν αμοιβές συναλλαγών δικτύου) που ονομάζεται "ανταμοιβή μπλοκ". Ένας ανθρακωρύχος κερδίζει την ανταμοιβή μπλοκ περίπου κάθε 10 λεπτά, ανεξάρτητα από την ποσότητα επεξεργαστικής ισχύος που φέρνουν συλλογικά οι ανθρακωρύχοι στο δίκτυο. Περισσότερη επεξεργαστική ισχύς αυξάνει μόνο τις πιθανότητες νίκης ενός ανθρακωρύχου, δεν επιταχύνει τον ανταγωνισμό. Οι ανθρακωρύχοι δεν μπορούν να επιταχύνουν ή αλλιώς να αλλάξουν το ντετερμινιστικό πρόγραμμα εφοδιασμού του Bitcoin.

Το παζλ απαιτεί από έναν ανθρακωρύχο να δημιουργήσει ένα νέο μπλοκ λαμβάνοντας όλες τις νέες και ανεπιβεβαίωτες συναλλαγές του δικτύου, καθώς και πληροφορίες από το προηγούμενο μπλοκ (δηλαδή, την «κεφαλίδα μπλοκ» του), και τις «κατακερματίζει» χρησιμοποιώντας τον αλγόριθμο SHA-256. Το Hashing είναι μια διαδικασία κατά την οποία μια συγκεκριμένη είσοδος (στην περίπτωση αυτή, πρόσφατα δεδομένα συναλλαγών και η κεφαλίδα μπλοκ) εισάγεται σε έναν αλγόριθμο για τη δημιουργία μιας συγκεκριμένης εξόδου[3]. Ένας ανθρακωρύχος πρέπει να λάβει αυτήν την είσοδο και να μαντέψει έναν αριθμό που ονομάζεται "nonce" που όταν εισαχθεί μαζί στο SHA-256, θα παράγει μια έξοδο που ικανοποιεί το όριο εξόδου που ορίζεται από το πρωτόκολλο Bitcoin. Η εξόρυξη καταλήγει στο να μαντέψουμε τις ασυνείδητες το συντομότερο δυνατό. Εάν ένας ανθρακωρύχος χτυπήσει το καθορισμένο όριο εξόδου, θα μεταδώσει το νέο του μπλοκ (το οποίο περιλαμβάνει το nonce της) σε άλλους ανθρακωρύχους του δικτύου, έτσι ώστε να μπορούν να το κατακερματίσουν οι ίδιοι και να επαληθεύσουν τη λύση του. Εάν η πλειοψηφία των ανθρακωρύχων - 51% ή περισσότερο - καταλήξουν σε συναίνεση για τη λύση της, θα της επιτραπεί να προσθέσει το νέο της μπλοκ στο blockchain και να λάβει την ανταμοιβή μπλοκ[4].

Όλα τα παραπάνω στοιχεία, θα αναλυθούν καλύτερα στις επόμενες ενότητες που ακολουθούν, με την πρώτη ενότητα να αναφέρεται στην αρχιτεκτονική του Blockchain,

στο δεύτερο κεφάλαιο μελετάται η χρήση του blockchain με IoT. Στην συνέχεια, αναφέρονται οι αλγόριθμοι συναίνεσης και συγκριτική μελέτη μεταξύ αυτών. Στην συνέχεια, μελετώνται οι διαφόρου τύπων επιθέσεις που συμβαίνουν στο δίκτυο του blockchain. Τέλος, γίνονται μελλοντικές επεκτάσεις για βελτιώσεις της ασφάλεια και κατευθύνσεις για την βελτίωση του δικτύου ενός blockchain.

Abstract

Bitcoin has been proposed as a safe haven for traditional assets for a number of reasons, including independence from monetary policy, a role as a store of value and limited correlation with traditional assets. While many of these arguments are compelling, empirical testing of Bitcoin's safe haven properties lacks a central component, a severe financial market crisis. In this paper, we provide a first assessment of Bitcoin's safe haven properties during a period of significant financial market turmoil in the Covid-19 era.

The Bitcoin network maintains a distributed public book that records ownership of all bitcoin, the network's inherent digital asset. New transactions are grouped into "blocks" and are added sequentially to the network's ongoing blockchain - hence the term "blockchain". The Bitcoin blockchain contains each block from the beginning, extending to the first block known as the "Genesis Block".

Identical copies of the blockchain are hosted on computers around the world that run Bitcoin software. These computers are called "nodes". This design ensures that no single entity controls the blockchain or protocol that governs it. The distributed nature of Bitcoin makes it decentralized and resilient to being controlled (or shut down) by any government or central authority. Theoretically, all nodes that maintain a complete copy of the blockchain - known as "complete nodes" - would have to be destroyed to delete the Bitcoin blockchain.

The nodes known as "miners" serve the purpose of validating Bitcoin transactions and blockchain book security. In the traditional banking system, when you transfer money from one bank account to another, banks act as trusted intermediaries,

withdrawing funds from one account and adding them to another. With Bitcoin, central intermediaries are being replaced by a trusted network of miners.

Miners compete to solve a work-proof puzzle with computational intensity. The "winning" miner is rewarded with a certain number of bitcoin (plus network trading fees) called "block rewards". A miner earns the block reward about every 10 minutes, regardless of the amount of processing power the miners collectively bring to the grid. More processing power only increases a miner's chances of winning; it does not speed up competition. Miners cannot speed up or otherwise change Bitcoin's deterministic supply program.

The puzzle requires a miner to create a new block by taking all the new and unconfirmed network transactions, as well as information from the previous block (i.e., its "block header"), and "fragmenting" them using the SHA-256 algorithm. Hashing is a process in which a specific input (in this case, recent trading data and the block header) is entered into an algorithm to generate a specific output. A miner must take this input and guess a number called "nonce" which when inserted together into SHA-256, will produce an output that meets the output limit set by the Bitcoin protocol. Mining ends up guessing the unconscious as soon as possible. If a miner hits the specified exit limit, he will pass on his new block (which includes its nonce) to other miners in the network, so that they can fragment it themselves and verify its solution. If a majority of miners - 51% or more - reach a consensus on a solution, they will be allowed to add their new blockchain to the blockchain and receive the blockchain reward.

All the above elements will be better analyzed in the following sections, with the first section referring to the Blockchain architecture, in the second chapter the use of the blockchain with IoT is studied. Next, the consent algorithms and a comparative study between them are reported. Next, the different types of attacks that occur in the blockchain network are studied. Finally, there are future extensions for security improvements and directions for improving a blockchain network.

1.Εισαγωγή στην τεχνολογία Blockchain

Σήμερα η *κρυπτογράφηση (encryption)* έχει γίνει λέξη-κλειδί τόσο στη βιομηχανία όσο και στον ακαδημαϊκό χώρο. Ως ένα από τα πιο επιτυχημένα νομίσματα κρυπτογράφησης, το Bitcoin σημείωσε τεράστια επιτυχία με την κεφαλαιαγορά της να φτάνει τα 10 δισεκατομμύρια δολάρια το 2016. Με μια ειδικά σχεδιασμένη δομή αποθήκευσης δεδομένων, οι συναλλαγές στο δίκτυο Bitcoin θα μπορούσαν να πραγματοποιηθούν χωρίς τρίτους και η βασική τεχνολογία για την κατασκευή Bitcoin είναι το *blockchain*, το οποίο προτάθηκε για πρώτη φορά το 2008 και εφαρμόστηκε το 2009 [4]. Το Blockchain θα μπορούσε να θεωρηθεί δημόσιο καθολικό (publicledger) και όλες οι δεσμευμένες συναλλαγές αποθηκεύονται σε μια λίστα μπλοκ (block-list). Αυτή η αλυσίδα αναπτύσσεται καθώς προσαρμόζονται συνεχώς νέα μπλοκ. Ασυμμετρική κρυπτογραφία και αλγόριθμοι κατανεμημένης συναίνεσης (distributedconsensusalgorithms) έχουν εφαρμοστεί για την ασφάλεια των χρηστών και τη συνοχή των καθολικών. Η τεχνολογία blockchain έχει γενικά βασικά χαρακτηριστικά της αποκέντρωσης, της επιμονής, της ανωνυμίας και της δυνατότητας ελέγχου. Με αυτά τα χαρακτηριστικά, το blockchain μπορεί να εξοικονομήσει σημαντικά το κόστος και να βελτιώσει την αποδοτικότητα.

Δεδομένου ότι επιτρέπει την ολοκλήρωση της πληρωμής χωρίς τράπεζα ή μεσάζοντα, το blockchain μπορεί να χρησιμοποιηθεί σε διάφορες χρηματοοικονομικές υπηρεσίες, όπως ψηφιακά περιουσιακά στοιχεία, εμβάσματα και ηλεκτρονικές πληρωμές. Επιπλέον, μπορεί επίσης να εφαρμοστεί σε άλλους τομείς, όπως έξυπνες συμβάσεις, δημόσιες υπηρεσίες, Internet of Things (IoT), συστήματα φήμης (reputationsystems) και υπηρεσίες ασφαλείας [5]. Αυτά τα πεδία προτιμούν το blockchain με πολλούς τρόπους. Πρώτα απ 'όλα, το blockchain είναι αμετάβλητο. Η συναλλαγή δεν μπορεί να παραβιαστεί όταν συσκευαστεί στο blockchain. Οι επιχειρήσεις που απαιτούν υψηλή αξιοπιστία και ειλικρίνεια μπορούν να

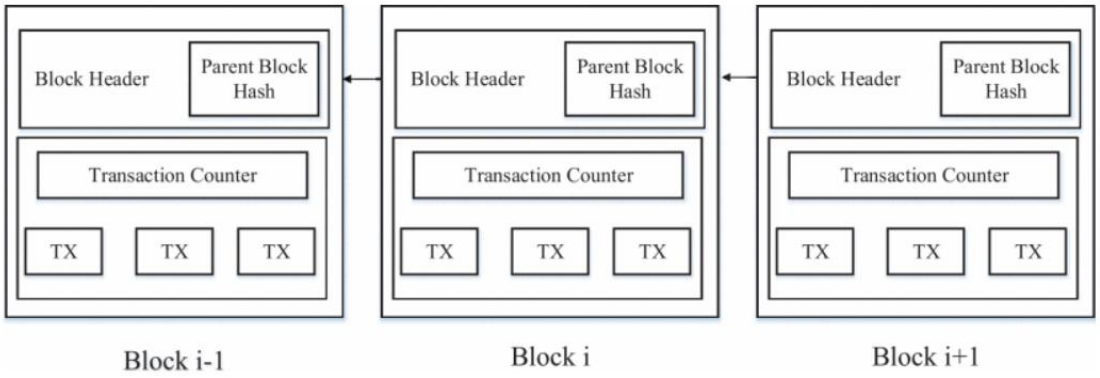
χρησιμοποιήσουν το blockchain για να προσελκύσουν πελάτες. Εκτός αυτού, το blockchain διανέμεται και μπορεί να αποφύγει το μόνο σημείο της κατάστασης αποτυχίας[5]. Όσον αφορά τα έξυπνα συμβόλαια, το συμβόλαιο θα μπορούσε να εκτελεστεί αυτόματα από τους ανθρώπους όταν το συμβόλαιο έχει αναπτυχθεί στο blockchain.

Αν και η τεχνολογία blockchain έχει μεγάλες δυνατότητες για την κατασκευή των μελλοντικών συστημάτων Διαδικτύου, αντιμετωπίζει μια σειρά τεχνικών προκλήσεων. Πρώτον, η επεκτασιμότητα είναι τεράστια ανησυχία. Το μέγεθος του μπλοκ Bitcoin περιορίζεται τώρα σε 1 MB ενώ ένα μπλοκ εξορύσσεται περίπου κάθε δέκα λεπτά. Στη συνέχεια, το δίκτυο Bitcoin περιορίζεται σε ποσοστό 7 συναλλαγών ανά δευτερόλεπτο, το οποίο είναι ανίκανο να διαπραγματευτεί συναλλαγές υψηλής συχνότητας. Ωστόσο, μεγαλύτερα μπλοκ σημαίνει μεγαλύτερο χώρο αποθήκευσης και πιο αργή διάδοση στο δίκτυο[6]. Αυτό θα οδηγήσει στη σταδιακή συγκέντρωση καθώς λιγότεροι χρήστες θα ήθελαν να διατηρήσουν ένα τόσο μεγάλο blockchain. Επομένως, η ανταλλαγή μεταξύ μεγέθους μπλοκ και ασφάλειας ήταν μια σκληρή πρόκληση. Δεύτερον, έχει αποδειχθεί ότι οι άνθρωποι θα μπορούσαν να επιτύχουν μεγαλύτερα έσοδα από το δίκαιο μερίδιό τους μέσω της εγωιστικής στρατηγικής εξόρυξης (selfishminingstrategy). Οι άνθρωποι κρύβουν τα περιουσιακά στοιχεία τους για περισσότερα έσοδα στο μέλλον. Με αυτόν τον τρόπο, τα υποκαταστήματα θα μπορούσαν να πραγματοποιούνται συχνά, γεγονός που εμποδίζει την ανάπτυξη blockchain. Ως εκ τούτου, πρέπει να προταθούν ορισμένες λύσεις για να επιλυθεί αυτό το πρόβλημα[6]. Επιπλέον, έχει αποδειχθεί ότι η διαρροή απορρήτου θα μπορούσε επίσης να συμβεί στο blockchain, ακόμη και οι χρήστες πραγματοποιούν συναλλαγές μόνο με το δημόσιο κλειδί και το ιδιωτικό κλειδί τους. Επιπλέον, οι τρέχοντες αλγόριθμοι συναίνεσης (consensusalgorithms) όπως η *απόδειξη της εργασίας (proof of work)* ή η *απόδειξη διακυβεύσεων (proof of stake)* αντιμετωπίζουν ορισμένα σοβαρά προβλήματα[7]. Για παράδειγμα, η απόδειξη της εργασίας σπαταλά πάρα πολύ ενέργεια ηλεκτρικής ενέργειας, ενώ το φαινόμενο ότι οι πλούσιοι γίνονται πλουσιότεροι θα μπορούσε να εμφανιστεί στην απόδειξη της διαδικασίας συναίνεσης μεριδίων (proof of stakeconsentprocess).

1.1.Η δομή ενός blockchain

Ένα blockchain είναι σαν ένα ψηφιακό καθολικό ((conventionalpublicledger)) που διατηρεί αρχείο συναλλαγών. Φανταστείτε το ως μια αλυσίδα που αποτελείται από

μπλοκ, και κάθε μπλοκ περιέχει μια δέσμη πληροφοριών συναλλαγής. Αυτά τα μπλοκ συνδέονται με τρόπο ώστε κάθε μπλοκ να έχει έναν σύνδεσμο με το προηγούμενο. Σκεφτείτε το σαν ένα οικογενειακό δέντρο όπου κάθε άτομο (μπλοκ) ξέρει ποιος είναι ο γονέας του (το μπλοκ πριν από αυτό). Ακόμα και οι μακρινοί συγγενείς (μπλοκ πιο πίσω) συνδέονται με το γενεαλογικό δέντρο. Το πρώτο μπλοκ σε μια αλυσίδα μπλοκ ονομάζεται «μπλοκ γένεσης» [7]. Είναι σαν τον γηραιότερο πρόγονο του γενεαλογικού δέντρου και δεν έχει γονείς γιατί είναι ο πρώτος. Αυτή η τεχνολογία χρησιμοποιείται σε πράγματα όπως τα κρυπτονομίσματα (όπως το Bitcoin) για να διασφαλιστεί ότι όλες οι συναλλαγές καταγράφονται με ασφάλεια και ότι δεν μπορούν εύκολα να αλλάξουν.



1.2.Τα χαρακτηριστικά ενός blockchain

Συνοπτικά, το blockchain έχει τα ακόλουθα βασικά χαρακτηριστικά.

• Αποκέντρωση (Decentralization)

Στα συμβατικά κεντρικά συστήματα συναλλαγών, κάθε συναλλαγή πρέπει να επικυρώνεται μέσω του κεντρικού αξιόπιστου οργανισμού (π.χ. της κεντρικής τράπεζας), αναπόφευκτα να έχει ως αποτέλεσμα τη μείωση του κόστους και της απόδοσης στους κεντρικούς διακομιστές[8]. Σε αντίθεση με την κεντρική λειτουργία, δεν απαιτείται πλέον τρίτο μέρος στο blockchain. Οι αλγόριθμοι συναίνεσης (consensusalgorithms) στο blockchain χρησιμοποιούνται για τη διατήρηση της συνοχής των δεδομένων στο κατανεμημένο δίκτυο.

• Ανθεκτικότητα (Resilience)

Οι συναλλαγές μπορούν να επικυρωθούν γρήγορα και οι άκυρες συναλλαγές δεν γίνονται δεκτές από έντιμους κόμβους (honestnodes)[8]. Είναι σχεδόν αδύνατο να διαγράψετε ή να επαναφέρετε τις συναλλαγές μόλις συμπεριληφθούν στο

blockchain. Μπορούν να εντοπιστούν αμέσως μπλοκ που περιέχουν μη έγκυρες συναλλαγές.

• Ανωνυμία (Anonymity)

Κάθε χρήστης μπορεί να αλληλεπιδράσει με το blockchain με μια δημιουργημένη διεύθυνση, η οποία δεν αποκαλύπτει την πραγματική ταυτότητα του χρήστη[9]. Σημειώστε ότι το blockchain δεν μπορεί να εγγυηθεί την τέλεια διατήρηση του απορρήτου λόγω του εγγενούς περιορισμού.

• Ελεξιμότητα (Auditability)

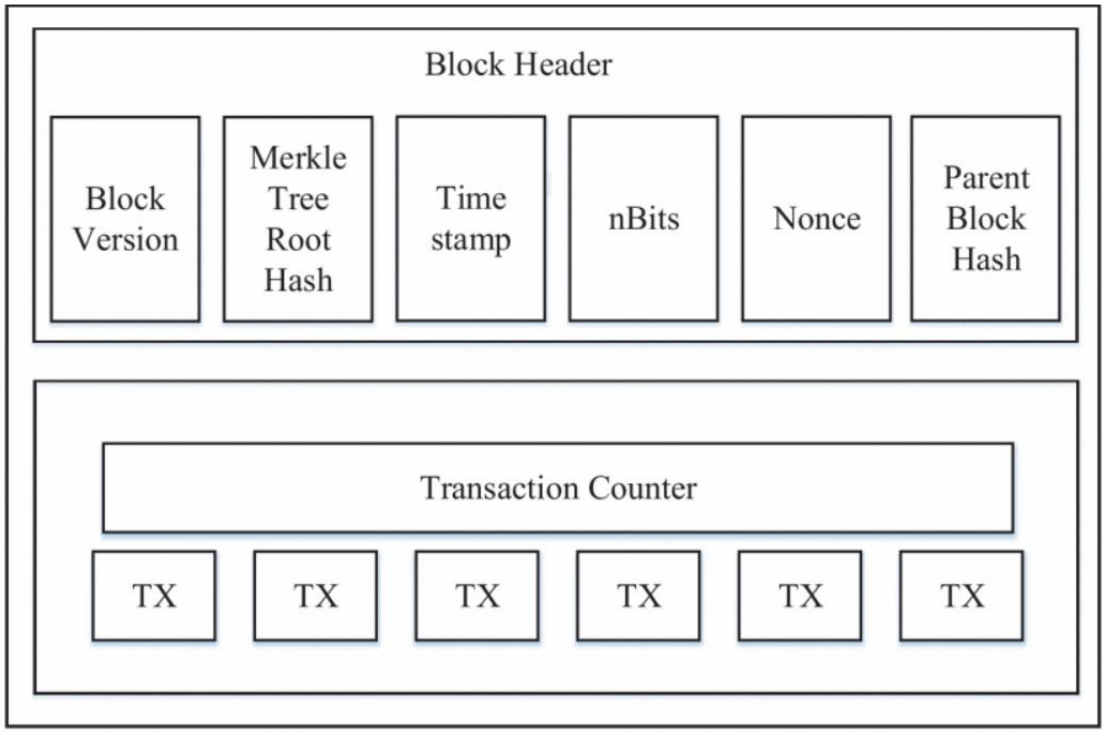
Το Bitcoin blockchain αποθηκεύει δεδομένα σχετικά με τα υπόλοιπα χρηστών βάσει του μοντέλου Unspent Transaction Output (UTX-O): Κάθε συναλλαγή πρέπει να αναφέρεται σε ορισμένες προηγούμενες μη χρησιμοποιημένες συναλλαγές. Μόλις η τρέχουσα συναλλαγή καταγραφεί στο blockchain, η κατάσταση αυτών των αναφερόμενων μη χρησιμοποιημένων συναλλαγών μεταβαίνει από μη δαπανημένη σε δαπάνη[9]. Έτσι, οι συναλλαγές θα μπορούσαν εύκολα να επαληθευτούν και να εντοπιστούν.

1.3.Δομικά μπλοκ Blockchain

Ένα μπλοκ αποτελείται από την *κεφαλίδα* του *μπλοκ (headerofblock)* και το *σώμα μπλοκ* (bodyofblock) όπως φαίνεται και στην εικόνα που ακολουθεί παρακάτω. Συγκεκριμένα, η κεφαλίδα του μπλοκ περιλαμβάνει[10]:

1. Έκδοση αποκλεισμού (Block ValidationRuleset): υποδεικνύει ποιο σύνολο κανόνων επικύρωσης μπλοκ πρέπει να ακολουθούν.
2. Κατακερματισμός ρίζας Merkle tree (Merkle Tree Root Hash): η τιμή κατακερματισμού όλων των συναλλαγών στο μπλοκ.
3. Χρονική σήμανση (Timestamp): τρέχουσα ώρα ως δευτερόλεπτα σε καθολική ώρα από την 1η Ιανουαρίου 1970.
4. nBits: όριο στόχου ενός έγκυρου κατακερματισμού μπλοκ.
5. Nonce: ένα πεδίο 4 byte, το οποίο συνήθως ξεκινά με 0 και αυξάνεται για κάθε υπολογισμό κατακερματισμού.
6. Κατακερματισμός γονικού μπλοκ (Parent Block Hash): τιμή κατακερματισμού 256-bit που δείχνει το προηγούμενο μπλοκ.

Το σώμα μπλοκ αποτελείται από έναν μετρητή συναλλαγών και συναλλαγές. Ο μέγιστος αριθμός συναλλαγών που μπορεί να περιέχει ένα μπλοκ εξαρτάται από το μέγεθος του μπλοκ και το μέγεθος κάθε συναλλαγής. Το Blockchain χρησιμοποιεί έναν ασύμμετρο μηχανισμό (asymmetricmechanism) κρυπτογράφησης για την επικύρωση του ελέγχου ταυτότητας των συναλλαγών [11]. Η ψηφιακή υπογραφή που βασίζεται σε ασύμμετρη κρυπτογραφία χρησιμοποιείται σε ένα αναξιόπιστο περιβάλλον. Στη συνέχεια παρουσιάζουμε εν συντομία την ψηφιακή υπογραφή (digitalsignature).



Κάθε χρήστης διαθέτει ένα ζευγάρι ιδιωτικού κλειδιού και δημόσιου κλειδιού. Το ιδιωτικό κλειδί που θα τηρείται εμπιστευτικό χρησιμοποιείται για την υπογραφή των συναλλαγών[11]. Οι ψηφιακές υπογεγραμμένες συναλλαγές μεταδίδονται σε ολόκληρο το δίκτυο. Η τυπική ψηφιακή υπογραφή εμπλέκεται σε δύο φάσεις: *φάση υπογραφής* και *φάση επαλήθευσης* . Για παράδειγμα, ένας χρήστης Alice θέλει να στείλει ένα μήνυμα στον άλλο Bob.

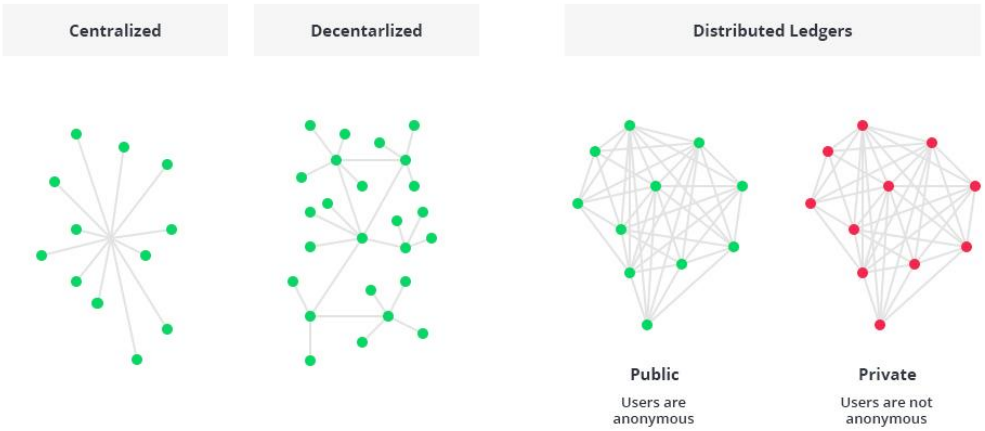
(1) Στη φάση υπογραφής, η Αλίκη κρυπτογραφεί τα δεδομένα της με το ιδιωτικό της κλειδί και στέλνει στον Bob το κρυπτογραφημένο αποτέλεσμα και τα πρωτότυπα δεδομένα[12].

(2) Στη φάση επαλήθευσης, ο Μπομπ επικυρώνει την τιμή με το δημόσιο κλειδί της Αλίκης. Με αυτόν τον τρόπο, ο Μπομπ θα μπορούσε εύκολα να ελέγξει αν τα δεδομένα έχουν αλλοιωθεί ή όχι. Ο τυπικός αλγόριθμος ψηφιακής υπογραφής που

χρησιμοποιείται σε blockchain είναι ο αλγόριθμος ψηφιακής υπογραφής ελλειπτικής καμπύλης (ECDSA - EllipticCurve Digital Signature Algorithm).

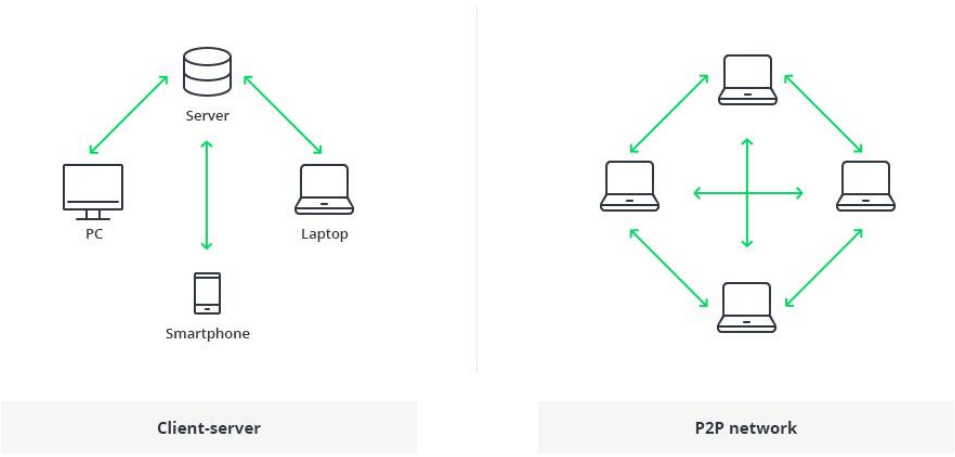
1.4.Αρχιτεκτονική Blockchain

Για αρχάριους, ας μάθουμε πρώτα τι είναι η τεχνολογία blockchain. Λογικά, ένα blockchain είναι μια αλυσίδα μπλοκ που περιέχουν συγκεκριμένες πληροφορίες (βάση δεδομένων), αλλά με ασφαλή και γνήσιο τρόπο που ομαδοποιείται σε ένα δίκτυο (peer-to-peer)[13]. Με άλλα λόγια, το blockchain είναι ένας συνδυασμός υπολογιστών που συνδέονται μεταξύ τους αντί ενός κεντρικού διακομιστή, πράγμα που σημαίνει ότι ολόκληρο το δίκτυο είναι decentralized network.



Η τεχνική blockchain επιτρέπει τη διανομή ψηφιακών πληροφοριών και όχι την αντιγραφή. Αυτό το κατανεμημένο καθολικό δίκτυο (distributedglobal network) παρέχει διαφάνεια, εμπιστοσύνη και ασφάλεια δεδομένων.

Η αρχιτεκτονική Blockchain χρησιμοποιείται πολύ ευρέως στον χρηματοοικονομικό κλάδο. Ωστόσο, αυτές τις μέρες, αυτή η τεχνολογία βοηθά στη δημιουργία λύσεων ανάπτυξης λογισμικού για κρυπτογράφηση και τήρηση αρχείων, ψηφιακό συμβολαιογράφο (digital notary) και έξυπνα συμβόλαια (smart contracts).



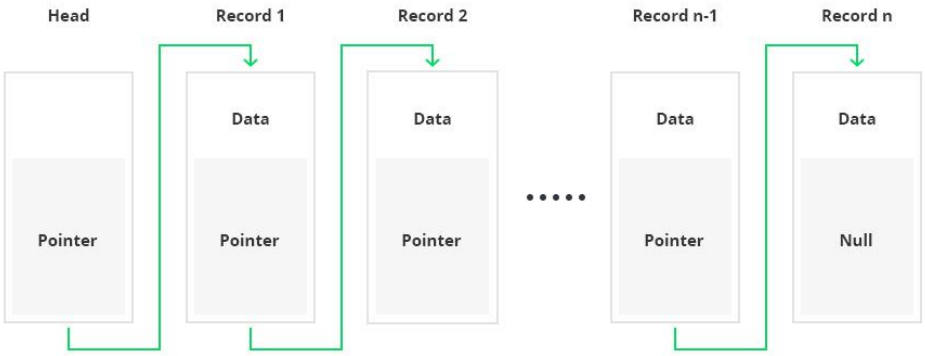
Η παραδοσιακή αρχιτεκτονική του World Wide Web χρησιμοποιεί ένα δίκτυο διακομιστή-πελάτη[14]. Σε αυτήν την περίπτωση, ο διακομιστής διατηρεί όλες τις απαιτούμενες πληροφορίες σε ένα μέρος, ώστε να είναι εύκολο να ενημερωθεί, λόγω του ότι ο διακομιστής είναι μια κεντρική βάση δεδομένων που ελέγχεται από έναν αριθμό διαχειριστών με δικαιώματα.

Στην περίπτωση του κατανεμημένου δικτύου αρχιτεκτονικής blockchain, κάθε συμμετέχων στο δίκτυο διατηρεί, εγκρίνει και ενημερώνει νέες καταχωρήσεις. Το σύστημα ελέγχεται όχι μόνο από ξεχωριστά άτομα, αλλά και από όλους στο δίκτυο blockchain. Κάθε μέλος διασφαλίζει ότι όλα τα αρχεία και οι διαδικασίες είναι σωστά, με αποτέλεσμα την εγκυρότητα των δεδομένων και την ασφάλεια. Έτσι, τα μέρη (parties/regions) που δεν εμπιστεύονται απαραίτητα το ένα το άλλο μπορούν να επιτύχουν μια κοινή συναίνεση.

Για να συνοψίσουμε τα πράγματα, το blockchain είναι ένα decentralized network, κατανεμημένο καθολικό δίκτυο (distributedglobal network) (δημόσιο ή ιδιωτικό) διαφόρων ειδών συναλλαγών που διοργανώνονται σε ένα δίκτυο P2P[15]. Αυτό το δίκτυο αποτελείται από πολλούς υπολογιστές, αλλά με τρόπο που τα δεδομένα δεν μπορούν να τροποποιηθούν χωρίς τη συναίνεση ολόκληρου του δικτύου (κάθε ξεχωριστός υπολογιστής).

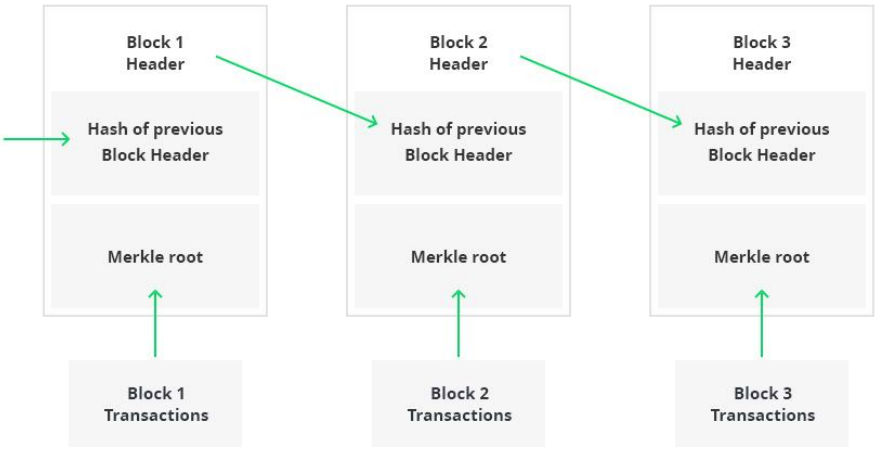
Η δομή της τεχνολογίας blockchain αντιπροσωπεύεται από μια λίστα μπλοκ με συναλλαγές σε μια συγκεκριμένη σειρά. Αυτές οι λίστες μπορούν να αποθηκευτούν ως επίπεδο αρχείο (μορφή txt.) ή με τη μορφή μιας απλής βάσης δεδομένων. Δύο ζωτικές δομές δεδομένων που χρησιμοποιούνται στο blockchain περιλαμβάνουν:

- Δείκτες - μεταβλητές που διατηρούν πληροφορίες σχετικά με τη θέση μιας άλλης μεταβλητής. Συγκεκριμένα, αυτό δείχνει τη θέση μιας άλλης μεταβλητής.
- Συνδεδεμένες λίστες - μια ακολουθία μπλοκ όπου κάθε μπλοκ έχει συγκεκριμένα δεδομένα και συνδέσμους προς το ακόλουθο μπλοκ με τη βοήθεια ενός δείκτη.



Λογικά, το πρώτο μπλοκ δεν περιέχει το δείκτη αφού αυτό είναι το πρώτο σε μια αλυσίδα[15]. Ταυτόχρονα, υπάρχει πιθανότατα ένα τελικό μπλοκ στη βάση δεδομένων blockchain που έχει δείκτη χωρίς τιμή.

Βασικά, το ακόλουθο διάγραμμα ακολουθίας blockchain είναι μια συνδεδεμένη λίστα εγγραφών:



Η αρχιτεκτονική Blockchain μπορεί να εξυπηρετήσει τους ακόλουθους σκοπούς για οργανισμούς και επιχειρήσεις:

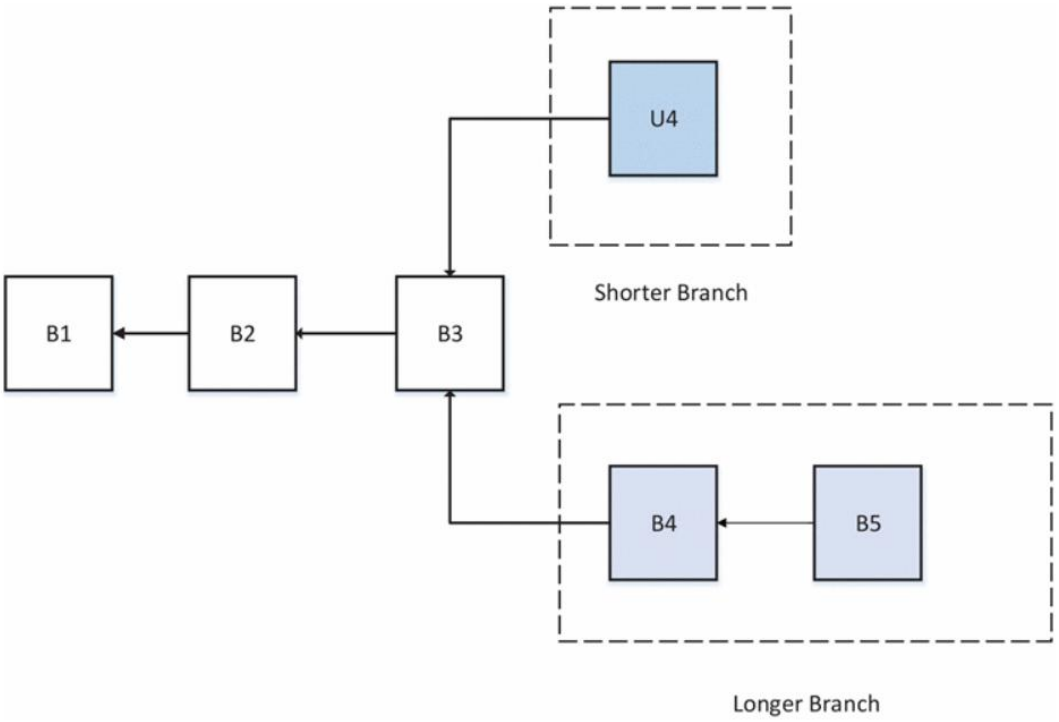
- Μείωση κόστους - πολλά χρήματα δαπανώνται για τη διατήρηση κεντρικών βάσεων δεδομένων (π.χ. τράπεζες, κυβερνητικά ιδρύματα) διατηρώντας τα τρέχοντα δεδομένα ασφαλή από εγκλήματα στον κυβερνοχώρο και άλλες διεφθαρμένες προθέσεις.
- Ιστορικό δεδομένων - μέσα σε μια δομή blockchain, είναι δυνατό να ελέγξετε το ιστορικό οποιασδήποτε συναλλαγής ανά πάσα στιγμή. Αυτό είναι ένα συνεχώς αναπτυσσόμενο αρχείο, ενώ μια κεντρική βάση δεδομένων είναι περισσότερο ένα στιγμιότυπο πληροφοριών σε ένα συγκεκριμένο σημείο.
- Ισχύς και ασφάλεια δεδομένων - μόλις εισαχθούν, τα δεδομένα είναι δύσκολο να παραβιαστούν λόγω της φύσης του blockchain. Χρειάζεται χρόνος για να προχωρήσουμε στην επικύρωση εγγραφής, καθώς η διαδικασία πραγματοποιείται σε κάθε ανεξάρτητο δίκτυο και όχι μέσω σύνθετης ισχύος επεξεργασίας[16]. Αυτό σημαίνει ότι το σύστημα θυσιάζει την ταχύτητα απόδοσης, αλλά αντ 'αυτού εγγυάται υψηλή ασφάλεια και εγκυρότητα δεδομένων.

1.5.Βασικοί αλγόριθμοι συναίνεσης

Η επίτευξη συναίνεσης (reachingconsensus) σε κατανεμημένο περιβάλλον είναι μια πρόκληση. Είναι επίσης μια πρόκληση για το blockchain καθώς διανέμεται το δίκτυο blockchain. Στο blockchain, δεν υπάρχει κεντρικός κόμβος που να διασφαλίζει ότι τα καθολικά σε κατανεμημένους κόμβους(distributednodes) είναι όλα τα ίδια[17]. Μερικά πρωτόκολλα απαιτούνται για να διασφαλιστεί ότι τα βιβλία σε διαφορετικούς κόμβους είναι συνεπή. Στη συνέχεια παρουσιάζουμε πολλές κοινές προσεγγίσεις για την επίτευξη συναίνεσης στο blockchain.

Το PoW (Απόδειξη εργασίας) είναι μια στρατηγική συναίνεσης (consensus) που χρησιμοποιείται στο δίκτυο Bitcoin. Σε ένα αποκεντρωμένο δίκτυο (decentralized network), κάποιος πρέπει να επιλεγεί για την καταγραφή των συναλλαγών. Ο ευκολότερος τρόπος είναι η τυχαία επιλογή (randomchoice). Ωστόσο, η τυχαία επιλογή είναι ευάλωτη σε επιθέσεις. Επομένως, εάν ένας κόμβος θέλει να δημοσιεύσει ένα μπλοκ συναλλαγών (transactionblock), πρέπει να γίνει πολλή δουλειά για να αποδειχθεί ότι ο κόμβος δεν είναι πιθανό να επιτεθεί στο δίκτυο. Γενικά η εργασία σημαίνει υπολογισμούς υπολογιστών. Στο PoW, κάθε κόμβος του δικτύου υπολογίζει μια τιμή κατακερματισμού της κεφαλίδας μπλοκ. Η

κεφαλίδα του μπλοκ περιέχει ένα nonce και οι κόμβοι θα άλλαζαν το nonce συχνά για να λάβουν διαφορετικές τιμές κατακερματισμού[17]. Η consensusαπαιτεί ότι η υπολογισμένη τιμή πρέπει να είναι ίση ή μικρότερη από μια συγκεκριμένη δεδομένη τιμή. Όταν ένας κόμβος φτάσει την τιμή-στόχο (goalpoint), θα μεταδίδει το μπλοκ σε άλλους κόμβους και όλοι οι άλλοι κόμβοι πρέπει να επιβεβαιώνουν αμοιβαία την ορθότητα της τιμής κατακερματισμού. Εάν το μπλοκ επικυρωθεί (verifiedblock), άλλοι κόμβοι θα προσθέσουν αυτό το νέο μπλοκ στα δικά τους μπλοκ[17]. Οι κόμβοι που υπολογίζουν τις τιμές κατακερματισμού καλούνται *κόμβοι (nodes)*και η διαδικασία PoW ονομάζεται *εξόρυξη (mining)* σε Bitcoin.



Στο decentralized network, μπορεί να δημιουργηθούν ταυτόχρονα έγκυρα μπλοκ όταν πολλοί κόμβοι βρουν την κατάλληλη nonce σχεδόν ταυτόχρονα. Ως αποτέλεσμα, μπορούν να δημιουργηθούν κλάδοι.

Ωστόσο, είναι απίθανο δύο ανταγωνιστικά πιρούνια (competingforks) να δημιουργήσουν το επόμενο μπλοκ ταυτόχρονα. Στο πρωτόκολλο PoW, μια αλυσίδα που μεγαλώνει στη συνέχεια κρίνεται ως η αυθεντική. Εξετάστε δύο forks που δημιουργήθηκαν από ταυτόχρονα επικυρωμένα μπλοκ U4 και B4. Οι κόμβοι συνεχίζουν να εξορύσσουν τα μπλοκ τους μέχρι να βρεθεί ένα μεγαλύτερο κλαδί. Τα B4, B5 σχηματίζουν μια μακρύτερη αλυσίδα, έτσι οι κόμβοι στο U4 θα μεταβούν στο μακρύτερο κλαδί.

Οι κόμβοι πρέπει να κάνουν πολλούς υπολογισμούς υπολογιστών στο PoW, ωστόσο αυτά τα έργα σπαταλούν πάρα πολύ πόρους (resources). Για να μετριαστεί η απώλεια, έχουν σχεδιαστεί ορισμένα πρωτόκολλα PoW στα οποία τα έργα θα μπορούσαν να έχουν κάποιες πλευρικές εφαρμογές[18]. Για παράδειγμα, το Primecoin αναζητά ειδικές πρώτες αλυσίδες αριθμών που μπορούν να χρησιμοποιηθούν για μαθηματική έρευνα.

Το PoS (Απόδειξη πονταρίσματος) είναι μια εναλλακτική λύση εξοικονόμησης ενέργειας έναντι του PoW. Οι κόμβοι στο PoS πρέπει να αποδείξουν την κυριότητα του ποσού του νομίσματος. Πιστεύεται ότι τα άτομα με περισσότερα νομίσματα θα είναι λιγότερο πιθανό να επιτεθούν στο δίκτυο. Η επιλογή που βασίζεται στο υπόλοιπο του λογαριασμού είναι αρκετά άδικη επειδή το μόνο πλουσιότερο άτομο είναι υποχρεωτικό να κυριαρχεί στο δίκτυο. Ως αποτέλεσμα, προτείνονται πολλές λύσεις με το συνδυασμό του μεγέθους πονταρίσματος για να αποφασιστεί ποια θα σφυρηλατήσει (forge) το επόμενο μπλοκ[18]. Συγκεκριμένα, το Blackcoin χρησιμοποιεί τυχαιοποίηση για να προβλέψει την επόμενη γεννήτρια. Χρησιμοποιεί έναν τύπο που αναζητά τη χαμηλότερη τιμή κατακερματισμού σε συνδυασμό με το μέγεθος του στοιχήματος. Peercoin ευνοεί την επιλογή βάσει ηλικίας νομισμάτων. Στο Peercoin, μεγαλύτερα και μεγαλύτερα σύνολα κερμάτων έχουν μεγαλύτερη πιθανότητα να εξορύξουν το επόμενο μπλοκ. Σε σύγκριση με το PoW, το PoS εξοικονομεί περισσότερη ενέργεια και είναι πιο αποτελεσματικό. Δυστυχώς, καθώς το κόστος εξόρυξης είναι σχεδόν μηδενικό, οι επιθέσεις ενδέχεται να προκύψουν. Πολλά blockchain υιοθετούν PoW στην αρχή και μετατρέπονται στα PoS σταδιακά[19]. Για παράδειγμα, το ethereum σκοπεύει να μετακινηθεί από τον Ethash (ένα είδος PoW) στο Casper (ένα είδος PoS).

Το PBFT (Practical Byzantine Fault Tolerance) είναι ένας αλγόριθμος αναπαραγωγής για την ανοχή. Το Hyperledger Fabric χρησιμοποιεί το PBFT ως τον consensusalgorithmtou, καθώς το PBFT θα μπορούσε να χειριστεί έως και 1/3 κακόβουλα αντίγραφα. Ένα νέο μπλοκ καθορίζεται σε έναν γύρο[19]. Σε κάθε γύρο, ένας πρωταρχικός θα επιλέγεται σύμφωνα με ορισμένους κανόνες. Και είναι υπεύθυνο για την παραγγελία της συναλλαγής. Η όλη διαδικασία θα μπορούσε να χωριστεί σε τρεις φάσεις: *προπαρασκευασμένη, προετοιμασμένη* και *δέσμευση*. Σε κάθε φάση, ένας κόμβος θα εισέλθει στην επόμενη φάση εάν έχει λάβει ψήφους από πάνω από τα 2/3 όλων των κόμβων. Έτσι, το PBFT απαιτεί κάθε κόμβος να είναι γνωστός στο δίκτυο. Όπως το PBFT, το Stellar Consensus Protocol (SCP) είναι επίσης ένα πρωτόκολλοPBFT. Στο PBFT, κάθε κόμβος πρέπει να υποβάλλει ερώτημα σε άλλους κόμβους, ενώ το SCP δίνει στους συμμετέχοντες το δικαίωμα να

επιλέξουν ποιο σύνολο άλλων συμμετεχόντων να πιστεύουν. Με βάση το PBFT, η Antshares έχει εφαρμόσει το dBFT τους (Delegated Byzantine Fault Tolerance)[20]. Στο dBFT, ορισμένοι επαγγελματικοί κόμβοι ψηφίζονται για την καταγραφή των συναλλαγών.

DPOS (Delegated Proof of Stake). Η κύρια διαφορά μεταξύ PoS και DPOS είναι ότι το PoS είναι άμεσα δημοκρατικό ενώ το DPOS είναι αντιπροσωπευτικό δημοκρατικό. Οι ενδιαφερόμενοι εκλέγουν τους αντιπροσώπους τους για τη δημιουργία και την επικύρωση των μπλοκ Με σημαντικά λιγότερους κόμβους για την επικύρωση του μπλοκ, το μπλοκ θα μπορούσε να επιβεβαιωθεί γρήγορα, οδηγώντας στη γρήγορη επιβεβαίωση των συναλλαγών. Εν τω μεταξύ, οι παράμετροι του δικτύου όπως το *μέγεθος μπλοκ* και τα *διαστήματα μπλοκ* θα μπορούσαν να συντονιστούν από τους αντιπροσώπους[20]. Επιπλέον, οι χρήστες δεν χρειάζεται να ανησυχούν για τους ανέντιμους εκπροσώπους, καθώς θα μπορούσαν να ψηφιστούν εύκολα. Το DPOS είναι η ραχοκοκαλιά του Bitshares.

Το Ripple είναι ένας αλγόριθμος συναίνεσης που χρησιμοποιεί συλλογικά αξιόπιστα υποδίκτυα στο μεγαλύτερο δίκτυο. Στο δίκτυο, οι κόμβοι χωρίζονται σε δύο τύπους: *διακομιστής* για συμμετοχή στη διαδικασία συναίνεσης και *πελάτης* για τη μεταφορά χρημάτων μόνο. Κάθε διακομιστής έχει μια μοναδική λίστα κόμβων (UNL - UniqueNodeList)[20]. Το UNL είναι σημαντικό για τον διακομιστή. Κατά τον καθορισμό του εάν θα τοποθετηθεί μια συναλλαγή στο global, ο διακομιστής θα ρωτήσει τους κόμβους στο UNL και εάν οι συμφωνίες που λήφθηκαν έφτασαν το 80%, η συναλλαγή θα συσκευαζόταν στο global. Για έναν κόμβο, το global θα παραμείνει σωστό εφόσον το ποσοστό των ελαττωματικών κόμβων στο UNL είναι μικρότερο από 20%.

2.Blockchain και IoT

Το Internet of Things (IoT) είναι ένα παράδειγμα ότι τα ετερογενή φυσικά αντικείμενα διασυνδέονται μέσω ενσύρματων ή ασύρματων τεχνολογιών και συνδέονται περαιτέρω άψογα στο Διαδίκτυο, επιτρέποντας οπουδήποτε και οποτεδήποτε συνδεσιμότητα[21]. Τα τελευταία χρόνια, είδαμε την ευρεία υιοθέτηση εφαρμογών IoT σε διάφορους τομείς της βιομηχανίας, συμπεριλαμβανομένης της κατασκευής, του αυτοματισμού του σπιτιού, των μεταφορών και της υγειονομικής περίθαλψης.

Οι περισσότερες υπάρχουσες μεγάλης κλίμακας βιομηχανικές υποδομές IoT (IIoT) αναπτύσσονταικαι συντηρούνται από μεμονωμένα μέρη. Συνήθως βασίζονται σε cloud και βασίζονται σε κεντρικά μοντέλα επικοινωνίας (centralizedcommunicationmodels), στο οποίο όλες οι συσκευές αναγνωρίζονται, πιστοποιούνται και συνδέονται μέσω διακομιστών cloud που παρέχουν άφθονες δυνατότητες υπολογισμού και αποθήκευσης.

Μαζί με την ταχεία αύξηση του μεγέθους και της πολυπλοκότητας των δικτύων IIoT, οι κεντρικές λύσεις IIoT γίνονται ωστόσο πιο ακριβές λόγω του υψηλού κόστους ανάπτυξης και συντήρησης που σχετίζεται με τις υποδομές δικτύου και cloud[22]. Αυτό το πρόβλημα επιδεινώνεται περαιτέρω από την αυξανόμενη ζήτηση τα δίκτυα IIoT από διαφορετικά μέρη να μπορούν να επικοινωνούν και να παρέχουν από κοινού αμετάβλητα και επαληθεύσιμα δεδομένα. Με τα παραδοσιακά δίκτυα IIoT, τα δεδομένα που παρέχονται από μεμονωμένα βιομηχανικά μέρη ενδέχεται να μην είναι αξιόπιστα επειδή μπορούν να πλαστογραφηθούν ή να τροποποιηθούν από τους επιτιθέμενους ή τον κάτοχο των δεδομένων. Είναι επιθυμητό να υπάρχουν μηχανισμοί για την επαλήθευση της αξιοπιστίας των δεδομένων σε δίκτυα IIoT.

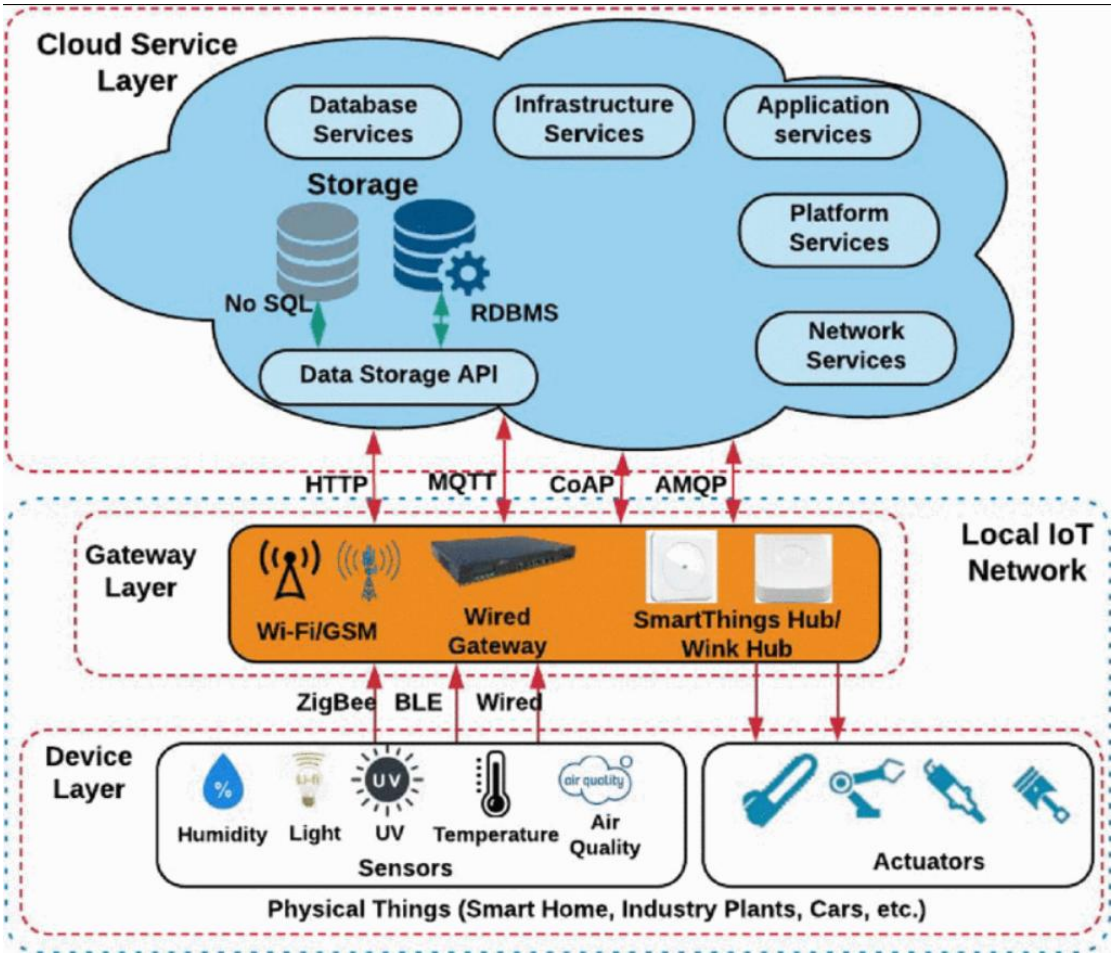
Η τεχνολογία blockchain, ωστόσο, δεν μπορεί να ενσωματωθεί άμεσα σε υπάρχουσες λύσεις IioT[23], λόγω των εξαιρετικά περιορισμένων πόρων στα δίκτυα IIoT και της απαίτησης της τεχνολογίας blockchain ότι κάθε συμμετέχων πρέπει να διατηρεί ένα ακριβές αντίγραφο του blockchain για να εγγυηθεί τη συνέπεια (consistency). Για παράδειγμα, το Bitcoin είναι μία από τις πιο επιτυχημένες εφαρμογές που βασίζονται σε blockchain μέχρι σήμερα. Το blockchain Bitcoin, παρόλο που δεν ενημερώνεται συχνά, αυτή τη στιγμή περιέχει περισσότερα από 190 GB δεδομένων[24], εκ των οποίων μόνο μερικά σχετίζονται με μεταφορές νομισμάτων. Σε σύγκριση με το Bitcoin, τα περισσότερα συστήματα IIoT μεγάλης κλίμακας δημιουργούν πολύ μεγαλύτερους όγκους δεδομένων και είναι απλώς αδύνατο να αποθηκευτούν όλα τα μπλοκ σε τοπικά δίκτυα IIoT.

2.1.Υποδομή IoT που βασίζεται στο cloud

Η εικόνα που ακολουθεί στην παρούσα ενότητα, δίνει μια επισκόπηση μιας τυπικής υποδομής IIoT βασισμένης σε cloud, η οποία αποτελείται κυρίως από τρία στρώματα:

1. στρώμα device,
2. στρώμα gateway και
3. στρώμα υπηρεσίας cloud.

Το στρώμα της συσκευής περιλαμβάνει ετερογενείς συσκευές IIoT, που ποικίλλουν από ισχυρές υπολογιστικές μονάδες έως εξαιρετικά χαμηλής ισχύος μικροελεγκτές[25]. Αυτές οι συσκευές συνδέονται με το επίπεδο πύλης μέσω διαφόρων τεχνολογιών ενσύρματης και ασύρματης δικτύωσης, όπως ZigBee, BLE, Ethernet, κ.λπ., και χρησιμεύουν ως γέφυρες στα clouds. Αυτές οι προσαρμοσμένες πύλες είναι συνήθως αναπόσπαστο μέρος της ανεπτυγμένης υποδομής IIoT, η οποία οδηγεί απευθείας σε λύσεις "stovepipe"[26]. Αυτό προκαλεί περαιτέρω θέματα διαλειτουργικότητας, δηλαδή τα δεδομένα και οι υπηρεσίες που παρέχονται από έναν οργανισμό δεν μπορούν να κοινοποιηθούν ή να χρησιμοποιηθούν από συσκευές των άλλων οργανισμών (λόγω διαφορετικών πρωτοκόλλων δικτύωσης, μορφών δεδομένων κ.λπ.) και οι χρησιμοποιούμενοι μηχανισμοί ασφαλείας είναι συχνά ιδιόκτητοι και χωρίς έγγραφα.



Συσκευές IoT

Οι περισσότερες συσκευές IoT αναπτύσσονται στον φυσικό κόσμο για τη μέτρηση και τη δειγματοληψία των σχετικών φυσικών ή κυβερνοχώρων τους. Έχουν περιορισμένους πόρους (resources), συμπεριλαμβανομένου του μεγέθους της μνήμης, της υπολογιστικής ισχύος και του εύρους ζώνης επικοινωνίας. Επιπλέον, οι συσκευές και οι υιοθετημένες τεχνολογίες δικτύωσης τους είναι εξαιρετικά ετερογενείς. Αυτή η ετερογένεια θέτει μια πρόκληση επιχορήγησης στη διασύνδεση συσκευών IioT[26]. Απαιτεί την αλληλεπίδραση μεταξύ των συσκευών IoT για να τεθεί η διαλειτουργικότητα στην πρώτη θέση, έτσι ώστε οι ετερογενείς συσκευές να μπορούν να μετασχηματιστούν σε αποδεκτές μορφές του χρήστη τόσο για τη syntaxόσο και για τη semantically.

IoT Storage

Σε ένα τοπικό δίκτυο IoT, συνήθως υιοθετείται ένα κεντρικό σχήμα αποθήκευσης για τη διαχείριση των δεδομένων IoT, αντί για τοπικά σχήματα (π.χ. αποθήκευση δεδομένων στην τοπική μνήμη συσκευών IoT) ή διανεμημένων σχημάτων (π.χ. αποθήκευση δεδομένων σε ορισμένους κόμβους με πλούσιους πόρους

αποθήκευσης στο δίκτυο)[27]. Σε ένα κεντρικό σχήμα αποθήκευσης, τα δεδομένα συλλέγονται από το gateway και στη συνέχεια αποστέλλονται και αποθηκεύονται σε έναν τοπικό κεντρικό αποθηκευτικό χώρο. Γενικότερα στα προγράμματα, η τοπική κεντρική αποθήκευση θα μπορούσε να είναι είτε ιστορικό είτε ιδιωτικό κέντρο δεδομένων, στο οποίο όλα τα δεδομένα αποθηκεύονται τοπικά και ιδιωτικά. Αυτός ο κεντρικός αποθηκευτικός χώρος μέσα σε ένα τοπικό δίκτυο IoT μπορεί να παρέχει ταχύτερη πρόσβαση στα πρόσφατα δεδομένα χωρίς πρόσβαση στο cloud. Το πού και πώς αναπτύσσεται ο τοπικός χώρος αποθήκευσης στο τοπικό δίκτυο IoT εξαρτάται από τις προδιαγραφές σχεδιασμού του συστήματος.

Μηχανή δεδομένων

Η μηχανή δεδομένων είναι ένα στοιχείο *λογισμικού* που μετατρέπει εισερχόμενα και εξερχόμενα ακατέργαστα δεδομένα από και προς τις συσκευές IoT σε απαιτούμενες φόρμες. Για παράδειγμα, στην προτεινόμενη αρχιτεκτονική IoT βασισμένη σε blockchain που θα επεξεργαστεί σε επόμενη ενότητα[27], τα ακατέργαστα δεδομένα σχηματίζονται ως συναλλαγές και κρυπτογραφούνται και μεταφορτώνονται στα clouds κατόπιν αιτήματος. Η μηχανή δεδομένων μπορεί να αναπτυχθεί στην πύλη ή σε αυτόνομη υπολογιστική εγκατάσταση στο τοπικό δίκτυο IoT. Για να εγγυηθεί την ασφάλεια στο τοπικό δίκτυο IoT, η μηχανή δεδομένων παρέχει επίσης πρόσθετες υπηρεσίες, όπως διαχείριση κλειδιών (π.χ. διανομή και ενημέρωση κλειδιών για την ασφαλή μεταφορά δεδομένων σε τοπικό δίκτυο IoT) και μηχανισμούς ασφαλείας (π.χ. υπηρεσίες ελέγχου ταυτότητας, εξουσιοδότησης και ελέγχου).

Gateway

Σε μια τυπική υποδομή IoT που βασίζεται σε cloud, η πύλη είναι μια οντότητα σύνδεσης που συνδέει το τοπικό δίκτυο IoT με ένα cloud. Στην προτεινόμενη αρχιτεκτονική IoT που βασίζεται σε blockchain, η πύλη διαδραματίζει δύο κύριους ρόλους. Από τη μία πλευρά, είναι η αφετηρία του τοπικού δικτύου IoT[27], που παρέχει λειτουργίες διαχείρισης δεδομένων και διαχείρισης δικτύου. Από την άλλη πλευρά, χρησιμεύει επίσης ως κόμβος P2P στο δίκτυο επικάλυψης blockchain, παρέχοντας λειτουργίες διακομιστή μεσολάβησης, όπως παροχή πληροφοριών δρομολόγησης, έλεγχο ταυτότητας κόμβων και διαχείριση ομάδων πολλαπλής διανομής.

Εκτός από τα επίπεδα device και gateway, το επίπεδο υπηρεσίας cloud παρέχει λειτουργίες που σχετίζονται με το cloud, όπως υπηρεσία βάσης δεδομένων και υπηρεσία εφαρμογής, για τη διαχείριση των δεδομένων που παρέχονται από τα

τοπικά δίκτυα IoT. Τόσο τα τοπικά δίκτυα IoT όσο και το επίπεδο υπηρεσιών cloud περιλαμβάνουν μαζί την πιο κοινή υπάρχουσα υποδομή IoT που βασίζεται σε cloud.

2.2.Ευκαιρίες και προκλήσεις για την ενσωμάτωση του Blockchain στο IoT

Το Blockchain, βασισμένο σε ένα decentralized network P2P και ενσωματωμένο σε κρυπτογραφικές διαδικασίες, μπορεί να προσφέρει πολλές νέες δυνατότητες και να βελτιώσει τις υπάρχουσες λειτουργίες των συστημάτων IoT[28]. Δεδομένου ότι το blockchain έχει δημιουργηθεί για αποκεντρωμένα περιβάλλοντα, το σχήμα ασφάλειάς του είναι πιο scale από τα παραδοσιακά και η ισχυρή προστασία του από την παραποίηση δεδομένων θα βοηθήσει στην πρόληψη απατεώνων συσκευών. Τα ακόλουθα χαρακτηριστικά της κατανεμημένης αρχιτεκτονικής του blockchain το καθιστούν ελκυστική τεχνολογία για την αντιμετώπιση πολλών προκλήσεων ασφάλειας και εμπιστοσύνης σε μεγάλης κλίμακας συστήματα IoT[29].

- Το Blockchain μπορεί να χρησιμοποιηθεί για τον εντοπισμό των μετρήσεων των συσκευών IoT και την αποτροπή πλαστογράφησης ή τροποποίησης δεδομένων.
- Οι συσκευές IoT μπορούν να ανταλλάσσουν δεδομένα μέσω blockchain για να δημιουργήσουν εμπιστοσύνη μεταξύ τους, αντί να περάσουν από τρίτο μέρος. Αυτό μειώνει σημαντικά το κόστος ανάπτυξης και λειτουργίας των εφαρμογών IoT.
- Η κατανεμημένη δομή του blockchain εξαλείφει μία μόνο πηγή αστοχίας στο οικοσύστημα IoT, προστατεύοντας τα δεδομένα των συσκευών IoT από παραβίαση.
- Το Blockchain επιτρέπει την αυτονομία της συσκευής μέσω έξυπνου συμβολαίου, ατομικής ταυτότητας, ακεραιότητας δεδομένων και υποστηρίζει την επικοινωνία P2P αφαιρώντας τεχνικά σημεία συμφόρησης και αναποτελεσματικότητας.
- Η διαμόρφωση των συσκευών IoT μπορεί να είναι περίπλοκη και το blockchain μπορεί να προσαρμοστεί καλά για να παρέχει αναγνώριση συσκευής IoT, έλεγχο ταυτότητας και απρόσκοπτη ασφαλή μεταφορά δεδομένων.

Η τεχνολογία Blockchain έχει τεράστιες δυνατότητες στη δημιουργία μη αξιόπιστων αποκεντρωμένων εφαρμογών IoT και παρέχει πολλά πλεονεκτήματα από τεχνική άποψη. Ωστόσο, η τεχνολογία blockchain είναι ακόμη στα αρχικά της στάδια και

υπάρχουν πολλά εμπόδια που περιορίζουν την εφαρμογή της τρέχουσας τεχνολογίας blockchain από την εφαρμογή σε εφαρμογές IoT.

Ένα από τα πιο προκλητικά προβλήματα είναι το πρόβλημα αποθήκευσης κατά την ενσωμάτωση της τεχνολογίας blockchain σε εφαρμογές IoT[29]. Σε σενάρια IoT, οι συσκευές IoT μπορούν να δημιουργήσουν τεράστιο όγκο δεδομένων σε σύντομο χρονικό διάστημα και τόσο το hash δεδομένων όσο και τα ίδια τα δεδομένα πρέπει να αποθηκευτούν. Όταν ένα blockchain μεγαλώνει με την πάροδο του χρόνου, όλοι οι συμμετέχοντες κόμβοι θα χρειάζονται μεγαλύτερη χωρητικότητα αποθήκευσης και μεγαλύτερο εύρος ζώνης για να είναι ενημερωμένοι με τις συναλλαγές που προστίθενται στο book, το οποίο είναι πιθανό να γίνει πολύ δαπανηρό.

2.2.1.Αρχιτεκτονική IoT με βάση Blockchain

Η προτεινόμενη αρχιτεκτονική IoT που βασίζεται σε blockchain, όπως φαίνεται στην εικόνα που ακολουθεί στην παρούσα ενότητα, αποτελείται από τρία επίπεδα:

1. τοπικά δίκτυα IoT,
2. το δίκτυο blockchain P2P και
3. τα clouds.

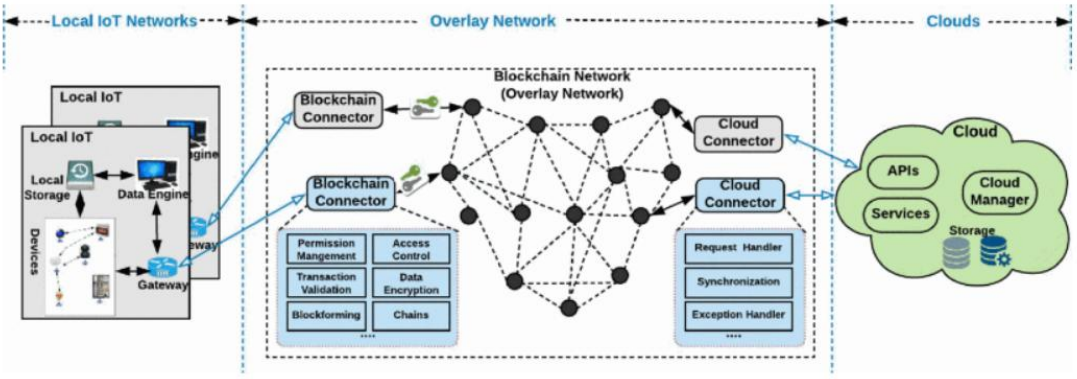
Πρώτα ακολουθούμε μια προσέγγιση από κάτω προς τα πάνω για να περιγράψουμε τα βασικά συστατικά κάθε στρώματος και στη συνέχεια παρουσιάζουμε τις λεπτομέρειες σχεδιασμού της προτεινόμενης ιεραρχικής δομής blockchain για να μετριάσουμε το ζήτημα της δυνατότητας αποθήκευσης[29].

Α. Αρχιτεκτονική συστήματος

1) Δίκτυο IoT

Εκτός από τις συνήθεις λειτουργίες τους, το βασικό πρόσθετο καθήκον των τοπικών δικτύων IoT είναι να προετοιμάσουν συναλλαγές από τα τεράστια ακατέργαστα δεδομένα που συλλέγονται από το δίκτυο. Λόγω της ετερογένειας συσκευών και εφαρμογών σε τοπικά δίκτυα IoT, τα δεδομένα πρέπει να μορφοποιηθούν και να κρυπτογραφηθούν σε συνεπή μορφή, έτσι ώστε οι δημιουργούμενες συναλλαγές να μπορούν εύκολα να λειτουργούν και να συνδέονται μεταξύ τους στο network overlayblockchain. Αυτές οι λειτουργίες γίνονται κυρίως στη μηχανή δεδομένων. Για την απρόσκοπτη συναρμολόγηση (fitting) των συναλλαγών στα μπλοκ, η προτεινόμενη αρχιτεκτονική χρησιμοποιεί έναν *σύνδεσμο blockchain* για να χρησιμεύσει ως διεπαφή μεταξύ του δικτύου IoT και του network

overlay[30]. Ο *σύνδεσμος blockchain* παρέχει τις λειτουργίες για την ασφάλεια των συναλλαγών και τους μηχανισμούς διαχείρισης της πρόσβασης των συσκευών. Στο δίκτυο IoT, αυτό μπορεί να επιτευχθεί με την ανάπτυξη μιας πλατφόρμας ασφαλείας που θα εγγυάται την αυθεντικότητα των ακατέργαστων δεδομένων από τις εξουσιοδοτημένες συσκευές IoT. Για παράδειγμα, στο έργο blockchain *της Emerson*, αξιοποιεί την *πλατφόρμα ασφαλείας Mocana*, η οποία βασίζεται σε αξιόπιστο υλικό, για να διασφαλίσει την ασφάλεια των συναλλαγών.



2) Network overlay

Αφού δημοσιευτούν οι συναλλαγές από τα τοπικά δίκτυα IoT μέσω των πυλών, οι κόμβοι στο δίκτυο επικάλυψης P2P είναι υπεύθυνοι για τη δημιουργία του blockchain. Η χρήση ενός δικτύου επικάλυψης P2P μπορεί να παρέχει αρκετά επιθυμητά χαρακτηριστικά, όπως επεκτασιμότητα, υψηλή διαθεσιμότητα και αυτοδιαμόρφωση. Οι πύλες των τοπικών δικτύων IoT οργανώνονται ως ομότιμες της επικάλυψης P2P μέσω *Blockchain Connectors*, οι οποίες παρέχουν ένα αποτελεσματικό ρελέ για την κατασκευή των μπλοκ από τις συναλλαγές. Η προτεινόμενη αρχιτεκτονική προϋποθέτει ότι το network overlayακολουθεί τα καθορισμένα πρωτόκολλα συναίνεσης blockchain, π.χ. PoW (Proof-of-Work) ή PoS (Proof-of-Stake)[30], ή Byzantine Fault Tolerance (BFT), ανάλογα με τις διαφορετικές εφαρμογές IoT. Σε γενικές γραμμές, τα πρωτόκολλα που βασίζονται σε BFT δεν έχουν προβλήματα *doublespending*, κάτι που είναι πιο κατάλληλο για βιομηχανικό IoT.

Τα σενάρια βιομηχανικού IoT τυπικά υιοθετούν μια επιτρεπόμενη ρύθμιση, η οποία λειτουργεί από τις γνωστές οντότητες και επιβάλλει αυστηρότερο έλεγχο πρόσβασης. Οι συναινέσεις που μοιάζουν με BFT έχουν διερευνηθεί ευρέως σε blockchain με άδεια, άλλα και με στόχο να ξεπεράσουν την PoW εξασφαλίζοντας ταυτόχρονα επαρκή ανοχή σε σφάλματα και ταχύτερη τελική ολοκλήρωση των

συναλλαγών[30]. Υποθέτουμε ότι το network overlayυιοθετεί ένα πρωτόκολλο BFT για την επίτευξη συναίνεσης, όπως το κλιμακούμενο BFT για ασφαλή βιομηχανική μέτρηση. Και το μοντέλο απειλής ακολουθεί τον ορισμό, δηλαδή, οι byzantinenodesείναι λιγότεροι από το 1/3 των συνολικών συμμετεχόντων κόμβων.

3) Clouds

Συνδέοντας τα τοπικά δίκτυα IoT με τα clouds, οι εφαρμογές IoT επωφελούνται από τους σχεδόν απεριόριστους υπολογιστικούς και αποθηκευτικούς πόρους του cloud για να αντισταθμίσουν τους τεχνολογικούς περιορισμούς του (π.χ. περιορισμένο μέγεθος αποθήκευσης, δυνατότητα επεξεργασίας και εύρος ζώνης επικοινωνίας)[30]. Στην προτεινόμενη αρχιτεκτονική, το δίκτυο επικάλυψης blockchain χρησιμεύει ως η γέφυρα που συνδέει τοπικά δίκτυα IoT και τα clouds μεταξύ τους. Για την ομαλή σύνδεση του δικτύου επικάλυψης με τα clouds, εκτός από τις βασικές λειτουργίες του επιπέδου υπηρεσίας cloud (π.χ. αποθήκευση δεδομένων, διαχείριση δεδομένων κ.λπ.), η προτεινόμενη αρχιτεκτονική απαιτεί ένα πρόσθετο στοιχείο γεφύρωσης, που αναφέρεται ως *σύνδεσμος cloud* για την επίλυση προβλημάτων συγχρονισμού blockchain μεταξύ του δικτύου επικάλυψης και των cloud[30].

2.3.5G: Ευκαιρίες και οφέλη για την υγειονομική περίθαλψη μέσω του Blockchain

Η τυποποίηση των δικτύων κινητής επικοινωνίας της 2ης, 3ης, 4ης και 5ης γενιάς πραγματοποιείται από το πρόγραμμα εταίρων για την τυποποίηση συστημάτων 3ης γενιάς (Πρόγραμμα Συνεργασίας 3ης Γενιάς, 3GPP - 3rd Generation Partnership Project)[31].

Το 5G έχει σχεδιαστεί για να ανταποκρίνεται στις ακόλουθες προκλήσεις:

- Αύξηση της κίνησης από κινητά.
- Αύξηση του αριθμού των συσκευών που είναι συνδεδεμένες στο δίκτυο.
- Μείωση των καθυστερήσεων στην εφαρμογή νέων υπηρεσιών.
- Έλλειψη φάσματος συχνοτήτων.

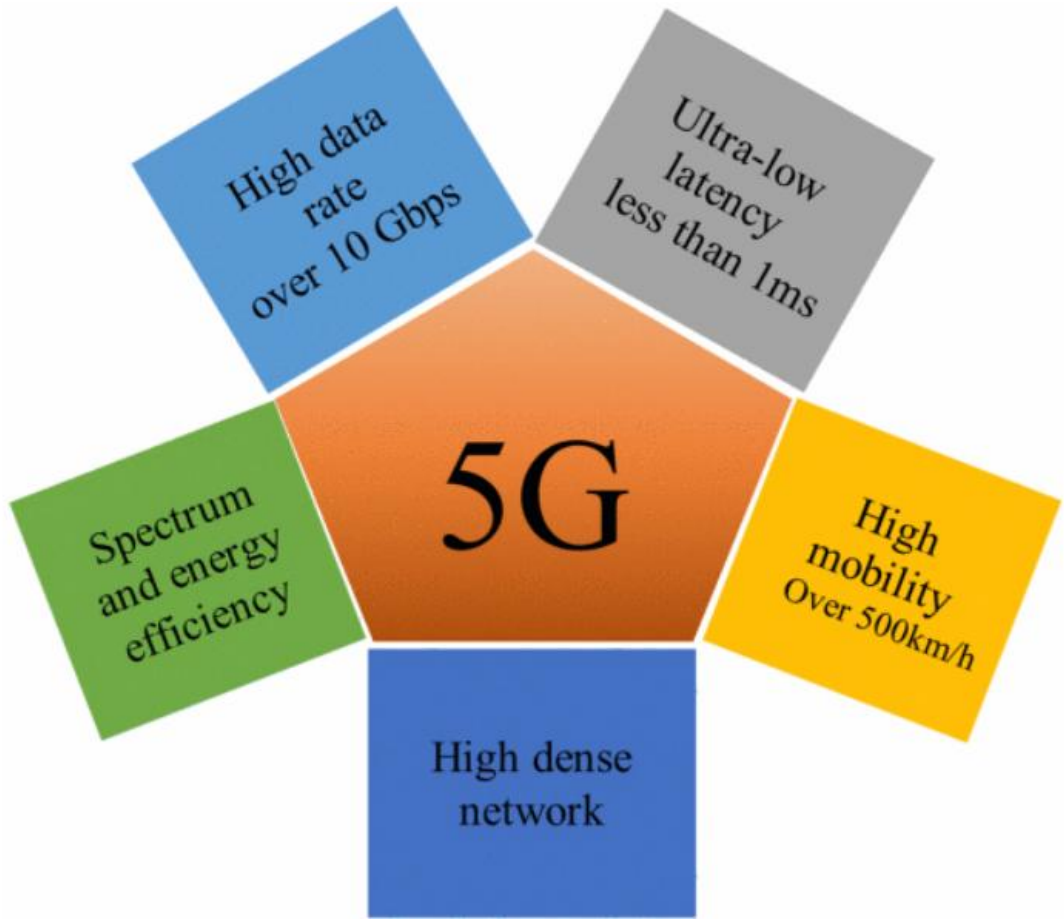
Το 5G έχει πολύ χαμηλή καθυστέρηση. Αυτή είναι μια από τις κύριες απαιτήσεις για έξυπνες εφαρμογές υγειονομικής περίθαλψης. Για παράδειγμα, για να εκτελέσετε χειρουργική επέμβαση εξ αποστάσεως στην τηλεχειρουργική, η καθυστέρηση στο δίκτυο πρέπει να είναι πολύ χαμηλή, καθώς η εσωτερική καθυστέρηση των

ρομποτικών συστημάτων μπορεί να φτάσει τα 100ms. Εάν το πρόσθετο δίκτυο έχει μεγάλη καθυστέρηση, η απομακρυσμένη χειρουργική επέμβαση θα είναι αδύνατη, καθώς οι ελάχιστες απαιτήσεις είναι μικρότερες από 200ms[32]. Το 5G, από την άλλη πλευρά, επιτρέπει την απομακρυσμένη λειτουργία καθώς έχει καθυστέρηση μικρότερη από 1ms.

Το 5G έχει υψηλό εύρος ζώνης, το οποίο επιτρέπει τη χρήση πολλών ιατρικών αισθητήρων και συστημάτων παρακολούθησης ταυτόχρονα. Ένα από τα κύρια επιτεύγματα του 5G είναι η χρήση mmWaves (κύματα υψηλής συχνότητας, άνω των 10 Ghz), η εφαρμογή των οποίων επιτρέπει την επέκταση του φάσματος και την επίτευξη υψηλού ρυθμού δεδομένων[32]. Ως αποτέλεσμα, υπάρχει μια ευκαιρία για τους γιατρούς να μοιραστούν περιεχόμενο υψηλής ποιότητας.

2.4.Ευκαιρίες και οφέλη Blockchain για την υγειονομική περίθαλψη

Το Blockchain είναι μια νέα τεχνολογία για decentralizedapps. Το Blockchain είναι ένα σύστημα ενός εύρους - ο λογαριασμός συναλλαγής λαμβάνεται από κάθε χρήστη και αναπαράγεται σε πολλούς διακομιστές χρηστών. Αυτό σημαίνει ότι δεν υπάρχει κεντρική βάση δεδομένων στο blockchain, όλα τα δεδομένα αντιγράφονται και αποθηκεύονται από τους συμμετέχοντες στο δίκτυο. Μόλις ένας από τους συμμετέχοντες προσθέσει ένα μπλοκ στο blockchain, τότε όλοι οι άλλοι χρήστες ενημερώνουν τα αρχεία τους και δεσμεύουν την αλλαγή. Αυτή η αρχιτεκτονική αποφεύγει ένα μόνο σημείο αποτυχίας[33]. Επιπλέον, το blockchain δεν μπορεί να ελεγχθεί από κανέναν συμμετέχοντα στο δίκτυο, ενώ είναι διαθέσιμο σε όλους τους συμμετέχοντες. Αυτή η ιδιότητα παρέχεται με συναίνεση όπου καθορίζονται οι κανόνες για τη χρήση του blockchain μεταξύ των συμμετεχόντων. Οι κύριες ευκαιρίες του blockchain για 5G και υγειονομική περίθαλψη δίνονται στην παρακάτω εικόνα.



Decentralized - χωρίς κεντρική διαχείριση, κάθε χρήστης διαχειρίζεται τα δικά του δεδομένα. Το blockchain δεν εξαρτάται από έναν κεντρικό έλεγχο για την εκτέλεση συναλλαγών[33]. Αντ 'αυτού, οι συμμετέχοντες στο δίκτυο υιοθετούν πρωτόκολλα συναίνεσης για την επαλήθευση των συναλλαγών. Η έλλειψη κεντρικής διαχείρισης στο blockchain αυξάνει την αποδοτικότητα ξεπερνώντας το μόνο αδύναμο σημείο του 5G. Η ικανότητα των ασθενών να διαχειρίζονται τις δικές τους πληροφορίες τους επιτρέπει να ελέγχουν όλα τα ιατρικά αρχεία.

Τα οφέλη του blockchain δικτύου, μπορεί να είναι κάποια από τα παρακάτω ή μέρος αυτών και ισχύουν τα εξής[33]:

Unchanged

Είναι σχεδόν αδύνατο να αλλάξετε οποιαδήποτε πληροφορία που έχει κατακερματιστεί στο blockchain. Κάθε συναλλαγή που περιλαμβάνεται στο μπλοκ είναι κρυπτογραφικά ασφαλισμένη χρησιμοποιώντας τη μέθοδο κατακερματισμού. Τα metadataκατακερματισμού του προηγούμενου μπλοκ περιλαμβάνονται στη λειτουργία κατακερματισμού του επόμενου, δημιουργώντας έτσι μια χρονολογική αλυσίδα μπλοκ, η αλλαγή ενός από αυτά είναι αδύνατη[34]. Τέτοια

unchangedobjectsπαρέχουν υψηλή απόδοση και ασφάλεια στη διατήρηση στατιστικών και συστήματος χρέωσης στην παροχή υπηρεσιών 5G[34]. Διασφαλίζει ότι τα ιατρικά αρχεία ασθενών, τα ιατρικά ευρήματα, τα εργαστηριακά και τα ερευνητικά αποτελέσματα είναι πάντα διαθέσιμα και προστατευμένα από χειραγώγηση.

Transparency

Οι πληροφορίες σχετικά με τις συναλλαγές και τους χειρισμούς σε κάθε μπλοκ αποθηκεύονται και είναι ορατές σε όλους τους συμμετέχοντες. Κάθε συμμετέχων έχει ίσα δικαιώματα πρόσβασης, επαλήθευσης και παρακολούθησης συναλλαγών. Τέτοιες ιδιότητες διατηρούν την ακεραιότητα του συστήματος και επιτρέπουν τη δημιουργία ανοικτών δικτύων αρχιτεκτονικής (εικονικά δίκτυα, κατανεμημένα δίκτυα) για 5G[34]. Η δυνατότητα παρακολούθησης κάθε συναλλαγής επιτρέπει τον προσδιορισμό των πηγών προέλευσης διαφόρων πλαστών προϊόντων και φαρμάκων.

SecurityandPrivacy

Η χρήση asymmetriccryptography και smart contracts εξασφαλίζει έλεγχο πρόσβασης και αποτελεσματικό έλεγχο ταυτότητας. Στο blockchain, η κρυπτογράφηση πραγματοποιείται χρησιμοποιώντας δημόσια και ιδιωτικά κλειδιά, τα οποία δημιουργούνται ως συμβολοσειρές τυχαίων αριθμών[35]. Αυτό καθιστά αδύνατο να μαντέψουμε τα ιδιωτικά κλειδιά, ακόμη και χρησιμοποιώντας τα δημόσια. Μια τέτοια κρυπτογράφηση αποτρέπει τη διαρροή δεδομένων με πολύ αξιόπιστο τρόπο.

Η ενσωμάτωση του blockchain με το 5G και το σύστημα υγειονομικής περίθαλψης μπορεί να είναι μια «θεραπεία» για 2 και 4 σημεία προβλημάτων στον χώρο της υγείας.

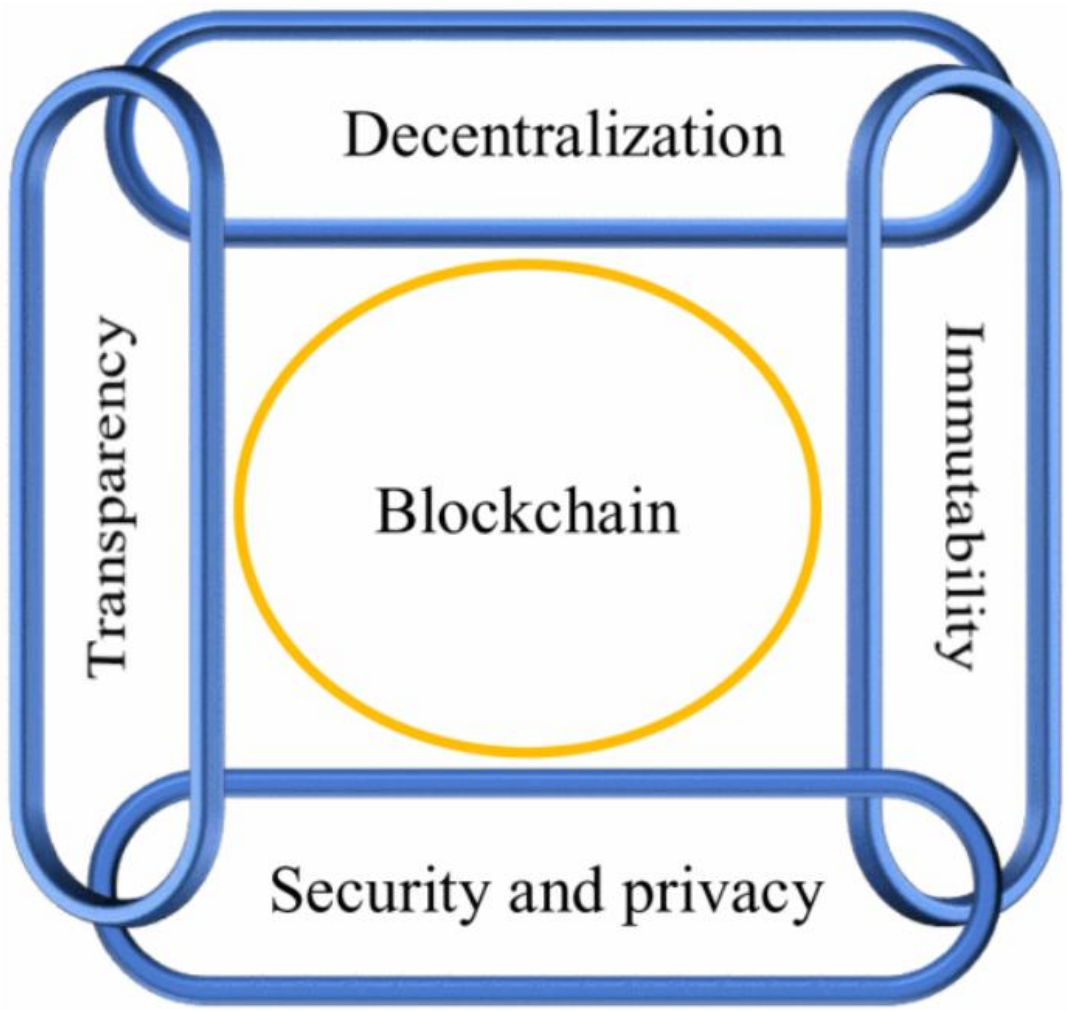
2.5.Αρχιτεκτονική βασισμένη σε Blockchain της 5G υγειονομικής περίθαλψης

Η αρχιτεκτονική υγειονομικής περίθαλψης που βασίζεται σε blockchain επιτρέπει την επίλυση πολλών προβλημάτων στο σύστημα. Η ενσωμάτωση του blockchain με το 5G βασίζεται στο γεγονός ότι το blockchain μπορεί να συνδεθεί με βασικές τεχνολογίες ειδικές για το 5G[36], όπως το NFV και το edge/cloud computing. Μια τέτοια ενσωμάτωση φαίνεται στην παρακάτω εικόνα.

Υπάρχει μια δυνατότητα επέκτασης των δυνατοτήτων επικοινωνίας με συσκευές IoT μέσω NFV, ο υπολογισμός Edge/cloud αυξάνει την ποιότητα και την ταχύτητα των υπηρεσιών για το σύστημα υγειονομικής περίθαλψης. Σε αυτή την περίπτωση, το κύριο καθήκον του blockchain είναι να δημιουργήσει μια ίση βάση δεδομένων για όλους τους χρήστες. Σε αυτή την αρχιτεκτονική, όλες οι συναλλαγές αποθηκεύονται σε αποκεντρωμένες βάσεις δεδομένων και είναι προσβάσιμες σε όλους τους συμμετέχοντες στο σύστημα (ασθενείς, γιατροί)[37].

Το 5G επιτρέπει στο δίκτυο να χωριστεί σε διαφορετικά κελιά, όπως μακρο, μικρο, pico και femto cells. Το σύστημα υγειονομικής περίθαλψης απαιτεί υψηλό ρυθμό δεδομένων. Διαχωρίζοντας το δίκτυο σε μικρότερα κελιά, είναι δυνατό να μεγιστοποιηθεί ο ρυθμός δεδομένων κάθε κυττάρου και να εφαρμοστούν πολλές εφαρμογές υγειονομικής περίθαλψης[37]. Εκτός αυτού, η διαίρεση του δικτύου παρέχει ευέλικτη κάλυψη και φασματική απόδοση.

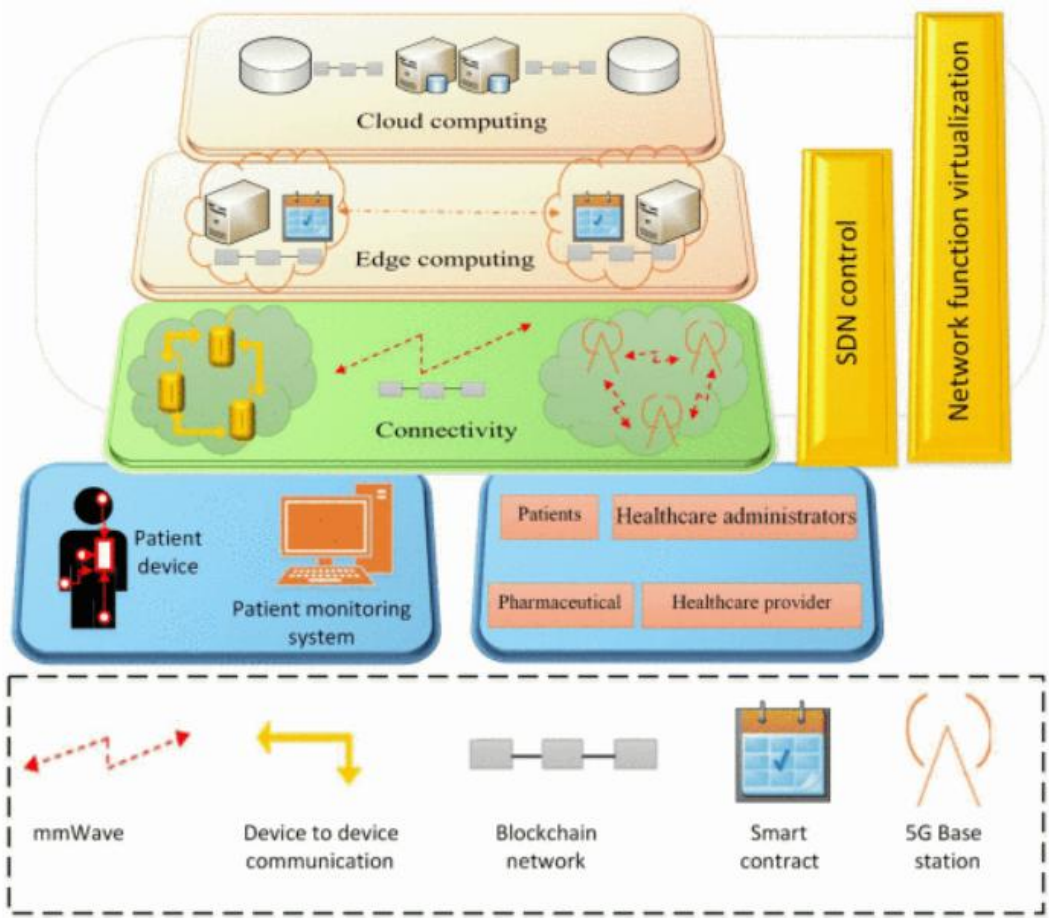
Η εφαρμογή του SDN αυξάνει την ταχύτητα και την ευελιξία του δικτύου διαχωρίζοντας το επίπεδο ελέγχου και το επίπεδο δεδομένων των μικρών κελιών. Οι τεχνολογίες δικτύου που περιλαμβάνονται στο SDN χρησιμεύουν για την υποστήριξη κέντρων δεδομένων και υποδομής εικονικού διακομιστή. Έτσι, το SDN μπορεί να υποστηρίξει αρκετές απαιτήσεις υγειονομικής περίθαλψης 5G. Επιπλέον, η χρήση του blockchain παρέχει ασφάλεια δεδομένων υγείας και διαλειτουργικότητα, έξυπνα συμβόλαια αυξάνουν την αξιοπιστία της διαδικασίας επαλήθευσης πρόσβασης.



Η τεχνολογία επικοινωνίας D2D, η οποία είναι μοναδική μόνο για το 5G, παρέχει άμεση σύνδεση συσκευών. Συνήθως, σε προηγούμενες γενιές δικτύων, όλα τα δεδομένα αποστέλλονται πρώτα στην πύλη και μέσω αυτής στο σταθμό βάσης. Ωστόσο, μια τέτοια μέθοδος επικοινωνίας θα είναι αναποτελεσματική εάν οι συσκευές διασύνδεσης βρίσκονται στην ίδια περιοχή[37], μέσα στον ίδιο σταθμό βάσης. σε αυτήν την περίπτωση, η άμεση σύνδεση των συσκευών μεταξύ τους οδηγεί σε αποτελεσματική χρήση των πόρων και αυξημένη ποιότητα. Η τεχνολογία επικοινωνίας D2D λύνει το πρόβλημα της αύξησης της πυκνότητας του δικτύου μειώνοντας τις συνδέσεις με το σταθμό βάσης σε έξυπνα συστήματα υγειονομικής περίθαλψης με πολλές συσκευές IoT. Επιπλέον, η εφαρμογή mmWaves σε μικρά κελιά επιτρέπει τη χρήση εύρους ζώνης που δεν είχαν χρησιμοποιηθεί πριν και την επίλυση προβλημάτων που σχετίζονται με την απώλεια διαδρομής. Τα κύματα mm είναι κύματα της τάξης των 20GHz έως 300GHz, με το 5G να μπορεί συνήθως να χρησιμοποιεί συχνότητες έως 90GHz[38].

Ο υπολογισμός άκρων επιτρέπει την επεξεργασία πληροφοριών στην άκρη, στην πλευρά της πηγής, γεγονός που μειώνει τον χρόνο απόκρισης του δικτύου. Στο

εγγύς μέλλον, η τεχνητή νοημοσύνη θα λάβει αποφάσεις με βάση τα ληφθέντα δεδομένα και τα καθήκοντα της υγειονομικής περίθαλψης. Σε αυτό το σενάριο, ο χρόνος απόφασης θα διαδραματίσει σημαντικό ρόλο και ο υπολογιστής αιχμής μπορεί να υποστηρίξει τέτοιες τεχνολογίες παρέχοντας επεξεργασμένα δεδομένα σε πραγματικό χρόνο[38]. Ο ρόλος του blockchain στο edge computing και στο cloud computing είναι να παρέχει ασφαλή ανταλλαγή δεδομένων μεταξύ συσκευών IoT και διακομιστών. Επιπλέον, διάφορα δεδομένα υγειονομικής περίθαλψης μπορούν να αποθηκευτούν στο cloud μέσω blockchain, γεγονός που ενισχύει περαιτέρω την ασφάλειά τους.



Η εισαγωγή υπολογιστικού Edge και επικοινωνίας D2D απαιτεί την επεξεργασία μεγάλου όγκου πληροφοριών στο Edge[38]. Για να γίνει αυτό, πολλές πρόσθετες συσκευές υλικού, συμπεριλαμβανομένων δρομολογητών, τείχους προστασίας, πρέπει να εγκατασταθούν στο άκρο του δικτύου. Η τεχνολογία NFV (Network FunctionsVirtualization) επιτρέπει την εισαγωγή συσκευών όπως εικονικών μηχανών σε συνηθισμένους διακομιστές.Η λύση σε αυτό το πρόβλημα είναι ένα δίκτυο που βασίζεται σε blockchain[39].

3.Τεχνολογία Blockchain και Crytpocurrencies

Το Blockchain είναι ένα κατανεμημένο σύστημα στο οποίο διατηρείται ένα κοινό βιβλίο συναλλαγών και μοιράζεται μεταξύ των συμμετεχόντων στο δίκτυο. Οι συναλλαγές διατηρούνται με τη μορφή αλυσίδας μπλοκ όπου κάθε μπλοκ αναφέρεται στο προηγούμενο μπλοκ χρησιμοποιώντας μια τιμή κατακερματισμού. Οι συμμετέχοντες πρέπει να συμφωνήσουν σε μια λίστα συναλλαγών[40]. Κάθε κόμβος έχει μια τοπική κατάσταση blockchain που μπορεί να διαφέρει από κόμβο σε κόμβο. Οι localstatusθα είναι διαφορετικές όταν δύο ή περισσότεροι κόμβοι θα εξορύσσουν ταυτόχρονα δύο διαφορετικά μπλοκ. Σε αυτή την περίπτωση, δύο μπλοκ θα δείχνουν το ίδιο προηγούμενο μπλοκ[41]. Η globalstatus ενός blockchain δημιουργείται με την ένωση όλων των localstates. Σε μιαglobalstate, το σημείο στο οποίο διαφορετικά μπλοκ έχουν το ίδιο προηγούμενο μπλοκ. Για να επιλύσετε το δίκτυο, διάφορες εφαρμογές του blockchain, όπως το Bitcoin και το Ethereum χρησιμοποιούν διαφορετικούς μηχανισμούς για να προσδιορίσουν τον κύριο κλάδο του blockchain[42]. Το Bitcoin επιλύει το πρόβλημα θεωρώντας έναν βαθύτερο κλάδο ως κύριο κλάδο του blockchain. Χρησιμοποιεί το πρωτόκολλο συναίνεσης του Nakamoto για το σκοπό αυτό. Ο κύριος κλάδος επιλέγεται ως κλάδος που έχει τον μεγαλύτερο αριθμό κόμβων[42]. Από την άλλη πλευρά, ένας αλγόριθμος συναίνεσης στο Ethereum, Greedy Heaviest Observation Subtree (GHOST) επιλέγει το βαρύτερο υποδέντρο ως κύριο κλάδο[42].

Στο Bitcoin ή σε οποιοδήποτε άλλο κρυπτονόμισμα, μια συναλλαγή είναι μια ατομική πράξη που αντιπροσωπεύει τη μεταφορά χρημάτων από τον αποστολέα στον παραλήπτη. Ένα δημόσιο κλειδί και μια ψηφιακά υπογεγραμμένη τιμή κατακερματισμού της προηγούμενης συναλλαγής ορίζει μια τρέχουσα συναλλαγή σε bitcoin[43]. Μια συναλλαγή προσδιορίζεται από την αξία κατακερματισμού της. Για την ψηφιακή υπογραφή της συναλλαγής, χρησιμοποιείται ένα ιδιωτικό κλειδί. Το δημόσιο κλειδί χρησιμοποιείται για την επαλήθευση της συναλλαγής. Κάθε κόμβος σε αυτό το δίκτυο από ομότιμους χρήστες διαθέτει ένα αντίγραφο του καθολικού. Εάν ο χρήστης Α θέλει να μεταφέρει κάποια κέρματα σε άλλο χρήστη Β, πρέπει να ανακοινώσει αυτήν τη συναλλαγή δημοσίως[43]. Στη συνέχεια, το δίκτυο επαληθεύει την ορθότητα αυτής της συναλλαγής. Για να διασφαλιστεί η συνέπεια, η έξοδος μιας συναλλαγής δεν πρέπει να χρησιμοποιείται ως είσοδος από ολόκληρο το blockchain περισσότερες από μία φορές. Εάν η έξοδος αναφέρεται περισσότερες από μία φορές, αυτό οδηγεί σε πρόβλημα διπλών δαπανών που απαγορεύεται αυστηρά στο δίκτυο[44].

Το Ethereum προτείνεται από τον Vitalik Buterin για την αντιμετώπιση των περιορισμών στο Bitcoin. Τα μπλοκ στο Ethereum περιέχουν επίσης μια λίστα συναλλαγών και την πιο πρόσφατη κατάσταση. Εκτός από τη μεταφορά χρημάτων, το Ethereum διασφαλίζει επίσης την εκτέλεση έξυπνων συμβάσεων. Χρησιμοποιεί το πρωτόκολλο GHOST για να εξασφαλίσει consentστο δίκτυο. Αντιμετωπίζει το ζήτημα των παλαιών μπλοκ που προκύπτουν όταν μια ομάδα μπλοκ που διαθέτουν περισσότερη υπολογιστική ισχύ από τους υπόλοιπους και έτσι συμβάλλουν περισσότερο στο δίκτυο. Αυτό θα οδηγήσει σε ζήτημα συγκεντρωτισμού.

Το πρωτόκολλο GHOST ενσωματώνει τα παλιά μπλοκ στον μεγαλύτερο υπολογισμό blockchain[45]. Τα παλαία μπλοκ επιβραβεύονται που εξαλείφουν το ζήτημα συγκεντρωτισμού. Οι κόμβοι ανταμείβονται τώρα ακόμα κι αν δεν έχουν καταφέρει να είναι μέρος του κύριου blockchain. Σε σύγκριση με το Bitcoin, το Ethereum έχει καλύτερο χρόνο αποκλεισμού (15 δευτερόλεπτα). Έχει ρυθμό επεξεργασίας συναλλαγών 11 ανά δευτερόλεπτο. Εκτιμάται ότι η κατανάλωση ενέργειας του Ethereum ανά συναλλαγή είναι περίπου 49 KWh[45].

3.1.Συγκριτική ανάλυση των αλγόριθμων συναίνεσης στο blockchain

Αυτή η ενότητα συζητά τις παραμέτρους που σχετίζονται με την αξιολόγηση των consentαλγορίθμων στο blockchain. Ο τύπος blockchain, ο ρυθμός συναλλαγών, η επεκτασιμότητα, το μοντέλο ανοχής αντίπαλου, η πειραματική ρύθμιση, ο λανθάνων χρόνος, η απόδοση, το εύρος ζώνης, το μοντέλο επικοινωνίας, η πολυπλοκότητα της επικοινωνίας, οι επιθέσεις, η κατανάλωση ενέργειας, η εξόρυξη, η κατηγορία συναίνεσης και η τελική συναίνεση προσδιορίζονται ως κρίσιμες παράμετροι για τη σύγκριση των διαφόρων consentαλγόριθμοι για το blockchain[46]. Συγκριτικήανάλυσηορισμένωναλγορίθμωνπουπροτάθηκανπρόσφατα: ELASTICO, Byzantine consensus without leaders, Silent consensus,Blockchain with unlimited scalability, Proof of Trust (PoT), Delegated Byzantine Fault Tolerance (DBFT) consensus, Proof of Proof of Work (PoPF), Ripple, Proof of Stake (PoS) καιProof of Work (PoW) εκτελούνται. Οι προσδιορισμένες παράμετροι και η σύγκριση των αλγόριθμων συναίνεσης ως προς αυτούς παρουσιάζονται ως παρακάτω.

• Τύπος Blockchain

Υπάρχουν τρεις τύποι blockchain, δημόσιο, ιδιωτικό και κοινοπραξία. Ο τύπος του blockchain καθορίζει τον έλεγχο συμμετοχής στον αλγόριθμο συναίνεσης. Αυτό πρέπει να ληφθεί υπόψη κατά την αξιολόγηση των αλγόριθμων συναίνεσης για να

ελέγξετε τι είδους συμμετοχή υποτίθεται στο σχεδιασμό[46]. Ο τύπος του blockchain πρέπει να επιλέγεται σύμφωνα με τη φύση της επιχειρηματικής εφαρμογής.

• Επεκτασιμότητα

Η επεκτασιμότητα είναι μια βασική απαίτηση για την αντιμετώπιση μεγάλων δεδομένων στο σημερινό περιβάλλον. Η επεκτασιμότητα επιτυγχάνεται εάν η αύξηση του αριθμού των κόμβων έχει ως αποτέλεσμα την επεξεργασία περισσότερων μπλοκ συναλλαγών[47]. Η απόδειξη εμπιστοσύνης και το ELASTICO είναι κλιμακούμενα. Η σιωπηρή συναίνεση και το PoW δεν είναι επεκτάσιμες λύσεις. Άλλοι αλγόριθμοι που εμπλέκονται σε συγκρίσεις δεν έχουν ακόμη δοκιμαστεί ως προς την επεκτασιμότητά τους.

• Μοντέλο Ανεκτικότητας Αντίπαλου

Το αντίπαλο μοντέλο ελέγχει το κλάσμα του δικτύου blockchain που μπορεί να αντέξει την αποτυχία ή την επίθεση χωρίς να επηρεάσει τη συναίνεση. Ο αλγόριθμος που προτείνεται για συναίνεση στο blockchain έρχεται με τιμή κατωφλίου (threshold) για αυτό το αντίπαλο μοντέλο[47]. Η υψηλότερη τιμή για το όριο του αντιπάλου είναι καλύτερη. Το ELASTICO έχει τον καλύτερο αντίπαλο έλεγχο από τους υπόλοιπους αλγόριθμους.

• Παράμετροι που σχετίζονται με την απόδοση

Ορισμένοι από τους υπάρχοντες αλγόριθμους συναίνεσης δεν αξιολογούνται πειραματικά. Συγκρίνονται μόνο θεωρητικά χρησιμοποιώντας αποδείξεις ορθότητας. Ωστόσο, μαζί με αυτό υπάρχει ανάγκη να υπάρχει μια ποσοτική ανάλυση που να εξετάζει την απόδοση και την ασφάλεια αυτών των αλγόριθμων συναίνεσης. Η καθυστέρηση, η απόδοση και το εύρος ζώνης είναι οι τρεις βασικές πτυχές απόδοσης στις οποίες πρέπει να επικεντρωθούμε για καθένα από τους αλγόριθμους συναίνεσης[47]. Εκτός από το ELASTICO, άλλοι αλγόριθμοι δεν αξιολογούνται πειραματικά ως προς αυτές τις πτυχές απόδοσης.

• Μοντέλο επικοινωνίας και πολυπλοκότητα

Σε σύγχρονη επικοινωνία, ο αποστολέας περιμένει τον παραλήπτη να αναγνωρίσει το αίτημα. Στην ασύγχρονη επικοινωνία, ο αποστολέας δεν χρειάζεται να περιμένει την απάντηση από τον παραλήπτη και να συνεχίσει την επικοινωνία. Για εφαρμογές σε πραγματικό χρόνο που δεν μπορούν να αντέξουν καθυστερήσεις, μπορούν να ληφθούν υπόψη τα PoW, PoT, Ripple και η σιωπηρή συναίνεση. Εάν αναμένονται περισσότερες λειτουργίες ανάγνωσης σε μια εφαρμογή, τότε πρέπει να επιλεγεί

σύγχρονο μοντέλο, καθώς δίνει άμεση απόκριση. Ο αλγόριθμος ELASTICO και ο ηγέτης χωρίς συναίνεση έχει μοντέλο σύγχρονης επικοινωνίας που υποτίθεται στο σχεδιασμό αλγόριθμου συναίνεσης[48]. Ο αλγόριθμος Leader χωρίς συναίνεση έχει γραμμικό και καλύτερο κόστος επικοινωνίας από το ELASTICO και το PoT. Το κόστος επικοινωνίας των υπολοίπων αλγορίθμων δεν έχει αναλυθεί ακόμη στη βιβλιογραφία.

• Επιθέσεις

Το Ripple είναι επιρρεπές σε επίθεση Sybil στην οποία ένας εισβολέας ελέγχει πολλούς κόμβους δικτύου δημιουργώντας διαφορετικές διευθύνσεις IP, εικονικές μηχανές και λογαριασμούς χρηστών. Οδηγός χωρίς συναίνεση, οι PoT είναι ασφαλείς απέναντι σε αυτήν την επίθεση[48]. Οι αλγόριθμοι δεν αξιολογούνται και αναλύονται σε σχέση με τον αριθμό των επιθέσεων ασφαλείας που είναι δυνατές σε ένα δίκτυο blockchain. Είναι σημαντικό να αναθεωρηθούν οι αλγόριθμοι όσον αφορά τις επιθέσεις ασφαλείας.

• Κατανάλωση ενέργειας

Η κατανάλωση ενέργειας καθορίζει την ποσότητα ενέργειας ή ηλεκτρικής ενέργειας που καταναλώνει η υποδομή υλικού στο δίκτυο blockchain. Η κατανάλωση ενέργειας σχεδόν όλων των συναινετικών αλγορίθμων δεν αξιολογείται πειραματικά.

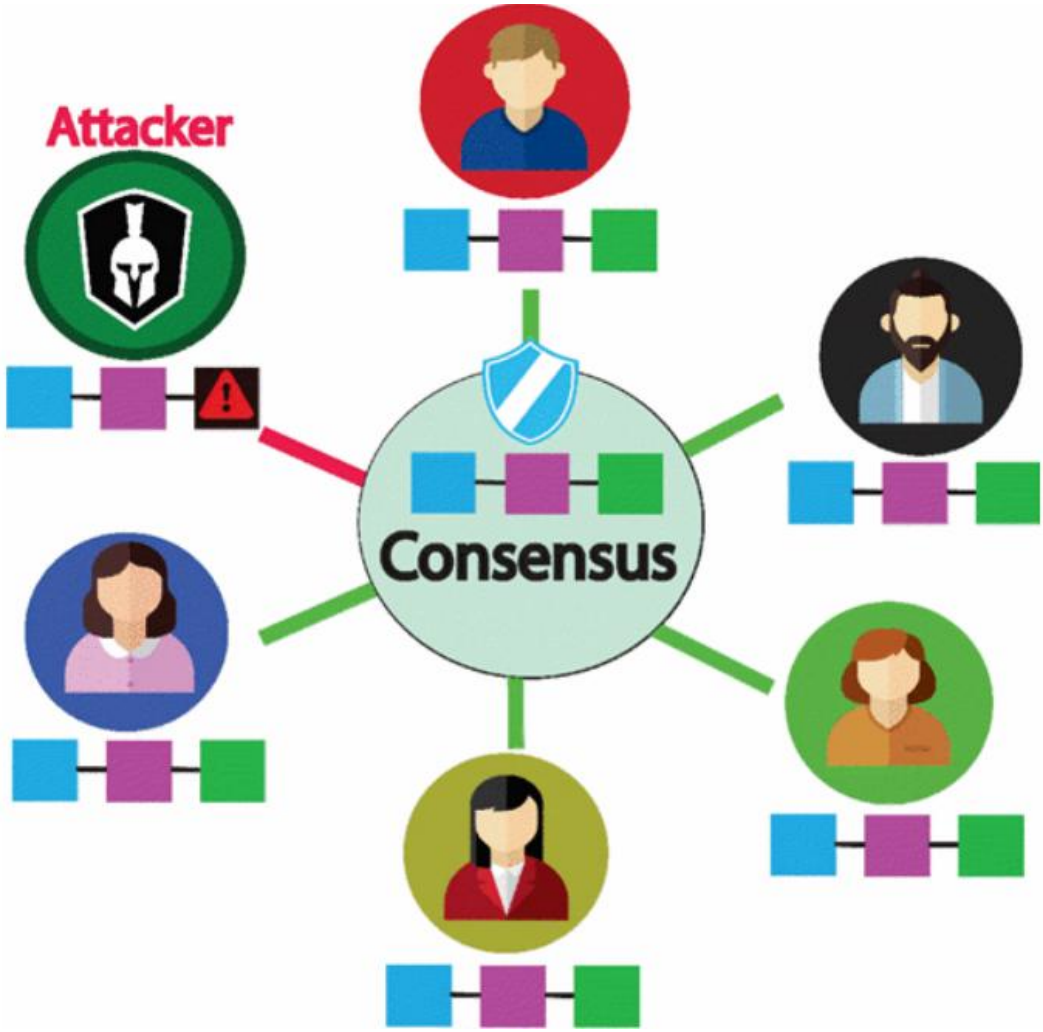
• Κατηγορία εξόρυξης και συναίνεσης

Καθορίζει τον τρόπο με τον οποίο πραγματοποιείται η διαδικασία εξόρυξης στο δίκτυο blockchain. Συνδέεται στενά με το πώς συμβαίνει η διαδικασία επαλήθευσης. Η συναίνεση που βασίζεται σε αποδείξεις είναι ιδανική για δίκτυα με μεγάλο αριθμό κόμβων. Η συναίνεση βάσει ψήφου, από την άλλη πλευρά, λειτουργεί καλύτερα με περιορισμένο αριθμό κόμβων[49]. Εάν το δίκτυο έχει μεγάλο αριθμό κόμβων, είναι προτιμότερο να χρησιμοποιείτε ELASTICO, PoW, PoPF και σιωπηρή συναίνεση. Σε άλλη περίπτωση, τα υπόλοιπα πρωτόκολλα συναίνεσης (που περιλαμβάνονται στη σύγκριση) θα ταίριαζαν καλύτερα[49].

3.2.Συμφωνία σε Κατανεμημένα Συστήματα και Blockchain

Η συναίνεση είναι μια βασική έννοια στα κατανεμημένα συστήματα και δεν περιορίζεται στο blockchain. Ισχύει για σενάρια στα οποία πολλές διαδικασίες ή κόμβοι πρέπει να διατηρούν μια κοινή κατάσταση του στοιχείου δεδομένων. Το blockchain χωρίς άδεια και με άδεια είναι δύο κύριοι τύποι blockchain. Στο blockchain

χωρίς άδεια, οι κόμβοι είναι ανώνυμοι. Μπορεί να προστεθεί ένα νέο παραβιασμένο μπλοκ συναλλαγών με αποτέλεσμα ένα κίνδυνο[50]. Το Fork συμβαίνει όταν μια έγκυρη συναλλαγή δεν ταιριάζει με τη μη έγκυρη. Ο πρωταρχικός στόχος του αλγόριθμου συναίνεσης είναι να επιτευχθεί συμφωνία μεταξύ των κόμβων έτσι ώστε κάθε κόμβος να συμφωνεί σε μία πραγματική τιμή. Στο blockchain με άδεια, οι κόμβοι δεν είναι ανώνυμοι και θεωρούνται ως γνωστές οντότητες[50].



Αποτυχία ασφαλείας

Οι αστοχίες ασφαλείας προκαλούνται ως αποτέλεσμα επιθέσεων ασφαλείας και πλαστοπροσωπίας. Τα δεδομένα ενδέχεται να καταστραφούν εξαιτίας αυτού.

Βλάβη λογισμικού

Οι αστοχίες του λογισμικού οφείλονται σε ελαττώματα σχεδιασμού και μοντελοποίησης. Αυτός ο τύπος βλάβης μπορεί να προκαλέσει άλλου τύπου αστοχίες, όπως συντριβή ή παράλειψη.

3.4.Αλγόριθμοι συναίνεσης υψηλού επιπέδου

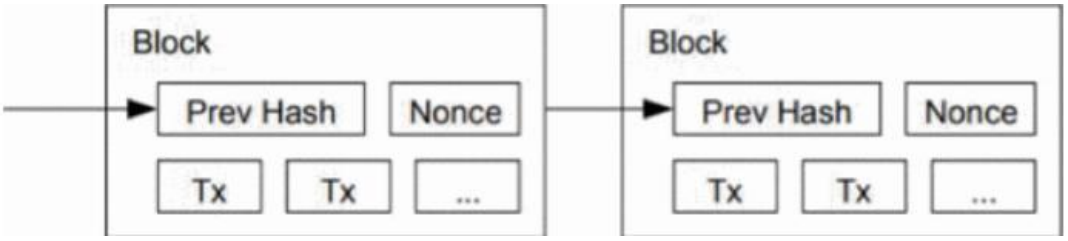
Δεδομένου ότι υπάρχουν σήμερα πάνω από 1.500 ενεργά κρυπτονομίσματα (δηλαδή ενεργά εμπορεύσιμα στην παγκόσμια αγορά) και είναι πιθανό να δημιουργηθεί ένα νέο κρυπτονόμισμα ανά πάσα στιγμή, το «υψηλού κύρους» σε αυτό το πλαίσιο καθορίζεται από το όριο αγοράς ενός κρυπτονομίσματος[51]. Παρόλο που οι τιμές της αγοράς κρυπτονομισμάτων βρίσκονται σε συνεχή ροή, αυτό το σχήμα κατάταξης καθορίστηκε ως το πιο δίκαιο στην παραγγελία των νομισμάτων (και των αλγορίθμων πίσω από αυτά).

Currency Name	Consensus Algorithm	Market Cap
Bitcoin	Proof of Work	$ 157.3 B
Ethereum	Proof of Work[1]	$ 95.7 B
Ripple	Ripple Protocol Consensus Algorithm	$ 37.1 B
Bitcoin Cash	Proof of Work	$ 21.4 B
Cardano	Proof of Stake	$ 11.8 B
Stellar	Stellar Consensus Protocol	$ 8.3 B
NEO[2]	Delegated Byzantine Fault Tolerance	$ 8.2 B
Litecoin	Proof of Work	$ 8.1 B
EOS	Delegated Proof of Stake	$ 6.5 B
NEM	Proof of Importance	$ 5.7 B

1. Planned switch to Proof of Stake sometime in 2018
2. Formerly known as Antshares

Α. Απόδειξη εργασίας (PoW)

Σύμφωνα με τη λευκή βίβλο Bitcoin, το σύστημα PoW λειτουργεί με σάρωση για μια τιμή που, όταν κατακερματιστεί, έχει ένα hash ξεκινώντας με έναν αριθμό μηδενικών bit. Αυτό επιτυγχάνεται προσθέτοντας ένα nonce (θέτοντας σε λειτουργία) στην αρχική τιμή έως ότου προκύπτουν hash και ξεκινήσουν με τον απαιτούμενο αριθμό μηδενικών bit. Μόλις βρεθεί αυτό το μηδενικό και ικανοποιηθεί η απόδειξη εργασίας[51], το μπλοκ δεν μπορεί να αλλάξει χωρίς να επαναλάβετε την εργασία για το συγκεκριμένο μπλοκ και όλα τα μπλοκ που ακολουθούν.



Όπως φαίνεται στο σχήμα παραπάνω, όλα τα μπλοκ, με εξαίρεση το πρώτο μπλοκ που δημιουργήθηκε από το σύστημα (το «μπλοκ γένεσης»), έχουν έναν κατακερματισμό που αποτελείται από τον κατακερματισμό του προηγούμενου μπλοκ παράλληλα με το μη απαιτούμενο για τη δημιουργία των απαραίτητων μηδενικών bit[51]. Το μπλοκ γένεσης είναι μια εξαίρεση καθώς δεν έχει προηγούμενο μπλοκ στο οποίο πρέπει να επισημανθεί: το hash του είναι εντελώς μηδενικό.

Β. Ripple Protocol Consensus Algorithm (RPCA)

Όπως υποδηλώνει το όνομα, ο αλγόριθμος RPCA είναι ένας αλγόριθμος συναίνεσης που χρησιμοποιείται αποκλειστικά από το κρυπτονόμισμα Ripple και αναπτύχθηκε ειδικά για την αντιμετώπιση προβλημάτων καθυστέρησης που υπάρχουν σε άλλους αλγόριθμους. Όπως ορίζεται στη λευκή βίβλο, το RPCA λειτουργεί ως εξής[52]:

- Κάθε διακομιστής λαμβάνει όλες τις έγκυρες συναλλαγές που έχει δει πριν από έναν νέο γύρο συναίνεσης και τις τοποθετεί σε μια δημόσια λίστα που ονομάζεται "σύνολο υποψηφίων".
- Κάθε διακομιστής συνδυάζει όλα τα υποψήφια σύνολα που βρίσκονται στη "Λίστα μοναδικών κόμβων", που είναι ένα σύνολο άλλων διακομιστών Ripple στους οποίους ο διακομιστής διατηρούσε αναφορά.
- Κάθε διακομιστής ψηφίζει για την ακρίβεια κάθε συναλλαγής σε μια σειρά από έναν ή πολλούς γύρους.
- Όλες οι συναλλαγές που συγκεντρώνουν τουλάχιστον 80% «ναι» στον τελευταίο γύρο γράφονται στο δημόσιο βιβλίο και το βιβλίο κλείνει.

Γ. PoS

1) Πρωτότυπη απόδειξη πονταρίσματος

Πρώτη εφαρμογή το 2012 με τη μορφή του κρυπτονομίσματος PeerCoin, το Proof of Stake (PoS) είναι υβριδικού σχεδιασμού, όπου το PoW χρησιμοποιείται για την αρχική κοπή νομισμάτων και το PoS στη συνέχεια χρησιμοποιείται για το μεγαλύτερο

μέρος της ασφάλειας του δικτύου. Μέσα σε ένα σύστημα PoS, η ηλικία κάθε νομίσματος λαμβάνεται υπόψη με τη μορφή "ημερών νομισμάτων". Αυτή η έννοια εξηγείται απλά μέσω παραδείγματος: το να κρατάς 10 νομίσματα για 10 ημέρες ισοδυναμεί με 100 ημέρες νομισμάτων[53]. Με τη δαπάνη αυτών των κερμάτων σε μια συναλλαγή, η ηλικία των κερμάτων καταναλώνεται και μηδενίζεται. Σε αντίθεση με ένα σύστημα PoW, όπου η αλυσίδα με την περισσότερη εργασία θεωρείται η κύρια αλυσίδα, ένα σύστημα PoS χρησιμοποιεί την αλυσίδα με την υψηλότερη ηλικία κατανάλωσης νομισμάτων.

D. Stellar Consensus Protocol (SCP)

Το Stellar Consensus Protocol (SCP), είναι ένα decentralizedπρωτόκολλο συναίνεσης όπου οι κόμβοι μέσα στο δίκτυο δεν χρειάζεται να εμπιστεύονται το σύνολο του δικτύου αλλά, μάλλον, έχουν τη δυνατότητα να επιλέξουν τους κόμβους που εμπιστεύονται. Αυτή η ομάδα κόμβων που εμπιστεύονται ο ένας τον άλλον αναφέρεται ως «φέτα απαρτίας», μια έννοια που εισήχθη για πρώτη φορά από αυτό το πρωτόκολλο[53]. Μια «απαρτία» είναι ένα σύνολο κόμβων επαρκών για την επίτευξη συμφωνίας, ενώ ένα κομμάτι απαρτίας είναι ένα υποσύνολο απαρτίας που πείθει έναν συγκεκριμένο κόμβο συμφωνίας.

Το SCP ξεκινά με ένα «πρωτόκολλο υποψηφιότητας» προτείνοντας νέες, υποψήφιες τιμές για συμφωνία. Κάθε κόμβος που λαμβάνει αυτές τις τιμές θα ψηφίσει για μία μόνο τιμή μεταξύ αυτών, η οποία τελικά έχει ως αποτέλεσμα μια τιμή να κερδίσει την πλειοψηφία. Μετά την επιτυχή εκτέλεση του πρωτοκόλλου υποψηφιότητας, αναπτύσσεται το «πρωτόκολλο ψηφοφορίας». Κατά τη διάρκεια αυτής της φάσης, οι κόμβοι ξεκινούν την ψηφοφορία σχετικά με το αν θα διαπραγματευτούν ή όχι οι τιμές που επιλέχθηκαν κατά την προηγούμενη φάση[53]. Σε περίπτωση που ένα σύνολο κόμβων δεν μπορεί να επιτύχει συναίνεση, η τιμή μεταφέρεται σε ψηφοδέλτιο υψηλότερης αξίας για να ψηφιστεί ξανά.

E. Εξουσιοδοτημένη απόδειξη συμμετοχής (dPOS)

Μέσα σε ένα σύστημα εξουσιοδότησης απόδειξης συμμετοχής (dPOS), τα ενδιαφερόμενα μέρη ψηφίζουν για την εκλογή οποιουδήποτε αριθμού μαρτύρων για τη δημιουργία μπλοκ. Κατά τη διάρκεια κάθε διαστήματος συντήρησης, η λίστα των μαρτύρων ανακατεύεται και κάθε μάρτυρας έχει τη σειρά να παράγει ένα μπλοκ στο σταθερό πρόγραμμα ενός τεμαχίου ανά αριθμός δευτερολέπτων (όπου εξαρτάται από την υλοποίηση)[53]. Οι μάρτυρες πληρώνονται για κάθε μπλοκ που παράγεται. Ωστόσο, εάν ένας μάρτυρας αποτύχει να δημιουργήσει ένα μπλοκ μετά την εκλογή του, μπορεί να ψηφιστεί στις μελλοντικές εκλογές.

Ειδικά για το blockchain EOS, τα μπλοκ παράγονται κάθε τρία δευτερόλεπτα από εξουσιοδοτημένους παραγωγούς και, ανά 21 μπλοκ, ο κατάλογος των εν λόγω παραγωγών ανακατεύεται. Εάν ένας παραγωγός δεν παρήγαγε κανένα μπλοκ μέσα στις τελευταίες 24 ώρες[53], αφαιρείται από την εξέταση μέχρι να ενημερώσει το blockchain για την πρόθεσή του να ξεκινήσει ξανά την παραγωγή μπλοκ.

ΣΤ. Απόδειξη Σημασίας (PoI)

Η απόδειξη σημασίας (PoI) χρησιμοποιείται στο δίκτυο NEM (New EconomyMovement), το οποίο χρησιμοποιεί ένα υποκείμενο κρυπτονόμισμα που ονομάζεται XEM. Κάθε λογαριασμός στο δίκτυο NEM έχει ένα υπόλοιπο XEM που χωρίζεται σε δύο μέρη: κατοχυρωμένο και μη επενδυμένο. Κάθε φορά που ένας λογαριασμός λαμβάνει XEM, αυτό το νέο XEM προστίθεται στο μη επενδυμένο υπόλοιπο του λογαριασμού. Το ένα δέκατο του αδιάθετου υπολοίπου κάθε λογαριασμού μεταφέρεται στο κατοχυρωμένο τμήμα κάθε 1440 μπλοκ[53]. Επιπλέον, όταν ένας λογαριασμός αποστέλλει XEM, το XEM λαμβάνεται τόσο από τα κατοχυρωμένα όσο και από τα μη επενδυμένα υπόλοιπα προκειμένου να διατηρηθεί ο ίδιος λόγος κατοχυρωμένου προς μη επενδυμένο.

Για να είναι ένας λογαριασμός επιλέξιμος για έναν "Υπολογισμό Σημασίας" πρέπει να κατέχει τουλάχιστον 10.000 κατοχυρωμένα XEM. Δεδομένης της επιλεξιμότητας, η σημασία υπολογίζεται με βάση το ποσό της κατοχυρωμένης XEM[54], την κατάταξη του λογαριασμού εντός του δικτύου (που βρέθηκε χρησιμοποιώντας τον αλγόριθμο NCDawareRank), συντελεστής στάθμισης με βάση την τοπολογική τοποθεσία του λογαριασμού (όπως, ο λογαριασμός είναι ένα ακέραιο ή μέρος ενός συμπλέγματος κόμβων) και δύο κατάλληλες σταθερές που καθορίζονται από το δίκτυο NEM.

3.4.1.Συγκρίσεις αλγορίθμων συναίνεσης υψηλού επιπέδου

Ο Πίνακας παρακάτω δείχνει μια βασική σύγκριση μεταξύ διαφόρων αλγορίθμων όπως παρέχεται. Σημειώστε ότι στην *εξοικονόμηση ενέργειας* δίνεται μόνο μια ασαφής ναι-όχι-μερική απάντηση, καθώς είναι αδύνατο να δοθούν ακριβείς αριθμοί για το πόση ενέργεια χρησιμοποιεί κάθε εφαρμογή λόγω συγκεχυμένων παραγόντων όπως η απόδοση και ο τύπος του επεξεργαστή[55]. Ο πιο παρακάτω Πίνακας, δείχνει πληροφορίες για αλγόριθμους που δεν περιλαμβάνονται.

Algorithm Name					
Property	***PoW***	***PoS***	***PBFT***[1]	***DPoS***	***Ripple***
Energy Saving	No	Partial	Yes	Partial	Yes
Tolerated power of adversary	< 25% computing power	<51% stake	< 33.3% replicas	< 51% validators	<20% faulty nodes

1. Practical Byzantine Fault Tolerance

Algorithm Name			
Property	***DBFT***	***SCP***	***PoI***
Energy Saving	Yes	Yes	Yes
Tolerated power of adversary	< 33.3% replicas	Variable	<50% importance

3.5.Υποψήφιοι αλγόριθμοι συναίνεσης

Τα ζητήματα ισχύος που υπάρχουν στα συστήματα PoW δεν έχουν περάσει απαρατήρητα. Υπάρχουν προς το παρόν πολυάριθμα εναλλακτικά πρωτόκολλα που δεν έχουν ακόμη κυκλοφορήσει ακόμη δημόσια. Παρ 'όλα αυτά, αυτά παρέχουν ενδιαφέρουσες πληροφορίες για το πώς η κοινότητα ανάπτυξης blockchain προσπαθεί να βελτιώσει τα ελαττώματα στις τρέχουσες εφαρμογές[57]. Για λόγους συντομίας, μόνο δύο τέτοιοι υποψήφιοι αλγόριθμοι συζητούνται εδώ.

Α. Απόδειξη της τύχης (PoL)

Επί του παρόντος, ακόμη ως απόδειξη της ιδέας, η λευκή βίβλος (Proof of Luck) αναφέρει ότι ο στόχος αυτού του νέου συστήματος είναι να μειώσει τις μεγάλες ποσότητες υπολογιστικής ισχύος που απαιτούνται από το PoW και να αυξήσει την απόδοση των συναλλαγών[57]. Μέσα σε αυτό το σύστημα, σε κάθε μπλοκ αποδίδεται μια τιμή "τύχης" καθώς εξορύσσεται, ο οποίος είναι ένας τυχαίος αριθμός μεταξύ μηδέν και ενός: οι μεγαλύτεροι αριθμοί είναι πιο τυχεροί και οι μικρότεροι αριθμοί είναι άτυχοι. Οι κόμβοι που εργάζονται για την επαλήθευση συναλλαγών εντός του δικτύου θα προτιμήσουν να προσθέσουν το μπλοκ τους στην αλυσίδα με την υψηλότερη τιμή τύχης, η οποία υπολογίζεται αθροίζοντας όλες τις τιμές τύχης που περιέχονται σε κάθε μπλοκ της αλυσίδας ξεκινώντας από το μπλοκ γένεσης έως την τελευταία συναλλαγή.

Πριν ολοκληρωθεί η εξόρυξη και η απόδειξη του μπλοκ μεταδοθεί στο δίκτυο, επιβάλλεται καθυστέρηση με βάση την τυχαία τιμή τύχης του μπλοκ που εξορύσσεται: υψηλότερη τιμή τύχης που ισοδυναμεί με μικρότερο χρόνο καθυστέρησης[58]. Αυτή η καθυστέρηση βελτιστοποιεί την επικοινωνία δικτύου μέσα στο σύστημα καθώς, εάν κάποιος άλλος ανθρακωρύχος λύσει την απόδειξη πρώτα σε ένα μπλοκ με υψηλότερη τιμή τύχης, ο αρχικός ανθρακωρύχος δεν θα χρειαστεί να μεταδώσει το μπλοκ του στο δίκτυο.

Β. Απόδειξη eXercise (PoX)

Σε αντίθεση με το Proof of Luck, το οποίο στοχεύει στη μείωση της υπολογιστικής ισχύος που απαιτείται από ένα σύστημα Proof of Work, το Proof of eXercise στοχεύει να κατευθύνει την υπολογιστική ισχύ προς επιστημονικά προβλήματα σε πραγματικό κόσμο. Η λευκή βίβλος PoX περιγράφει ένα σύστημα όπου οι κόμβοι θα αντιμετωπίζουν προβλήματα που βασίζονται σε πίνακες που παρέχονται από τους λεγόμενους «εργοδότες» μέσα στο σύστημα[58]. Το σκεπτικό για τη χρήση πινάκων είναι διπλό: οι μήτρες είναι σύνθετες, επιτρέποντας ευκολότερο συντονισμό της δυσκολίας του δικτύου και οι πίνακες αποτελούν βασική αφαίρεση για πολλά επιστημονικά υπολογιστικά προβλήματα. Η λευκή βίβλος παρέχει τα ακόλουθα προβλήματα ως παραδείγματα: αλληλουχία DNA και RNA, ανάλυση δομής πρωτεΐνης, εξόρυξη δεδομένων, ανίχνευση προσώπου και άλλα.

Καθώς τα απαιτούμενα δεδομένα για αυτά τα προβλήματα μήτρας πρέπει να αποθηκεύονται και να είναι άμεσα διαθέσιμα, με κόστος, από έναν εργοδότη στο δίκτυο, τίθεται σε εφαρμογή ένα σύστημα «πίστωσης ομήρων». Για να λάβει ένας κόμβος ένα πρόβλημα που πρέπει να λύσει, πρέπει πρώτα να «υποβάλει προσφορά» σε αυτό το πρόβλημα[58], βάζοντας μια κατάθεση που θα επιστραφεί όταν ολοκληρωθεί επιτυχώς το πρόβλημα. Ομοίως, ένας εργοδότης πρέπει επίσης να καταθέσει ένα ποσό που έχει μεγαλύτερο συνολικό κόστος από το κόστος αποθήκευσης των δεδομένων μήτρας. Με την ολοκλήρωση του προβλήματος, η λύση που παράγεται από τον κόμβο αποστέλλεται στους επαληθευτές[58], οι οποίοι θα χρησιμοποιήσουν ένα πιθανό σχήμα επαλήθευσης για να επαληθεύσουν τα δεδομένα παράλληλα πριν δεσμευτούν στο blockchain.

4.Επιθέσεις στο Blockchain

Το ηλεκτρονικό ψάρεμα (phishing) είναι η δόλια προσπάθεια απόκτησης ευαίσθητων πληροφοριών, όπως ονόματα χρηστών, κωδικοί πρόσβασης και στοιχεία πιστωτικών καρτών (και χρημάτων), συχνά για κακόβουλους λόγους, με τη μεταμφίεση ως αξιόπιστη οντότητα σε μια ηλεκτρονική επικοινωνία[59]. Αντιπροσωπεύει το 98% των κοινωνικών περιστατικών και το 93% των παραβιάσεων το 2ο τρίμηνο του 2018. Ο στόχος μπορεί να είναι οτιδήποτε από το να κάνετε τους ανθρώπους να σας στέλνουν χρήματα, να σας παραδίδουν ευαίσθητες πληροφορίες ή ακόμα και να κατεβάζουν άθελά τους κακόβουλο λογισμικό και οι συντάκτες αυτών των επιθέσεων θα χρησιμοποιούν ψέματα, τέχνασμα, πλαστογραφία και πλήρη χειραγώγηση για να τους δουν να πετυχαίνουν[60]. Ο κίνδυνος επιθέσεων ηλεκτρονικού "ψαρέματος" δεν είναι η παρουσία τρωτών σημείων στο σύστημα, αλλά η ευκολία και η απροσεξία του ανθρώπου. Συχνά το ηλεκτρονικό "ψάρεμα" χρησιμοποιεί την Κοινωνική Μηχανική (Social Engineering): ένα είδος επίθεσης που βασίζεται στην ανθρώπινη αστοχία και όχι σε ένα ελάττωμα υλικού ή λογισμικού για να λειτουργήσει.

Πολλά έργα blockchain που έχουν ισχυρές πολιτικές ασφάλειας αποδείχθηκαν ανίσχυρα πριν από τις επιθέσεις χρησιμοποιώντας ηλεκτρονικό ψάρεμα (phishing) και τα μέλη των κοινοτήτων blockchain και οι επενδυτές έχασαν τα χρήματά τους. Σύμφωνα με την Cisco και την Kaspersky Lab έρευνα δείχνει ότι ο μεγαλύτερος αριθμός επιτυχείς επιθέσεις σε έργα blockchain έγιναν με τη βοήθεια ηλεκτρονικού "ψαρέματος" και απάτης χωρίς να χακάρει την ίδια την υποδομή blockchain[61]. Οι ειδικοί της Kaspersky Lab παρακολούθησαν 1000 πορτοφόλια Ethereum, όπου οι χρήστες εξαπατήθηκαν για να καταγράψουν 21.000 επιθέσεις (ETH)[62], το οποίο ισοδυναμεί με περίπου 10 εκατομμύρια δολάρια με βάση τις τρέχουσες τιμές. Ο αριθμός αυτός δεν περιλαμβάνει τα χρήματα που έκλεψαν οι εγκληματίες απευθείας από τα πορτοφόλια των θυμάτων. Το μεγαλύτερο μέρος των προβλημάτων έγκειται στην ευπάθεια των κρυπτοσυστημάτων που χρησιμοποιούν τεχνολογία αποκλεισμού (blockingtechnology).

Στην περίπτωση του Ethereum, τα προβλήματα δεν παρατηρήθηκαν στην ίδια την πλατφόρμα αλλά στα κρυπτοσυστήματα: αντιμετώπισαν τρωτά σημεία στα δικά τους έξυπνα συμβόλαια[63], παραβίαση, συμβιβασμό λογαριασμών διαχειριστή (Slack, Telegram), ιστότοπους ψαρέματος που αντιγράφουν το περιεχόμενο ιστότοπων εταιρειών που εκδίδουν ICO (Information Commissioner's Office).

4.1.Κίνδυνοι για το blockchain

Μία από τις πιο συζητημένες τεχνολογίες σήμερα είναι η distributed ledger technology, ένα decentralized σύστημα καταγραφής συναλλαγών με μηχανισμούς επεξεργασίας, επικύρωσης και έγκρισης συναλλαγών που καταγράφονται στη συνέχεια σε ένα immutable book[64].

Η distributedledgertechnology εκμεταλλεύεται μια σειρά καθιερωμένων αρχών, όπως κρυπτογραφία δημόσιου κλειδιού, δικτύωση ομότιμων (P2P) και αλγόριθμους συναίνεσης (π.χ. απόδειξη της εργασίας (PoW), απόδειξη συμμετοχής (PoS),Practical Byzantine Fault Tolerance).

Το Blockchain είναι μια εφαρμογή της distributed ledger technology (DLT) και αναδύονται άλλες νέες τεχνολογίες όπως το Directed Acyclic Graph (DAG) [65]. Το IOTA και το Hashgraph είναι παραδείγματα DLT που βασίζονται σε DAG.

Ακολουθούν 10 κίνδυνοι ασφάλειας blockchain που έχουν εντοπιστεί, βάσει της μελέτης που αναπτύχθηκε κατά την εκπόνηση της εργασίας και αυτά έχουν ως εξής:

Είναι ο κώδικας λογισμικού αρκετά ώριμος για να αντικαταστήσει το νόμο;

Σε ένα κατανεμημένο περιβάλλον τεχνολογίας, τα έξυπνα συμβόλαια συμφωνούνται με βάση έναν κωδικό λογισμικού και την ημερομηνία που έχει συμφωνηθεί να εκτελεστεί[66], καθώς η ίδια η σύμβαση είναι νόμος. Αν και αυτή η αμετάβλητη φύση είναι η βασική δύναμη αυτής της τεχνολογίας και ενισχύει την εμπιστοσύνη μεταξύ των μερών, πρέπει επίσης να είναι αρκετά ώριμη για να αντικαταστήσει το νόμο.

Υπήρξαν περιπτώσεις στο παρελθόν όταν ορισμένα από τα γνωστά DLT έπρεπε να είναι «hard forcared» φαινόμενο σύμφωνα με το οποίο ο κυβερνητικός κώδικας πρέπει να αντικατασταθεί με έναν νέο. Το 2016, για παράδειγμα, το Ethereum έπρεπε να γίνει σκληρό μετά από μεγάλη συζήτηση μεταξύ της κοινότητας καθώς μια απροσδόκητη διαδρομή κώδικα επέτρεψε στους χρήστες να αποσύρουν χρήματα και ένας άγνωστος χρήστης κατάφερε να αποσύρει 50 εκατομμύρια δολάρια ΗΠΑ. Δεν συμφωνούν όλοι στην κοινότητα με την απόφαση, η οποία οδήγησε σε διαφορετικές εκδόσεις του Ethereum, δηλαδή στα Ethereum και Ethereum Classic[66].

Αυτή η λήψη αποφάσεων δεν είναι εύκολη ή γρήγορη, καθώς απαιτεί συμφωνία μεταξύ της κοινότητας. Ένας άλλος σημαντικός τομέας είναι η εφαρμογή του νόμου. Σε περιπτώσεις όπου υπάρχουν δικαστικές αποφάσεις για την αναίρεση μιας έξυπνης σύμβασης για νομική μη συμμόρφωση, πώς θα άλλαζαν τα προηγούμενα δεδομένα στα μπλοκ;

Στο πλαίσιο της γεωργίας, όπου οι έξυπνες συμβάσεις είναι πολύ χρήσιμες εφαρμογές DLT[67], η απουσία νομικής οντότητας ή ανθρώπου για να ερμηνεύσει τον κώδικα σε περίπτωση διαφωνίας είναι ένας σημαντικός κίνδυνος που πρέπει να θυμόμαστε. Είναι πολύ σημαντικό, επομένως, να διατηρηθεί η σύμβαση απλή.

Τα πρότυπα είναι υποανάπτυκτα και δεν έχουν ωριμάσει ακόμη

Βρισκόμενοι σε ένα στάδιο ταχείας τεχνολογικής ανάπτυξης, δεν υπάρχουν ακόμη ώριμα πρότυπα που να αφορούν την DLT. Σε αυτό το σημείο, υπάρχουν διάφορες ανταγωνιστικές ιδιόκτητες και διαχειριζόμενες πλατφόρμες DLT και πλαίσια[68]. Η απουσία διεθνών προτύπων εγκυμονεί κινδύνους που σχετίζονται με τον αποκλεισμό των πελατών, την έλλειψη διαλειτουργικότητας, την ιδιωτικότητα και την ασφάλεια.

Συνεχίζονται διεθνείς προσπάθειες σε αυτούς τους τομείς, συμπεριλαμβανομένης της Τεχνικής Επιτροπής ISO 307 για τεχνολογίες Blockchain και Distributed Ledger και εργασία στον τομέα τυποποίησης ITU-T της ITU (International Telecommunication Union).

Η ενεργειακή απαίτηση μπορεί να είναι υψηλή

Μια μεθοδολογία για την επίτευξη συναίνεσης για την εισαγωγή ενός νέου μπλοκ δεδομένων μεταξύ των συμμετεχόντων κόμβων είναι ένα βασικό χαρακτηριστικό του blockchain. Υπάρχουν διάφοροι τρόποι επίτευξης συναίνεσης, ο καθένας με τα δικά του πλεονεκτήματα και μειονεκτήματα.

Αυτό που χρησιμοποιείται από το Bitcoin και το Ethereum, η πιο διάσημη από τις εφαρμογές blockchain, είναι η απόδειξη της εργασίας (PoW). Λειτουργεί με την αρχή «δύσκολο να δημιουργηθεί, εύκολο να επαληθευτεί», πράγμα που σημαίνει ότι πρέπει να δαπανηθεί πολλή ενέργεια από τον κόμβο για να κερδίσει διακριτικά κινήτρων. Για μια μεγάλη αλυσίδα όπως το Bitcoin[69], οι εκτιμήσεις υποδεικνύουν ότι το μέγεθος των δεδομένων υπερβαίνει τα 100 gigabytes και οι απαιτήσεις ηλεκτρικής ενέργειας περισσότερο από ολόκληρη τη χώρα της Ιρλανδίας.

Αν και αυτό ισχύει για τη μεθοδολογία PoW, άλλες εναλλακτικές λύσεις όπως η απόδειξη του στοιχήματος (PoS), ο Practical Byzantine Fault Toleranceκαι το authorizedproof-of-stakemodelαπαιτούν λιγότερη ενέργεια. Ωστόσο, έχουν τα δικά τους μειονεκτήματα, για παράδειγμα στην περίπτωση του PoS, οι χρήστες με περισσότερα στοιχήματα θα έχουν μεγαλύτερο έλεγχο στη λήψη αποφάσεων.

Εμπιστευτείτε τους προγραμματιστές και τους διαχειριστές blockchain

Ένα πολύ υψηλό επίπεδο εμπιστοσύνης αποδίδεται στους προγραμματιστές και τους διαχειριστές του blockchain. Είναι μια νέα τεχνολογία όπου ένας μεγάλος αριθμός οντοτήτων καινοτομεί για να δημιουργήσει λύσεις. Οι εστίες, οι ιδιοκτήτες και οι εφαρμογές λογισμικού διαφέρουν.

Η εφαρμογή αυτών των τεχνολογιών εξαρτάται σε μεγάλο βαθμό από την κοινότητα των προγραμματιστών που υποστηρίζουν το έργο ή τον ιδιοκτήτη[70]. Αυτές οι αποφάσεις βασίζονται σε κώδικες που διέπουν τη συναίνεση και την ανάπτυξη της κοινότητας.

Ταυτόχρονα, είναι σημαντικό να δημιουργηθεί ανθεκτικότητα στα δίκτυα έτσι ώστε να μπορούν να τους εμπιστευτούν κρίσιμα δεδομένα[70], πληροφορίες και υπηρεσίες. Η εκτίμηση κινδύνου του έργου είναι σημαντική πριν κάνετε μια επιλογή.

Αυξημένη ευθύνη για τον χρήστη

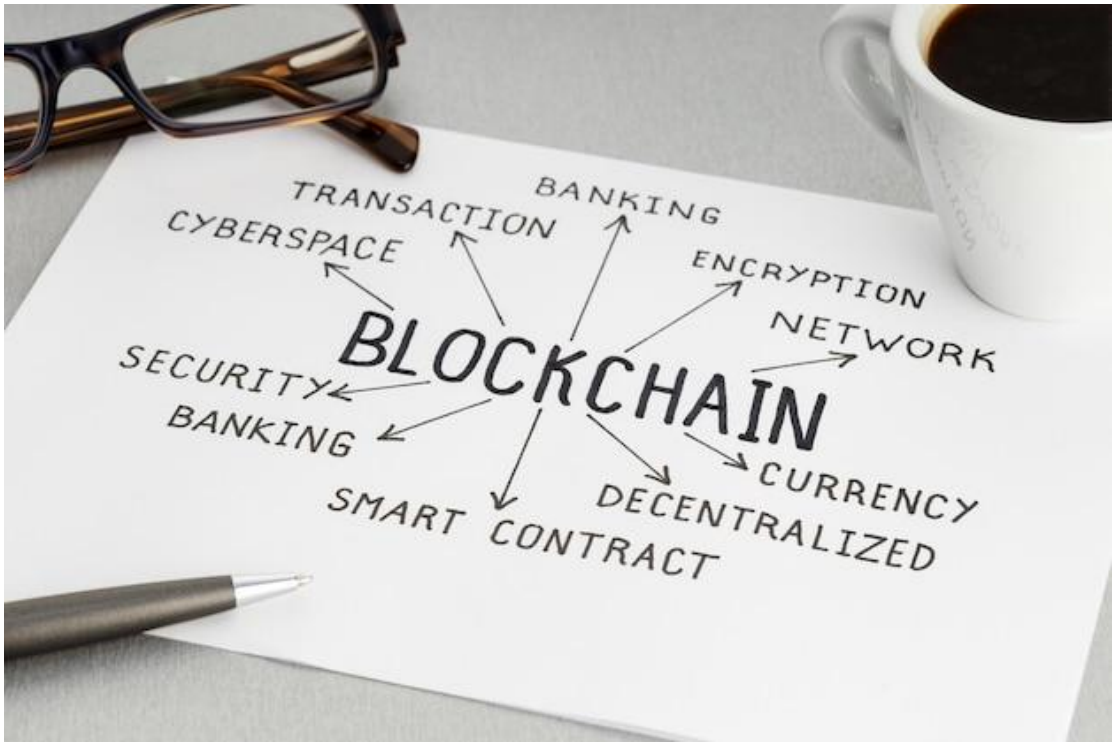
Από τον ίδιο τον σχεδιασμό του, η εφαρμογή blockchain δεν έχει κεντρική αρχή - τουλάχιστον στην περίπτωση δημόσιων blockchains όπως το Bitcoin - η οποία επιβάλλει πρόσθετη ευθύνη στον χρήστη. Δεν υπάρχει οντότητα για να επισκεφθείτε σε περίπτωση απώλειας ιδιωτικών κλειδιών από άτομα (ή απώλειες ως αποτέλεσμα αποκάλυψης ιδιωτικού κλειδιού)[71].

Επίσης, δεν υπάρχει δυνατότητα επαναφοράς ξεχασμένων κωδικών πρόσβασης και ονομάτων χρήστη που έχουν συνηθίσει τα άτομα. Τα άτομα πρέπει να είναι ιδιαίτερα προσεκτικά, όπως στο Διαδίκτυο, πριν δημοσιεύσουν οτιδήποτε. Η σημασία της εισαγωγής των σωστών δεδομένων είναι επίσης πολύ σημαντική καθώς είναι πολύ δύσκολο να γίνουν διορθώσεις αργότερα.

Εφαρμογή της νομοθεσίας περί απορρήτου δεδομένων

Η προστασία των δεδομένων και το απόρρητο αποτελούν μείζον μέλημα και πρωτοβουλίες για την πρόληψη της κατάχρησής τους αναλαμβάνονται από χώρες και περιοχές (π.χ. Ένωση Εθνών της Νοτιοανατολικής Ασίας (ASEAN), Γενικός Κανονισμός Προστασίας Δεδομένων της Ευρωπαϊκής Ένωσης (EU GDPR)[72].

Για παράδειγμα, ο ΓΚΠΔ (Γενικός Κανονισμός Προσωπικών Δεδομένων) της ΕΕ έχει θεσπίσει το «δικαίωμα στη λήθη», ενώ ο σχεδιασμός των DLT είναι προσανατολισμένος στο «ποτέ να μην ξεχνάμε». Παρόλο που υπάρχει πιθανότητα να παραμείνει άγνωστη η ταυτότητα στο σύστημα, εγείρει ανησυχίες για την ασφάλεια σε μεγάλο βαθμό σε σχέση με δραστηριότητες κατά της νομιμοποίησης εσόδων από παράνομες δραστηριότητες (AML - Anti-moneylaundering) και γνωρίζει τις απαιτήσεις των πελατών σας (KYC - KnowYourCustomer).



Πολιτικοί και κανονιστικοί κίνδυνοι

Το πολιτικό και ρυθμιστικό πλαίσιο γύρω από το blockchain είναι στα σπάργανα και συνεπώς εγκυμονεί υψηλούς κινδύνους[73]. Οι διακυμάνσεις στην τιμή του Bitcoin και οι αναφορές για παραβίαση κρυπτονομισμάτων έχουν οδηγήσει σε αυξημένη ρύθμιση από πολλές χώρες και έχουν προσελκύσει ρυθμιστικό ενδιαφέρον.

Αυτοί οι κανονισμοί ποικίλλουν από πλήρη απαγόρευση κατοχής κρυπτονομισμάτων (π.χ. Μπαγκλαντές), απαγόρευση ή κανονισμό για συναλλαγές κρυπτονομισμάτων (Κίνα, Σαουδική Αραβία) έως απαγόρευση κατοχής αρχικών προσφορών νομισμάτων (ICO). Ορισμένα έργα blockchain, ειδικά εκείνα που αφορούν συναλλαγές σε νομίσματα ή διασυνοριακές συναλλαγές, απαιτούν συμμόρφωση με το KYC/AML και είναι σημαντικό να κατανοήσουμε το εθνικό πλαίσιο πριν εμβαθύνουμε σε αυτά τα έργα.

Ταυτόχρονα, οι κυβερνήσεις βλέπουν τα DLT ως τεχνολογία υψηλού δυναμικού και επενδύουν στη χρήση της εφαρμογής του. Ένα έργο χωρίς τη χρήση κρυπτονομίσματος γενικά θα έχει λιγότερες κανονιστικές προκλήσεις από εκείνες που το έχουν.Προς το παρόν, δεν υπάρχει διεθνές πλαίσιο συνεργασίας μεταξύ των φορέων χάραξης πολιτικής και των ρυθμιστικών αρχών στον τομέα αυτό, πράγμα που σημαίνει ότι υπάρχει έλλειψη κατάλληλης προστασίας των καταναλωτών στο διεθνές περιβάλλον[74].

Ταχύτητα συναλλαγών

Η ταχύτητα συναλλαγής είναι ένα σημαντικό στοιχείο καθώς ορισμένα από τα δημόσια blockchains δεν έχουν υψηλές ταχύτητες συναλλαγών. Στο blockchain Bitcoin, ένα νέο μπλοκ εμφανίζεται κατά μέσο όρο κάθε δέκα λεπτά, αλλά δεν είναι εγγυημένο και αυτός ο χρόνος μπλοκ είναι διαφορετικός για κάθε blockchain.

Για την επεκτασιμότητα, είναι σημαντικό να κατανοήσετε την απαίτηση των εφαρμογών ως προς την ταχύτητα (συναλλαγές ανά δευτερόλεπτο (tps)) πριν επιλέξετε μια λύση. Θεωρητικά, το δίκτυο Visa μπορεί να χειριστεί περίπου 50.000 tps, το οποίο είναι πολύ περισσότερο από αυτό που προσφέρουν τα περισσότερα ώριμα blockchains σήμερα.

Κακόβουλοι χρήστες

Ελλείψει ταυτοποίησης τρίτου μέρους, το σύστημα είναι επιρρεπές σε κινδύνους από κακόβουλους χρήστες σε ψευδώνυμα συστήματα, δηλαδή χωρίς απαίτηση αποκάλυψης ταυτότητας (identitydisclosurerequirement)[75].

Παρόλο που τα DLT έχουν σχεδιαστεί για να αποθαρρύνουν κακόβουλες προθέσεις, μπορεί να υπάρχουν καταστάσεις όπου οι κακόβουλοι χρήστες έχουν μεγαλύτερα κίνητρα για να παίξουν το σύστημα και τουλάχιστον να προκαλέσουν βλάβη βραχυπρόθεσμα και να ζητήσουν ένα hard fork. Αυτές οι καταστάσεις είναι πιο πιθανές όταν αποκτούν μεγαλύτερο έλεγχο του συστήματος.

Ταυτότητα και ασφάλεια

Τα δημόσια blockchains πραγματοποιούν συναλλαγές με βάση το δημόσιο και ιδιωτικό κλειδί του ατόμου και δεν διατηρούν την αντιστοίχιση της ταυτότητας με το κλειδί. Αυτό εγείρει περιορισμούς ασφαλείας για τους επιβολείς του νόμου και εφαρμογές όπου η ταυτότητα είναι σημαντική.

Αντίθετα, υπάρχουν ανησυχίες για την προστασία της ιδιωτικής ζωής στην αποκάλυψη ταυτότητας σε blockchains χωρίς άδεια που απαιτούν τη δημοσιοποίηση δεδομένων και αποκάλυψη ιστορικών συναλλαγών[75]. Τα περισσότερα DLT χρησιμοποιούν αλγόριθμους κρυπτογράφησης που είναι δύσκολο να σπάσουν από κανονικούς μη κβαντικούς υπολογιστές.

Προχωρώντας, όπου ο κβαντικός υπολογισμός (βασισμένος σε κυβικά και όχι σε δυαδικά ψηφία) αποκτά δυναμική και ενισχύει τις υπολογιστικές του δυνάμεις. Υπήρξε μεγάλος αριθμός επιτυχιών επιθέσεων σε DLT και υπάρχουν κίνδυνοι ασφάλειας που σχετίζονται με το DLTs30 (π.χ. επιθέσεις blockchain, phishing, κακόβουλο λογισμικό, κρυπτογράφηση, endpointminers, ευπάθειες

εφαρμογής[75], κλοπή πορτοφολιών, επιθέσεις τεχνολογίας, επιθέσεις παλαιού τύπου που έχουν εκσυγχρονιστεί, dictionaryattack, επιθέσεις που βασίζονται σε κβαντικούς υπολογιστές).

4.2.Use case επιθέσεων

Ασφάλιση συσκευών άκρης με έλεγχο ταυτότητας

Καθώς η εστίαση στον τομέα της πληροφορικής μετατοπίζεται σε υποτιθέμενες «έξυπνες» συσκευές με δεδομένα και συνδεσιμότητα, το ίδιο ισχύει και για την ασφάλεια. Σε τελική ανάλυση, η επέκταση του δικτύου μπορεί να είναι καλή για την αποδοτικότητα της πληροφορικής, την παραγωγικότητα και τη χρήση ενέργειας (δηλαδή, καλή για τους πόρους του cloud και των κέντρων δεδομένων), αλλά αντιπροσωπεύει μια πρόκληση ασφάλειας για τους CISO (chief information securityofficer)[76], τους CIO (chiefinformationofficer) και την ευρύτερη επιχείρηση. Πολλοί αναζητούν στη συνέχεια τρόπους χρήσης blockchain για την ασφάλεια IoT και βιομηχανικών συσκευών IoT (IioT), δεδομένου ότι η τεχνολογία ενισχύει τον έλεγχο ταυτότητας, βελτιώνει την απόδοση και ροή δεδομένων και βοηθά στη διαχείριση αρχείων.

Βελτιωμένο απόρρητο και ακεραιότητα δεδομένων

Παρόλο που το Blockchain δημιουργήθηκε αρχικά χωρίς συγκεκριμένους ελέγχους πρόσβασης (λόγω της δημόσιας διανομής του), ορισμένες εφαρμογές blockchain αντιμετωπίζουν πλέον τις προκλήσεις εμπιστευτικότητας δεδομένων και ελέγχου πρόσβασης. Αυτή είναι σαφώς μια κρίσιμη πρόκληση σε μια εποχή όπου τα δεδομένα μπορούν εύκολα να χειριστούν ή να πλαστογραφηθούν, αλλά η πλήρης κρυπτογράφηση δεδομένων blockchain διασφαλίζει ότι αυτά τα δεδομένα δεν θα είναι προσβάσιμα σε μη εξουσιοδοτημένα μέρη κατά τη μεταφορά (τόσο μικρή έως καθόλου πιθανότητα για επιτυχημένο man-in-middle [MiTM])[77].

Αυτή η ακεραιότητα δεδομένων επεκτείνεται σε συσκευές IoT και IIoT. Για παράδειγμα, η IBM παρέχει την πλατφόρμα της Watson IoT με τη δυνατότητα διαχείρισης δεδομένων IoT σε ιδιωτικό καθολικό blockchain, το οποίο είναι ενσωματωμένο στις υπηρεσίες cloud του Big Blue. Η υπηρεσία ακεραιότητας δεδομένων Blockchain της Ericsson παρέχει πλήρως ελεγχόμενα, συμβατά και αξιόπιστα δεδομένα σε προγραμματιστές εφαρμογών που εργάζονται στην πλατφόρμα Predix PaaS της GE.

Ασφαλής ιδιωτική αποστολή μηνυμάτων

Startups όπως το Obsidian χρησιμοποιούν blockchain για να εξασφαλίσουν ιδιωτικές πληροφορίες που ανταλλάσσονται σε συνομιλίες, εφαρμογές ανταλλαγής μηνυμάτων και μέσω κοινωνικών μέσων. Σε αντίθεση με την κρυπτογράφηση από άκρο σε άκρο που χρησιμοποιούν οι χρήστες όπως το WhatsApp και το iMessage, ο αγγελιοφόρος του Obsidian χρησιμοποιεί blockchain για να εξασφαλίσει τα μεταδεδομένα των χρηστών[78]. Ο χρήστης δεν θα χρειαστεί να χρησιμοποιήσει email ή οποιαδήποτε άλλη μέθοδο ελέγχου ταυτότητας για να χρησιμοποιήσει το messenger. Τα μεταδεδομένα κατανέμονται τυχαία σε ένα βιβλίο και έτσι δεν θα είναι διαθέσιμα για συγκέντρωση σε ένα μόνο σημείο, από το οποίο θα μπορούσε να παραβιαστεί.

4.3.Τύποι επιθέσεων e-phishing

Οι επιθέσεις ηλεκτρονικού "ψαρέματος" μπορεί να έχουν μεγάλο εύρος στόχων ανάλογα με τον επιτιθέμενο. Θα μπορούσαν να είναι γενικά μηνύματα ηλεκτρονικού ψαρέματος που αναζητούν οποιονδήποτε έχει λογαριασμό PayPal. Αυτά είναι συνήθως αναγνωρίσιμα ως phishing[79].

Το ηλεκτρονικό ψάρεμα μπορεί να φτάσει στο άλλο άκρο όταν ένα μήνυμα ηλεκτρονικού ταχυδρομείου απευθύνεται σε ένα άτομο. Ο επιτιθέμενος φροντίζει πολύ να δημιουργεί το email, συνήθως λόγω της πρόσβασης που έχουν. Εάν το μήνυμα ηλεκτρονικού ταχυδρομείου βρίσκεται σε αυτό το άκρο του φάσματος, είναι πολύ δύσκολο ακόμη και για τους πιο προσεκτικούς να μην πέσουν θύματα αυτού. Οι στατιστικές δείχνουν ότι το 91% των παραβιάσεων της ασφάλειας πληροφοριών ξεκινούν με κάποιο είδος ηλεκτρονικού ψαρέματος.

4.4.Πρόληψη του e-phishing

Η προστασία με ιστότοπους απάτης σε μαύρη λίστα (ανάπτυξη Yandex, Google και άλλων ανάλογων) ήταν από καιρό η μόνη μέθοδος που χρησιμοποιείται στην

προστασία κατά του ψαρέματος. Η σύγχρονη προστασία κατά του ψαρέματος βασίζεται στη χρήση πολλών τεχνικών και μεθόδων που χρησιμοποιούνται συχνότερα με τη μηχανική μάθηση και την τεχνητή νοημοσύνη[80].

Για τον εντοπισμό ιστότοπων ηλεκτρονικού "ψαρέματος", ένας μεγάλος αριθμός αλγορίθμων αναπτύσσεται και βελτιώνεται συνεχώς. Οι περισσότεροι από τους υπάρχοντες αλγόριθμους αντι-ψαρέματος βασίζονται στην αναζήτηση και τη σύγκριση ιστότοπων με τον αρχικό: σύγκριση γραφής και εμφάνισης στη γραμμή διευθύνσεων του ονόματος ιστότοπου, σύγκριση του περιεχομένου του ιστότοπου. Τέτοιοι αλγόριθμοι επιτρέπουν την εφαρμογή ειδικών επεκτάσεων για προγράμματα περιήγησης που ειδοποιούν τους χρήστες σχετικά με την αναξιοπιστία του ιστότοπου και την πιθανή επίθεση ηλεκτρονικού ψαρέματος και φίλτρα ανεπιθύμητης αλληλογραφίας στα γραμματοκιβώτια. Για προστασία από το ηλεκτρονικό ψάρεμα (phishing), χρησιμοποιείται ενεργά η προστασία των κωδικών πρόσβασης των χρηστών, η οποία χρησιμοποιεί την αποθήκευση των κωδικών πρόσβασης όχι τους κωδικούς πρόσβασης, αλλά τα hashes τους.

Παρά το γεγονός ότι πολλές εταιρείες ξοδεύουν τεράστια ποσά για να μελετήσουν το phishing και να αναπτύξουν ειδικά εργαλεία και αλγόριθμους για τον εντοπισμό και τον αποκλεισμό του, δεν υπάρχουν εργαλεία που να παρέχουν 100% προστασία από τέτοιες επιθέσεις[81]. Λόγω του γεγονότος ότι οι επιθέσεις ηλεκτρονικού ψαρέματος πραγματοποιούνται ως επί το πλείστον με τη συμμετοχή του θύματος, οι μέθοδοι προστασίας από το ψάρεμα περιλαμβάνουν συνδυασμό τεχνικών και κοινωνικών εργαλείων μηχανικής.

4.5.Επιθέσεις και αντίμετρα σε μπλοκ αλυσίδων

4.5.1.Επιθέσεις και αντίστοιχα αντίμετρα στο επίπεδο δεδομένων

Malleabilityattack (επίθεση ελατότητας)

Επίθεση

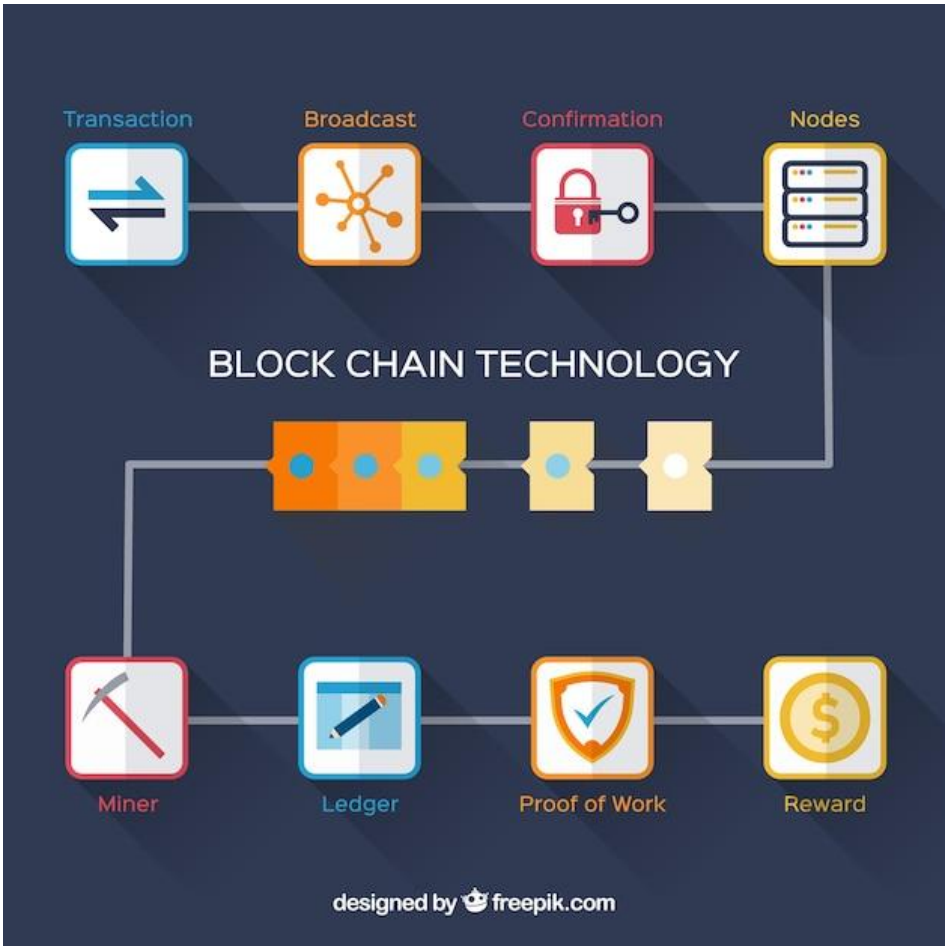
Η επίθεση ελατότητας είναι μια παραλλαγή επίθεσης διπλής δαπάνης (double cost attack), που προέρχεται από την ελατότητα της υπογραφής. Στο Bitcoin , το SSL (Secure Sockets Layer) χρησιμοποιείται στην υπογραφή, έτσι ώστε αφού ένας εισβολέας αλλάξει μερικά byte της υπογραφής, η υπογραφή να εξακολουθεί να είναι έγκυρη. Σε μια τέτοια κατάσταση[82], οι επιτιθέμενοι παρακολουθούν τις συναλλαγές σε δίκτυο bitcoin και τροποποιούν την υπογραφή των συναλλαγών διατηρώντας παράλληλα την επικύρωση των συναλλαγών. Μετά την αλλαγή της υπογραφής των συναλλαγών, παράγεται διαφορετική ταυτότητα συναλλαγής. Στη συνέχεια, οι

επιτιθέμενοι μεταδίδουν τις δύο συναλλαγές σε δίκτυο bitcoin, με αποτέλεσμα το αποτέλεσμα της διπλής δαπάνης.

Αντίμετρα

Το Segregated Witness (SW) είναι ένας τρόπος επίλυσης της εύπλαστης επίθεσης στο blockchain[82]. Διαχωρίζει την υπογραφή σεναρίου της συναλλαγής σε ένα πεδίο διάρκειας που προστέθηκε πρόσφατα, το οποίο μειώνει το μέγεθος της συναλλαγής και κάνει το μπλοκ να φιλοξενήσει περισσότερες συναλλαγές. Επιπλέον, το SW περιορίζει το μέγεθος του μπλοκ σε 1M, το οποίο μειώνει την επίθεση DDoS για εκείνα τα πλαστά μπλοκ με μεγάλο μέγεθος που πρέπει να ελέγξετε και να απορρίψετε. Ωστόσο, η SW έχει τους δικούς της περιορισμούς. Επειδή η SW μειώνει το τέλος συναλλαγής, έτσι οι κόμβοι έχουν κίνητρο να συσκευάσουν αυτές τις ανεπιθύμητες συναλλαγές με υψηλότερο τέλος συναλλαγής από τις συνηθισμένες συναλλαγές. Επιπλέον, το SW αυξάνει την πολυπλοκότητα της ανανέωσης του λογισμικού και απαιτούνται περισσότερες σκέψεις σχετικά με τη συμβατότητα κατά την ενημέρωση του λογισμικού.

Andrychowicz et al. έκανε μια τροποποίηση της προδιαγραφής Bitcoin, προτείνοντας να υπολογίσει hashes συναλλαγής χωρίς τα σενάρια εισόδου της. Με αυτόν τον τρόπο, ανεξάρτητα από το σενάριο εισόδου[83], η συναλλαγή θα έχει την ίδια τιμή κατακερματισμού, επιλύοντας έτσι το πρόβλημα της ελατότητας. Σε αυτήν την περίπτωση, ο εισβολέας θα μπορούσε να προσαρμόσει τα σενάρια εισόδου οποιασδήποτε συναλλαγής σε δίκτυο blockchain και να μεταδώσει τη νέα συναλλαγή. Ωστόσο, η αξία κατακερματισμού της αρχικής συναλλαγής και η τροποποιημένη νέα συναλλαγή είναι οι ίδιες, χωρίς καμία διαφορά από πριν.



Dziembowski et al. πρότεινε ένα χρονοδιάγραμμα δέσμευσης βασισμένο στο Bitcoin για να αντισταθεί στην ελαστικότητα των συναλλαγών, κατασκευάζοντας συναλλαγές με *ασφάλεια*. Η γενική ιδέα των συναλλαγών με *ασφάλεια* είναι να χρησιμοποιήσετε μια χρονομετρημένη δέσμευση αντί να χρησιμοποιήσετε άμεσα ένα χρονικό κλείδωμα. *Οι* συναλλαγές *ασφαλειών* δενχρειάζεται να υπογράφονται από προμηθευτές, επομένως μπορούν να δημιουργηθούν και να υπογραφούν από επιτιθέμενους αφού επιβεβαιωθεί η συναλλαγή *κατάθεσης* και γίνει γνωστό το hash της [83]. Ένα μειονέκτημα αυτής της κατασκευής είναι ότι οι πωλητές πρέπει επίσης να κάνουν μια κατάθεση.

Time hijackingattack (Επίθεση αεροπειρατείας χρόνου)

Επίθεση

Οι επιθέσεις παραβίασης χρόνου συμβαίνουν λόγω της ευπάθειας της επεξεργασίας χρονικής σφραγίδας Bitcoin. Ο μετρητής ώρας του δικτύου bitcoin τροποποιείται και ο χρόνος κόμβων αλλάζει επίσης [84]. Θα υιοθετηθεί χρόνος συστήματος προσανατολισμένος στο υλικό για να αντικαταστήσει τον προηγούμενο χρόνο δικτύου. Η αεροπειρατεία είναι επιρρεπής στην εμφάνιση όταν ο αντίπαλος εκτελεί την επίθεση Sybil με ανακριβείς χρονικές σημάνσεις ταυτόχρονα, η οποία προσθέτει πολλούς κόμβους Sybil στο δίκτυο.

Αντίμετρα

Ο περιορισμός των περιοχών ανοχής και το πρωτόκολλο χρόνου δικτύου μπορούν να αξιοποιηθούν για τον χειρισμό των επιθέσεων αεροπειρατείας χρόνου. Ma et al. πρότεινε ένα βελτιστοποιημένο πρωτόκολλο χρονικής σήμανσης για την επίτευξη συναίνεσης μέσω εξωτερικών υπηρεσιών χρονικής σήμανσης εμπιστοσύνης, το οποίο περιόρισε το εύρος των χρονικών σημάνσεων στο blockchain, μειώνοντας έτσι τις επιθέσεις αεροπειρατείας χρόνου[85]. Επιπλέον, η επίθεση απαγωγής χρόνου θα

μπορούσε να αποφευχθεί περιορίζοντας τα χρονικά εύρη αποδοχής ή χρησιμοποιώντας τον χρόνο συστήματος του κόμβου.

Quantumattack (Κβαντική επίθεση)

Επίθεση

Οι κβαντικές επιθέσεις είναι επιθέσεις στο κρυπτογραφικό τμήμα του blockchain. Ο πυρήνας του είναι να λύσει το μαθηματικό πρόβλημα της κρυπτογραφικής εξάρτησης[85]. Οι κβαντικοί υπολογιστές έχουν πλεονεκτήματα στην επίλυση μαθηματικών προβλημάτων της κρυπτογραφίας. Οι επιτιθέμενοι εξαπολύουν κβαντικές επιθέσεις σε blockchain για να προκαλέσουν σύγκρουση hash.

Αντίμετρα

Khalifa et al. πρότεινε γενικά αμυντικά μέτρα κατά των κβαντικών ελαστικών blockchains και ανέλυσε διεξοδικά το κβαντικό σχέδιο μετά την υπογραφή για να επιλέξει μια κατάλληλη εναλλακτική λύση για να αντικαταστήσει την πιο σοβαρή απειλή στις παραδοσιακές ψηφιακές υπογραφές.

4.5.2.Επιθέσεις και αντίστοιχα αντίμετρα στο επίπεδο δικτύου

Επίθεση DDoS (distributed denial-of-service)

Επίθεση

Η κατανεμημένη άρνηση παροχής υπηρεσιών (DDoS) είναι μια μαζική επίθεση DoS που κάνει τους νόμιμους χρήστες να μην έχουν πρόσβαση στην κανονική υπηρεσία δικτύου. Το blockchain χρησιμοποιείται για τον μετριασμό της επίθεσης DDoS που βασίζεται σε συσκευή IoTχρησιμοποιώντας στατική κατανομή πόρων για τη συσκευή[86]. Ωστόσο, η επίθεση DDoS μπορεί επίσης να συμβεί σε blockchain. Muhammad et al. επισήμανε μια νέα μορφή επίθεσης DDoS, στην οποία οι επιτιθέμενοι ελέγχουν μια ομάδα λογαριασμού Sybil και καθένας από τους λογαριασμούς κατέχει πολλαπλές δημόσιες διευθύνσεις. Ο εισβολέας θα ξεκινήσει πολλές πρωτότυπες συναλλαγές σε πολύ σύντομο χρονικό διάστημα, προκειμένου να δημιουργήσει συναλλαγές που είναι απίθανο να αντιμετωπιστούν πρώτα. Wang et al. πρότεινε ένα είδος επίθεσης DDoS σε blockchain και το ονόμασε ως επίθεση τριγώνου (triangleattack)[86]. Σε triangleattack, μια συναλλαγή προστίθεται στην αλυσίδα αλλά δεν μεταδίδεται σε άλλους κόμβους σε ισχύ.

Αντίμετρα

Muhammad et al. ανέπτυξε σχέδια βάσει αμοιβών και ηλικίας για την επίλυση επιθέσεων DDoS σε μνήμη Bitcoin. Σε σχεδιασμό βάσει αμοιβών, μια εισερχόμενη συναλλαγή πρέπει να πληρώσει τόσο την ελάχιστη χρέωση ρελέ όσο και την ελάχιστη αμοιβή εξόρυξης, εάν γίνει αποδεκτή από τη μνήμη, κάτι που περιορίζει την εισερχόμενη συναλλαγή, φιλτράρει τις ανεπιθύμητες συναλλαγές και μειώνει το μέγεθος της δεξαμενής μνήμης[87]. Στον σχεδιασμό ηλικίας, το ελάχιστο όριο ηλικίας εφαρμόζεται ως φίλτρο της δεξαμενής μνήμης. Μόνο η μέση τιμή της συναλλαγής που πληροί τα κριτήρια ηλικίας θα γίνει αποδεκτή από τη μνήμη, ενώ οι μη επιβεβαιωμένες συναλλαγές θα απορρίπτονται[87]. Οι επιτιθέμενοι πρέπει να περιμένουν τις συναλλαγές για να αποκτήσουν σημαντική ηλικία εάν συνεχίσουν την επίθεσή του, αυξάνοντας το κόστος επίθεσης και μειώνοντας το παράθυρο εκκίνησης της επίθεσης.

Wu et al. πρότεινε μια εντελώς διαφορετική μέθοδο και έλυσε το δυναμικό πρόβλημα των επιθέσεων εξόρυξης για πρώτη φορά. Η δεξαμενή εξόρυξης χρησιμοποιεί τον αλγόριθμο μάθησης Nash για να αποκτήσει αποτελεσματικά τη μέγιστη μακροπρόθεσμη χρησιμότητα[87]. Το πειραματικό αποτέλεσμα δείχνει ότι αυτή η μέθοδος αποδίδει καλύτερα από τους βασικούς myopia learning algorithmsγιατί εστιάζει μόνο στο τρέχον μέγιστο εισόδημα.

Eclipse attack (Επίθεση έκλειψης)

Επίθεση

Η επίθεση Eclipse επιτρέπει σε έναν εισβολέα να έχει πολλές IP διευθύνσεις για να ελέγξει όλες τις συνδέσεις ενός έντιμου κόμβου blockchain. Αυτό το είδος επίθεσης στοχεύει να αποτρέψει την είσοδο των νεότερων πληροφοριών μπλοκ σε κόμβους έκλειψης, απομονώνοντας τους κόμβους των θυμάτων. Επιπλέον, οι αντίπαλοι μπορούν να επηρεάσουν την άποψη των έντιμων κόμβων στο blockchain, κάνοντας τους ειλικρινείς κόμβους να σπαταλήσουν την υπολογιστική ισχύ σε ξεπερασμένη προβολή του blockchain[88]. Hammi et al. ανέπτυξε μια νέα μέθοδο για να επιτύχει την επίθεση Eclipse που εμποδίζει όλες τις συνδέσεις ειλικρινών κόμβων με ελάχιστο μόνο αριθμό διευθύνσεων IP. Walck et al. πρότεινε το TendrilStaller που συνέβη στο δίκτυο Bitcoin.

Ο εισβολέας καθυστερεί τη διάδοση του blockchain κατά δέκα λεπτά, οπότε το θύμα δεν μπορεί να αποκτήσει την πιο πρόσφατη προβολή του blockchain[88]. Αυτό το είδος επίθεσης είναι πολύ εύκολο να συμβεί, επειδή η απαίτηση για την εκτέλεση της επίθεσης έκλειψης είναι μόνο ένας πλήρης κόμβος Bitcoin και δύο ελαφροί κόμβοι.

Αντίμετρα

Προκειμένου να λυθεί η επίθεση έκλειψης του blockchain, οι Ethan Heilman et al. πρότεινε τα ακόλουθα δέκα αντίμετρα[89]:

• Αντικαταστήστε την ντετερμινιστική τυχαία έξωση.

• Δημιουργήστε εξερχόμενη σύνδεση με τυχαία επιλογή.

• Δοκιμή πριν το evitc.

• Εκτελέστε σύνδεση ανιχνευτή.

• Προσθήκη συνδέσμων αγκύρωσης.

• Δημιουργήστε περισσότερους κόμβους.

• Προσθέστε περισσότερους εξερχόμενους συνδέσμους.

• Απαγόρευση ανεπιθύμητων μηνυμάτων.

• Διαφοροποίηση εισερχόμενων συνδέσμων.

• Εντοπίστε ανώμαλη συμπεριφορά.

Signorini et al. εισήγαγε το ADvISE, ένα εργαλείο ανίχνευσης μη φυσιολογικής συμπεριφοράς blockchain, το οποίο χρησιμοποιεί μεταδεδομένα για να συγκεντρώσει πιθανώς μοχθηρό αίτημα που μπορεί να υπάρχει στο δίκτυο ή το σύστημα, ενώ αντιστέκεται στην επίθεση ηλιακών εκλείψεων. Η ADVISE συγκέντρωσε και ανέλυσε φαύλους κλάδους για να αναπτύξει μια βάση δεδομένων απειλής, η οποία μπορεί να εντοπίσει και να αποτρέψει επιθέσεις στο μέλλον[89].

Επίθεση Sybil

Επίθεση

Η επίθεση Sybil ελέγχει το σύστημα δικτύου blockchain δημιουργώντας ένα μεγάλο αριθμό ψευδώνυμων ταυτότητας, αξιοποιώντας τον πλεονασμό και την ανωνυμία του blockchain[90]. Οι απειλές από την επίθεση στο Sybil υπάρχουν πάντα εάν δεν λυθεί το πρόβλημα της ισοτιμίας των πόρων και του συντονισμού μεταξύ των οντοτήτων. Στην επίθεση Sybil, μια οντότητα (ένας κόμβος) μπορεί να παρουσιάσει πολλαπλές ταυτότητες, καθιστώντας την οντότητα να αποκτά δυσανάλογη επιρροή στο δίκτυο Peer-to-Peer.

Αντίμετρα

Ο καθαρός consensusmechanism, PoW μπορεί να αποτρέψει αποτελεσματικά την επίθεση Sybil, επειδή υιοθετεί μία CPU-onevote. Σε μια τέτοια κατάσταση, οι επιτιθέμενοι είναι δύσκολο να παράγουν πολλαπλές εικονικές ταυτότητες, γεγονός που μειώνει την πιθανότητα επίθεσης Sybil. Μια άλλη προσέγγιση για την υπεράσπιση της επίθεσης στο Sybil είναι η χρήση μιας αξιόπιστης υπηρεσίας για την απόδειξη των ταυτοτήτων[90]. Σε πιστοποιημένα αναγνωριστικά αναγνωρισμένης εταιρείας, κάθε κόμβος πρέπει να πιστοποιείται με ένα τρίτο μέρος κατά την είσοδο στο δίκτυο Peer-to-Peer.

Εκτός από τις μεθόδους που αναφέρθηκαν προηγουμένως, οι George et al. πρότεινε ένα υβριδικό πρωτόκολλο δύο μερών με τη συμβατότητα διαφόρων εικονικών νομισμάτων και το ονόμασε ως Xim για την αντιμετώπιση της επίθεσης Sybil. Επιπλέον, το Xim θα μπορούσε να χειριστεί επιθέσεις DoS και κάποιες επιθέσεις συμπερασμάτων βάσει χρονισμού, το οποίο είναι ένα πολύ χρήσιμο πρωτόκολλο. Ο Xim θα μπορούσε συγκαλυμμένα να βρει έναν συνεργάτη λόγω

διαφήμισης σε blockchain με decentralizedσύστημα[91]. Τα αποτελέσματα του πειράματος δείχνουν ότι ο σχεδιασμός του Xim καθιστά το κόστος επίθεσης γραμμικό με το συνολικό ποσό των συμμετεχόντων κόμβων και η μικτή μέθοδος πιθανότητας μειώνει την επίδραση των επιθέσεων DoS που βασίζονται σε Sybil.

Επίθεσηδρομολόγησης BGP (BorderGatewayProtocol)

Επίθεση

Το πρωτόκολλο Border Gateway ανήκει σε εξωτερικά πρωτόκολλα δρομολόγησης που συνδέουν διαφορετικά δίκτυα στο Διαδίκτυο. Στην επίθεση δρομολόγησης BGP, γνωστή και ως BGP hijacks, κάθε κακόβουλο AS (Αυτόνομο Σύστημα) μπορεί να δημιουργήσει ψεύτικες διαφημίσεις για οποιοδήποτε πρόθεμα και να τις διαφημίσει στους γείτονές του, ανακατευθύνοντας την κίνηση που κατευθύνεται σε δεδομένους προορισμούς[91]. Μόλις η κίνηση των κόμβων ελέγχεται από επιτιθέμενους, ο μηχανισμός συναίνεσης θα μπορούσε να καταστραφεί. Επιπλέον, οι πληροφορίες όπως οι συναλλαγές θα μπορούσαν να χειριστούν οι επιτιθέμενοι.

Η επίθεση δρομολόγησης BGP θα μπορούσε να χρησιμοποιηθεί για τον διαχωρισμό ενός δικτύου blockchain σε πολλά ανεξάρτητα δίκτυα που δεν μπορούν να επικοινωνούν μεταξύ τους [92]. Σε μια τέτοια κατάσταση, το blockchain θα εισχωρήσει σε πολλές παράλληλες αλυσίδες. Στη συνέχεια, οι επιτιθέμενοι μπορούν να πραγματοποιήσουν συναλλαγές σε αυτά τα παράλληλα. Τέλος, η μεγαλύτερη αλυσίδα θα επιβιώσει ενώ η συναλλαγή των άλλων παράλληλων συνδέσμων θα απορριφθεί μετά τη διακοπή της επίθεσης[92].

Αντίμετρα

Maria et al. παρουσίασε ένα δίκτυο Bitcoin μεγάλης ασφάλειας και επεκτασιμότητας και το ονόμασε ως SABER. Στο δίκτυο SABER, οι χρήστες θα μπορούσαν να μεταδώσουν μπλοκ παγκοσμίως μέσω μιας σειράς συνδέσεων για να αντισταθούν στις επιθέσεις δρομολόγησης. Επιπλέον, οι κόμβοι φιλοξενούνται με βάση τις πολιτικές δρομολόγησης μεταξύ τομέων, προστατεύοντας την τοποθεσία επίθεσης δρομολόγησης και την οικονομικά προτιμώμενη διαδρομή των πελατών Bitcoin[93]. Το SABER μπορεί να αποτρέψει τους αντιπάλους επιπέδου AS από το διαχωρισμό του δικτύου bitcoin και να βελτιστοποιήσει την εγγύηση ασφάλειας του συστήματος. Επιπλέον, οι κόμβοι ρελέ SABER είναι συν-σχεδιασμένοι λογισμικού-υλικού που μπορούν να λειτουργήσουν υπό υψηλό φορτίο με ελάχιστη παρέμβαση λογισμικού.

4.5.3.Επιθέσεις και αντίστοιχα αντίμετρα στο επίπεδο συναίνεσης και κινήτρων

Selfishminingattack (Εγωιστική επίθεση εξόρυξης)

Επίθεση

Είναι δύσκολο για έναν επιτιθέμενό να επεξεργαστεί το μαθηματικό παζλ στο PoW, οπότε οι επιτιθέμενοι είναι ικανοί να συνεργάζονται μεταξύ τους, να σχηματίζουν μια δεξαμενή εξόρυξης και να μοιράζονται τις ανταμοιβές του bitcoin. Αυτοί οι επιτιθέμενοι ονομάζονται selfishattackers (εγωιστές επιτιθέμενοι). Η εγωιστική εξόρυξη είναι η επίθεση κατά την οποία οι selfishattackersχρησιμοποιούν μια σειρά εγωιστικών στρατηγικών για να αποκτήσουν περισσότερα έσοδα από ό, τι τους αξίζει[94]. Σε μια εγωιστική επίθεση εξόρυξης, οι selfishattackersμπορούν να αποκτήσουν ένα σχετικά σταθερό εισόδημα, σε σύγκριση με την εξόρυξη μόνο. Ωστόσο, είναι άδικο για εκείνους τους έντιμους κόμβους που ακολουθούν το πρωτόκολλο όπως περιγράφει ο PoW.

Kartik et al. εισήγαγε μια σειρά στρατηγικών εξόρυξης, συμπεριλαμβανομένης της επίμονης επίθεσης, η οποία εφαρμόζεται σε ένα μεγάλο εύρος παραμέτρων και θα μπορούσε να αποφέρει περισσότερα έσοδα από επιτιθέμενους. Liu et al. ανέλυσε ύποπτες συμπεριφορές επιτιθέμενων σε blockchains με βάση PoW στην περίπτωση πολλαπλών αντιπάλων[94]. Επιπλέον, καθόρισαν τη δημοσίευση (n) για την επέκταση των στρατηγικών των αντιπάλων. Azimy et al. ανέπτυξε έναν προσομοιωτή δικτύου Bitcoin και έθεσε διαφορετικές παραμέτρους για τον εντοπισμό αλλαγών στο εισόδημα των επιτιθέμεων σε διαφορετικές διαμορφώσεις. Τα αποτελέσματα δείχνουν ότι με ισχυρότερους εγωιστές επιτιθέμενους, η εγωιστική εξόρυξη κάνει τους ισχυρούς πιο δυνατούς και τους αδύναμους πιο αδύναμους. Cao et al. παρουσίασε zerodeterminer(ZD)[94], μια βελτιστοποιημένη στρατηγική, για την επιβολή της συνεργασίας μεταξύ miners in the miningcomplex, αυξάνοντας το συνολικό εισόδημα του συνόλου των miningmines.

Αντίμετρα

Zhang et al. πρότεινε μια οπισθοδρομική συμβατή μέθοδο προστασίας για την αντιμετώπιση της selfishmining, η οποία είναι ανώτερη από τους προηγούμενους μηχανισμούς προστασίας. Σε αυτόν τον μηχανισμό προστασίας, η στρατηγική ανάλυσης αγνοεί τα μπλοκ που δεν κυκλοφορούν εγκαίρως και, αντίθετα, απονέμει τα μπλοκ που συγχωνεύουν συνδέσμους στα προηγούμενα ανταγωνιστικά μπλοκ τους [95]. Επομένως, μέχρι να κυκλοφορήσει το ανταγωνιστικό μπλοκ, το μπλοκ παραμένει μυστικό και δεν θα λειτουργήσει σε αυτούς τους δύο κλάδους. Αυτό το

σχήμα επιτυγχάνει μια μεγάλη ισορροπία μεταξύ αποτελεσματικότητας και χρόνου ανάκτησης μερών [95]. Αν και το σχέδιο είναι αποτελεσματικό σε μια συγκεκριμένη κατάσταση απειλής, η πραγματική κατάσταση μπορεί να είναι πολύ πιο περίπλοκη.

Zhen et al. πρότεινε ένα μοντέλο στο οποίο η εξόρυξη μεταξύ δύο minerseίναι ένα επαναληπτικό παιχνίδι. Επιπλέον, ανέπτυξαν μια υποκατηγορία της στρατηγικής ZD για να απαλύνουν το δίλημμα των επιτιθέμενων. Pachal et al. πρότεινε μια νέα ορθολογική στρατηγική εξόρυξης που αποκεντρώνει το σύστημα Bitcoin με μόνο το 28% των επιτιθέμενων, γεγονός που μειώνει σημαντικά την πιθανότητα selfishmining[96]. Chicarino et al. πραγματοποίησε ανάλυση μέσω του προσομοιωτή NS3. Ταυτόχρονα, τα αποτελέσματα της προσομοίωσης έδειξαν ότι η πιθανότητα ανίχνευσης επιθέσεων είναι υψηλή όταν η διχοτόμηση έχει ύψος μεγαλύτερο ή ίσο με 2. Επιπλέον, η ακρίβεια για τηνselfishminingattackείναι 99,99%.

Doublespendattack (Επίθεση διπλών δαπανών)

Επίθεση

Η επίθεση Finney πήρε το όνομά της από τον Hal Finney, ο οποίος περιέγραψε αρχικά μια παραλλαγή αυτής της Doublespendattackκαι την ονόμασε μια συναλλαγή 0-επιβεβαίωσης. Επιτυγχάνεται με τον έλεγχο της μετάδοσης του μπλοκ[97].

Αντίμετρα

Για επίθεση πλειοψηφίας και επίθεση εναλλακτικού ιστορικού, η προσθήκη χρόνων επιβεβαίωσης μπλοκ μπορεί αποτελεσματικά να αποτρέψει τέτοιου είδους επίθεση. Επιπλέον, η αποφυγή σχηματισμού δεξαμενών εξόρυξης μεγάλης κλίμακας που διαθέτουν υψηλό ποσοστό υπολογιστικής ισχύος είναι επίσης ένας τρόπος για να μειωθεί η πιθανότητα εναλλακτικής ιστορικής επίθεσης και επίθεσης πλειοψηφίας.

Επιπλέον, οι Kovalchuk et al. παρείχε ένα ανώτατο όριο για την πιθανότητα επιτυχίας του επιτιθέμενου, το οποίο δημιουργεί ένα κόμβο-απόφασης μήκους l που εμφανίζεται σε N χρονοθυρίδες[97]. Ο Dey ενσωμάτωσε εποπτευόμενες μεθόδους μηχανικής μάθησης με τη θεωρία των παιχνιδιών για την επίλυση του προβλήματος της επίθεσης της πλειοψηφίας. Επιπλέον, έθεσαν πράκτορες λογισμικού για τον εντοπισμό κακόβουλης συμπεριφοράς στο blockchain[97]. Για τη δικαιοσύνη και τη νομιμότητα των συναλλαγών δικτύου blockchain, αυτή η μέθοδος εφαρμόζει έναν έξυπνο πράκτορα, ο οποίος θα αποτελείται από δύο διαφορετικά μέρη:

• την πιθανότητα κάθε ενδιαφερόμενου μέρους λόγω των προηγούμενων συναλλαγών των ενδιαφερομένων

• την πιθανότητα των ενδιαφερόμενων μερών με βάση τις τρέχουσες αξίες αγαθών ή υπηρεσιών της τρέχουσας συναλλαγής.

Εάν τα εποπτευόμενα ενδιαφερόμενα μέρη θεωρηθούν κακόβουλα και σκοπεύουν να εξαπολύσουν επίθεση με πλειοψηφία, η τρέχουσα συναλλαγή αυτών των μετοχών θα ακυρωθεί. Bae et al. μείωσε τις συμπεριφορές επίθεσης διπλής δαπάνης επιλέγοντας τυχαίες ομάδες εξόρυξης[97]. Τα αποτελέσματα του πειράματος δείχνουν ότι εάν η ποσότητα των ομάδων είναι μεγαλύτερη ή ίση με 2, η πιθανότητα επιτιθέμενων να δημιουργήσουν το μπλοκ prochain είναι μικρότερη από 50%. Chen et al. υλοποίησε ένα νέο υβριδικό πρόγραμμα κατασκευής blockchain το οποίο συνδυάζει PoW και equity για να καθορίσει εάν ο επιτιθέμενος επιτρέπεται να κατασκευάζει μπλοκ. Τα πειραματικά αποτελέσματα δείχνουν ότι τα στοιχήματα παίζουν καθοριστικό ρόλο στο υβριδικό διάλυμαστην αρχή, οδηγώντας στο αποτέλεσμα ότι οι επιτιθέμενοι δεν μπορούν να ξεκινήσουν μια επίθεση πλειοψηφίας ακόμα κι αν οι επιτιθέμενοι ελέγχουν το μεγαλύτερο μέρος της υπολογιστικής ισχύος[97].

Briberyattack (Επίθεση δωροδοκίας)

Επίθεση

Σε Briberyattack, οι επιτιθέμενοι θα έκαναν πρώτα μια συναλλαγή και μετά ο προμηθευτής περιμένει την επιβεβαίωση της συναλλαγής. Εν τω μεταξύ, οι

επιτιθέμενοι αποκτούν μια προσωρινή πλειοψηφία της ικανότητας εξόρυξης ενοικιάζοντάς την από τους ονομαστικούς ιδιοκτήτες. Εάν το κόστος της δωροδοκίας είναι χαμηλότερο από τη συναλλαγή, η επίθεση είναι επιτυχής[98]. Υπάρχουν τρεις τρόποι για τους εισβολείς να νοικιάσουν την ικανότητα εξόρυξης. Πρώτον, οι πληρωμές εκτός ζώνης μπορούν να πληρώσουν απευθείας τους ιδιοκτήτες, ώστε να μπορούν να λειτουργούν όπως επιλέγει ο εισβολέας. Ωστόσο, η έλλειψη εσωτερικής εμπιστοσύνης καθιστά δύσκολο για τους εισβολείς να εξαπολύσουν ανώνυμα επίθεση δωροδοκίας[98]. Δεύτερον, οι επιτιθέμενοι θα μπορούσαν να δημιουργήσουν ένα συγκρότημα εξόρυξης για να πληρώσουν μια απόδοση στις αγορές, το οποίο ονομάζεται miningaggregationmechanism με negativecharges. Τρίτον, οι επιτιθέμενοι μπορούν να αποκτήσουν την ικανότητα εξόρυξης χρησιμοποιώντας εσωτερική πληρωμή με φασαρία, στο οποίο οι επιτιθέμενοι μπορούσαν να δωροδοκήσουν μέσω διακριτικού.

Αντίμετρα

Για Briberyattack, ο μηχανισμός PoW μπορεί να το αποτρέψει καλά, επειδή οι επιτιθέμενοι απαιτούν μεγάλο κόστος εάν θέλουν να τον δωροδοκήσουν στο PoW και να κάνουν μια επιτυχημένη επίθεση. Το κόστος της επίθεσης θα είναι πολύ μεγαλύτερο από τη συναλλαγή της [99]. Ο Bonneau περιέγραψε πολλούς παράγοντες που θα μπορούσαν να μετριάσουν την επίθεση δωροδοκίας. Πρώτον, η αναγνώριση ή η αποδοχή δωροδοκιών δεν είναι τόσο απλοϊκή για τους κατόχους του blockchain και τους επιτιθέμενους απαιτούν σημαντικό κεφάλαιο και ανοχή στον κίνδυνο, επειδή ο εισβολέας δεν θα μπορούσε να ανακτήσει τις δωροδοκίες εάν η επίθεση αποτύχει. Επιπλέον, οι πωλητές ενδέχεται να απαιτούν περισσότερες επιβεβαιώσεις για μια μεγάλη συναλλαγή που αυξάνει το κόστος δωροδοκίας των επιτιθέμενων γραμμικά[99]. Επιπλέον, οι κάτοχοι θα έχουν κίνητρο να αρνηθούν το βραχυπρόθεσμο εισόδημα, ενώ μειώνουν τις μακροπρόθεσμες δυνατότητες εσόδων.

Refundattack (Επίθεση επιστροφής χρημάτων)

Επίθεση

McCorry et al. παρουσίασε επίθεση επιστροφής χρημάτων στο πρωτόκολλο BIP70. Περιέγραψαν δύο τύπους επιθέσεων επιστροφής χρημάτων: Επιθέσεις εμπόρων Silkroad και επιθέσεις εμπόρων αγοράς. Στις επιθέσεις εμπόρων Silkroad, οι επιτιθέμενοι κάνουν τους πελάτες να στέλνουν πληρωμές σε παράνομους εμπόρους μέσω έντιμων εμπόρων και εύλογα τους αρνούνται να συμμετάσχουν οι ίδιοι στις συναλλαγές επιστροφής χρημάτων αργότερα. Η κύρια ουσία της επίθεσης εμπόρων Silkroad εξαρτάται από την ικανότητα ανταλλαγής διευθύνσεων

επιστροφής χρημάτων και τις διευθύνσεις Bitcoin που ελέγχεται από παράνομους εμπόρους. Επιπλέον, οι πελάτες δεν χρειάζεται να χρησιμοποιούν ψηφιακές υπογραφές για να εγκρίνουν τις διευθύνσεις Bitcoin των παράνομων εμπόρων[100]. Σε αντίθεση με τις επιθέσεις εμπόρων silkroad, το επίκεντρο των επιθέσεων εμπόρων στην αγορά είναι οι τρέχουσες πολιτικές επιστροφής χρημάτων των Coinbase και BitPay, που λαμβάνουν διευθύνσεις επιστροφής χρημάτων μέσω email. Στη συνέχεια, οι απατεώνες έμποροι παρασύρουν πελάτες σε επιθέσεις phishing μέσω της φήμης αξιόπιστων εμπόρων.

Αντίμετρα

McCorry et al. πρότεινε refereesνα λύσουν το πρόβλημα της επίθεσης επιστροφής χρημάτων[100]. Οι έμποροι καλούνται να παρέχουν επαληθεύσιμα στοιχεία, τα οποία εξαλείφουν το κίνητρο του εισβολέα για επικερδείς επιθέσεις. Περισσότερες πληροφορίες όπως η διεύθυνση παράδοσης προστίθενται στο τροποποιημένο μήνυμα αιτήματος πληρωμής, καθιστώντας τη συναλλαγή συνδεδεμένη με τη διεύθυνση επιστροφής χρημάτων. Ωστόσο, αυτή η λύση είναι ελλιπής γιατί δεν μπορεί να προστατεύσει την πρώτη επίθεση προτού έχουν μια βάση δεδομένων που αποθηκεύει την απόδειξη προηγούμενων εγκρίσεων και αμφισβητούμενων συναλλαγών. Επιπλέον, η ανάπτυξη και η διατήρηση μιας τέτοιας βάσης δεδομένων είναι δαπανηρή[100].

4.5.4.Επιθέσεις και αντίστοιχα αντίμετρα στο επίπεδο της σύμβασης

Attack of smart contracts

Επίθεση

Τα smartcontracts είναι ουσιαστικά μια σειρά κωδικών προγράμματος και ο ακέραιος αριθμός στο smartcontract έχει το ανώτερο και το κάτω όριο. Η τιμή της παραλλαγής είναι πάνω από το ανώτερο όριο, τότε θα γίνει 0. Όταν η τιμή που αποθηκεύεται από την παραλλαγή είναι χαμηλότερη από το κατώτερο όριο, θα γίνει ο μεγαλύτερος αριθμός ακέραιου αριθμού[101]. Εκτός από τη διαδικασία αποθήκευσης παραλλαγής, μπορεί να συμβεί υπερχείλιση στη διαδικασία υπολογισμού και μετατροπής τιμής. Τον Ιούλιο του 2018, το BeautyChain (BEC) υπέστη από επίθεση υπερχείλισης ακέραιων αριθμών, προκαλώντας μεγάλη απώλεια[101].

Αντίμετρα

Η υπερχείλιση ακεραίων είναι ένα κοινό ζήτημα ασφάλειας στα smartcontractsEtherem. Το Lity αφαιρεί ενεργά την επίθεση υπερχείλισης ακέραιων αριθμών, αυξάνοντας την ασφάλεια tousmartcontract. Για να είμαστε πιο συγκεκριμένοι, το Lity χρησιμοποιεί δύο τρόπους για να διατηρήσει την επίθεση υπερχείλισης ακέραιου αριθμού από πτυχές κώδικα και πτυχές χρόνου εκτέλεσης

• Το Lity χρησιμοποιεί έναν ασφαλέστερο τύπο δεδομένων που ονομάζεται *safeuint,* οι λειτουργίες του οποίου τυλίγονται αυτόματα σε συναρτήσεις SafeMath.

• Το Virtual Machine που συνδέεται με το Lily ανιχνεύει υπερχείλιση ακέραιων κατά την εκτέλεση και σταματά το αντίστοιχο συμβόλαιο, αντί να συνεχίσει το σφάλμα.

Το Osiris είναι ένα πλαίσιο που συνδυάζει τη συμβολική εκτέλεση με την tarnish analysis που μπορεί να βοηθήσει στον έλεγχο της υπερχείλισης ακέραιων αριθμών στο smartcontract[101]. Ο Gao πρότεινε το Easyflow για την επίλυση επίθεσης υπερχείλισης ακεραίων στο Ethereum. Η Easyflow ταξινόμησε τα smartcontractsστις ακόλουθες κατηγορίες: ασφαλή συμβόλαια, εμφανείς υπερχειλίσεις, καλά προστατευμένες υπερχειλίσεις και πιθανές υπερχειλίσεις[102]. Στην αρχική τους αξιολόγηση, αυτή η μέθοδος μπορεί να ανιχνεύσει ακέραια σφάλματα υπερχείλισης σε ευάλωτη σύμβαση με μικρή επιβάρυνση. Επιπλέον, θα πρέπει να είστε προσεκτικοί κατά την κωδικοποίηση και να ελέγχετε το εύρος της ενημερωμένης

κατάστασης αυτών των παραλλαγών για να διαπιστώσετε εάν υπερχειλίζεται ή υποβάλλεται.

Re-entryattack (Επίθεση επανεισόδου)

Επίθεση

Οι επιθέσεις επανεισόδου προκαλούνται από ορισμένες λειτουργίες που δεν έχουν σχεδιαστεί για να εισάγονται εκ νέου από προγραμματιστές. Ταυτόχρονα, κακόβουλα συμβόλαια ονομάζουν αυτές τις λειτουργίες κατά τρόπο επαναλαμβανόμενο και τότε οι ειλικρινείς λογαριασμοί ενδέχεται να χάσουν [102]. Το συμβάν DAO (Digital Autonomous Organization) είναι ένα παράδειγμα επίθεσης επανεισόδου στο έξυπνο συμβόλαιο που συνέβη το 2016. Σε αυτήν την επίθεση, προκλήθηκαν απώλειες Ether αξίας 60 εκατομμυρίων από επιτιθέμενους που εκμεταλλεύονται τα μειονεκτήματα του κάτω ανοιχτού κώδικα.

Αντίμετρα

Ο καλύτερος τρόπος για να αποφύγετετην Re-entryattackείναι να χρησιμοποιήσετε τη λειτουργία μεταφοράς για να επιτύχετε λογαριασμούς μεταφοράς και να χρησιμοποιήσετε τη συνάρτηση απαιτεί για να ελέγξετε το αποτέλεσμα. Για χάρη της μείωσης της απώλειας της επίθεσης DAO, το Ethereum κάνει hard fork και διαιρεί την αλυσίδα σε ETH και ETC, αποσύροντας τη συναλλαγή κατά τη διάρκεια της επίθεσης[103]. Το ReGuard είναι μια αυτόματη ανίχνευση που μπορεί να κάνει δοκιμασίες για να αντιμετωπίσει το πρόβλημα των επιθέσεων εκ νέου εισόδου. Rodler et al. πρότεινε την ονομασία Sereum για την επίλυση του προβλήματος της επίθεσης εκ νέου εισόδου, εποπτεύοντας τη ροή δεδομένων του έξυπνου συμβολαίου με δυναμική παρακολούθηση της βλάβης. Το Sereum λειτουργεί σε υποχρεωτική λειτουργία και είναι ενσωματωμένο στο blockchainσύστημα[103]. Τα πειραματικά αποτελέσματα έδειξαν ότι το Sereum θα μπορούσε να προστατεύσει το υπάρχον smartcontractαπό την επίθεση εκ νέου εισόδου με αμελητέα έξοδα.

Shortaddressattack (Σύντομη επίθεση διευθύνσεων)

Επίθεση

Όταν καλείτε τη μέθοδο μεταφοράς για την απόσυρση κερμάτων, εάν επιτρέπεται στον χρήστη να εισαγάγει μια σύντομη διεύθυνση, αυτό συμβαίνει συνήθως επειδή η ανταλλαγή δεν έχει κάνει καμία επεξεργασία. Για παράδειγμα, η νομιμότητα του

μήκους της διεύθυνσης που έχει εισαγάγει ο χρήστης δεν επαληθεύεται, πράγμα που μπορεί να οδηγήσει σε επίθεση σύντομης διεύθυνσης.

Αντίμετρα

Τα smartcontracts ανταλλάσσουν πληροφορίες συναλλαγών μέσω σαφώς καθορισμένων διεπαφών σε μη αξιόπιστο κατανεμημένο δίκτυο, δίνοντας στους επιτιθέμενους την ευκαιρία να εξαπολύσουν επίθεση στοsmartcontract. Για να αντιμετωπίσουν αυτό το πρόβλημα, οι Feng et al. ανέπτυξε ένα σύστημα ανίχνευσης που ονομάζεται SmartScopy, το οποίο μπορεί να συνθέσει αυτόματα αντιμαχόμενες συμβάσεις για την προστασία της ασφάλειας τωνsmartcontracts. Στο σύστημα Ethereum, το SmartScopy πραγματοποιεί εξερεύνηση χώρου σύμφωνα με τη δυαδική διεπαφή εφαρμογήςπροδιαγραφή smartcontracts με κίνδυνο ασφάλειας[104]. Επιπλέον, το SmartScopy εισήγαγε την αξιολόγηση συμβόλων με βάση την περίληψη, μειώνοντας τον αριθμό των οδηγιών που αξιολογήθηκαν με σύμβολο χωρίς καμία επίδραση στην ακρίβεια ερωτήματος ευπάθειας. Τα αποτελέσματα των πειραμάτων αναφέρουν ότι το SmartScopy είναι καλύτερο από άλλους έξυπνους αναλυτές συμβάσεων, όπως το Oyente από την άποψη της ακρίβειας, της αξιοπιστίας και του χρόνου εκτέλεσης.

5.Βελτιώσεις ασφαλείας στο Blockchain

Η ασφάλεια του blockchain βασίζεται σε μεγάλο βαθμό σε κρυπτογραφικές τεχνικές. Τα τελευταία χρόνια, η κρυπτογραφική έρευνα έχει αποφέρει ανακαλύψεις που ενισχύουν σημαντικά την ασφάλεια των δικτύων blockchain. Αυτές οι εξελίξεις περιλαμβάνουν:

- Post-QuantumCryptography: Με την εμφάνιση των κβαντικών υπολογιστών, οι παραδοσιακοί κρυπτογραφικοί αλγόριθμοι μπορεί να γίνουν επιρρεπείς σε επιθέσεις. Η μετακβαντική κρυπτογραφία στοχεύει στην ανάπτυξη μεθόδων κρυπτογράφησης ανθεκτικών στις κβαντικές απειλές. Η ενσωμάτωση της μετακβαντικής κρυπτογραφίας σε συστήματα blockchain διασφαλίζει τη μακροπρόθεσμη ασφάλειά τους.
- Zero-Knowledge Proofs: Οι αποδείξεις μηδενικής γνώσης, όπως τα zk-SNARK, επιτρέπουν την επικύρωση των συναλλαγών χωρίς να αποκαλύπτονται ευαίσθητες πληροφορίες. Αυτή η τεχνολογία ενισχύει το απόρρητο και την εμπιστευτικότητα στα δίκτυα blockchain, καθιστώντας τα πιο ασφαλή για διάφορες περιπτώσεις χρήσης.

Βελτιώσεις Συναινετικού Μηχανισμού

Οι αλγόριθμοι συναίνεσης βρίσκονται στον πυρήνα της ασφάλειας του blockchain. Οι βελτιώσεις σε αυτόν τον τομέα οδήγησαν σε πιο ισχυρά και ασφαλή δίκτυα. Οι αξιοσημείωτες εξελίξεις περιλαμβάνουν:

- Proof of Stake (PoS): Το PoS έχει αναδειχθεί ως μια φιλική προς το περιβάλλον εναλλακτική λύση στη συναίνεση της ενεργοβόρας απόδειξης εργασίας (PoW). Το PoS ενισχύει την ασφάλεια απαιτώντας από τους επικυρωτές να ποντάρουν ένα σημαντικό ποσό κρυπτονομισμάτων ως εγγύηση. Η κακόβουλη συμπεριφορά θα είχε ως αποτέλεσμα την απώλεια περιουσιακών στοιχείων, δίνοντας κίνητρο για έντιμη συμμετοχή.
- Delegated Proof of Stake (DPoS): Το DPoS εισάγει ένα εξουσιοδοτημένο μοντέλο όπου οι κάτοχοι διακριτικών ψηφίζουν εκπροσώπους που επικυρώνουν τις συναλλαγές. Αυτό το σύστημα ελαχιστοποιεί τον κίνδυνο συγκέντρωσης και ενισχύει την ασφάλεια με τη συμμετοχή περιορισμένου αριθμού αξιόπιστων κόμβων.

Έξυπνη ασφάλεια συμβολαίου

Τα έξυπνα συμβόλαια είναι συμβάσεις αυτοεκτελούμενες με τους όρους της συμφωνίας απευθείας γραμμένους σε κώδικα. Οι ευπάθειες ασφαλείας στα έξυπνα συμβόλαια έχουν οδηγήσει σε σημαντικές απώλειες στο παρελθόν. Οι βελτιώσεις στην ασφάλεια των έξυπνων συμβολαίων περιλαμβάνουν:

- FormalVerification: Οι επίσημες τεχνικές επαλήθευσης χρησιμοποιούνται για να αποδειχθεί μαθηματικά η ορθότητα των έξυπνων συμβολαίων. Με την αυστηρή επαλήθευση του κώδικα, τα τρωτά σημεία και τα σφάλματα μπορούν να εντοπιστούν και να διορθωθούν πριν από την ανάπτυξη.
- Security Audits: Οι έλεγχοι ασφάλειας τρίτων έχουν γίνει μια τυπική πρακτική. Οι ανεξάρτητες εταιρείες εξετάζουν διεξοδικά τον κώδικα έξυπνων συμβολαίων για να εντοπίσουν τα τρωτά σημεία και να διασφαλίσουν τη συμμόρφωση με τις βέλτιστες πρακτικές ασφαλείας.

Διαχείριση Ταυτότητας και Πρόσβασης

Οι λύσεις διαχείρισης ταυτότητας και πρόσβασης (IAM) έχουν ενσωματωθεί σε δίκτυα blockchain για τη βελτίωση της ασφάλειας. Αυτά τα μέτρα περιλαμβάνουν:

- Decentralized Identity (DID): Τα συστήματα DID παρέχουν στους χρήστες έλεγχο των πληροφοριών ταυτότητάς τους, μειώνοντας τον κίνδυνο κλοπής ταυτότητας. Οι χρήστες μπορούν να μοιράζονται επιλεκτικά δεδομένα, διασφαλίζοντας το απόρρητο και την ασφάλεια.
- Multi-SignatureWallets: Τα πορτοφόλια πολλαπλών υπογραφών απαιτούν πολλά ιδιωτικά κλειδιά για την εξουσιοδότηση μιας συναλλαγής. Αυτό το πρόσθετο επίπεδο ασφάλειας αποτρέπει τη μη εξουσιοδοτημένη πρόσβαση και μειώνει τον κίνδυνο κλοπής κεφαλαίων.

Οι βελτιώσεις στην ασφάλεια του blockchain συνέβαλαν καθοριστικά στην επέκταση της χρησιμότητας και στην υιοθέτηση αυτής της μετασχηματιστικής τεχνολογίας. Καθώς το blockchain συνεχίζει να διεισδύει σε διάφορους κλάδους, η συνεχής έρευνα και ανάπτυξη μέτρων ασφαλείας θα είναι ζωτικής σημασίας για την αντιμετώπιση των αναδυόμενων απειλών και τη διασφάλιση της συνεχούς εμπιστοσύνης και ακεραιότητας των δικτύων blockchain. Με κρυπτογραφικές προόδους, βελτιώσεις του μηχανισμού συναίνεσης, έξυπνα μέτρα ασφάλειας συμβολαίων και ισχυρή διαχείριση ταυτότητας, η τεχνολογία blockchain είναι έτοιμη να εκπληρώσει την υπόσχεσή της για ασφαλή και αποκεντρωμένα συστήματα για ένα ευρύ φάσμα εφαρμογών.

6.Μελλοντικές κατευθύνσεις

Με βάση την παραπάνω συστηματική εξέταση σχετικά με την ασφάλεια των τρεχόντων συστημάτων blockchain , παραθέτουμε μερικές μελλοντικές κατευθύνσεις που θα ενθαρρύνουν τις ερευνητικές προσπάθειες σε αυτόν τον τομέα. Πρώτον, στις μέρες μας ο πιο δημοφιλής μηχανισμός συναίνεσης που χρησιμοποιείται στο blockchain είναι το PoW. Ωστόσο, ένα σημαντικό μειονέκτημα του PoW είναι η σπατάλη υπολογιστικών πόρων. Για την επίλυση αυτού του προβλήματος, το Ethereum προσπαθεί να αναπτύξει έναν υβριδικό μηχανισμό συναίνεσης των PoW και PoS. Η διεξαγωγή ερευνών και η ανάπτυξη πιο αποτελεσματικών μηχανισμών συναίνεσης θα συμβάλουν σημαντικά στην ανάπτυξη του blockchain.

Δεύτερον, με την αύξηση του αριθμού των dAPP που είναι πλούσια σε χαρακτηριστικά, η διαρροή απορρήτου και ο κίνδυνος blockchain θα είναι πιο σοβαρός. Το ίδιο το dAPP, καθώς και η διαδικασία επικοινωνίας μεταξύ του dAPP και του Διαδικτύου, αντιμετωπίζουν αμφότεροι κινδύνους διαρροής απορρήτου. Υπάρχουν μερικές ενδιαφέρουσες τεχνικές που μπορούν να εφαρμοστούν σε αυτό το πρόβλημα: codeobfuscation, applicationhardening, trustedexecutioncomputation(π.χ. Intel SGX) κ.λπ. Τρίτον, το blockchain θα παράγει πολλά δεδομένα, συμπεριλαμβανομένων πληροφοριών μπλοκ, δεδομένων συναλλαγών, σύμβασης bytecode, κλπ. Ωστόσο, δεν είναι έγκυρα όλα τα δεδομένα που είναι αποθηκευμένα στο blockchain.

Lunardi et.al. προτείνει έναν κατανεμημένο έλεγχο πρόσβασης στην αρχιτεκτονική που βασίζεται σε λογιστικό IoT. Λόγω του περιορισμένου χώρου αποθήκευσης στο gateway, οι συντάκτες προτείνουν να παραμετροποιήσουν και να ορίσουν τον όγκο των πληροφοριών που θα αποθηκευτούν στο τοπικό βιβλίο IoT, το οποίο αποθηκεύει μόνο τις νέες πληροφορίες στο καθολικό. Ωστόσο, οι συγγραφείς δεν ανέφεραν τη λύση για την αποθήκευση παλιών πληροφοριών στην εξωτερική αποθήκευση και τον τρόπο για να επιτευχθεί αυτό. Sharma et.al. προτείνετε μια κατανεμημένη αρχιτεκτονική που βασίζεται σε blockchain με ομιχλώδεις κόμβους ελεγκτή με δυνατότητα λογισμικού (SDN - Software-definednetworking) στην άκρη του δικτύου. Αξιοποιώντας μια κατανεμημένη αρχιτεκτονική κόμβων ομίχλης που χρησιμοποιεί SDN και blockchain, το προτεινόμενο μοντέλο προσπαθεί να φέρει υπολογιστικούς πόρους στην άκρη του δικτύου IoT. Αυτή η δομή μειώνει την καθυστέρηση πρόσβασης σε μεγάλες ποσότητες δεδομένων με ασφαλή τρόπο, ωστόσο, δεν αντιμετωπίζει ζητήματα αποθήκευσης blockchain.

Οι Wilkinson et.al προτείνουν ένα δίκτυο αποθήκευσης cloud P2P, το *Storj* , το οποίο επιτρέπει στους χρήστες να μεταφέρουν και να μοιράζονται δεδομένα χωρίς να βασίζονται σε τρίτο πάροχο δεδομένων. Το δίκτυο αποθήκευσης ελέγχει περιοδικά κρυπτογραφικά την ακεραιότητα και τη διαθεσιμότητα του αρχείου. Στο *Storj*, χρησιμοποιεί το MetaDisk, ένα blockchain για αποθήκευση μεταδεδομένων αποκέντρωσης, για να διατηρήσει τη συνέπεια μεταξύ των clouds. Παρόμοια με το *Storj, η Sia* είναι επίσης μια πλατφόρμα για αποκεντρωμένη αποθήκευση, η οποία επιτρέπει τον σχηματισμό συμβάσεων αποθήκευσης μεταξύ ομοτίμων. Στη *Sia* , απαιτείται από τους παρόχους αποθήκευσης να αποδεικνύουν, σε τακτά χρονικά διαστήματα, ότι εξακολουθούν να αποθηκεύουν τα δεδομένα του πελάτη τους.

7.Συμπεράσματα

Με την πρόσφατη τάση προς το blockchain, πολλές εφαρμογές και επιχειρήσεις κινούνται προς λύσεις που βασίζονται σε blockchain. Αυτό κατέστησε σημαντική την ολοκληρωμένη ανάλυση του blockchain όσον αφορά τα χαρακτηριστικά απόδοσης και ασφάλειας. Πρόσφατα, έχουν γίνει κάποιες ερευνητικές προσπάθειες σχετικά με τη σύγκριση των υφιστάμενων αλγορίθμων συναίνεσης που χρησιμοποιούνται στο blockchain και την πρόταση ενός νέου. Σε αυτήν την εργασία, συζητήσαμε λεπτομερώς τους μηχανισμούς συναίνεσης, τις κατηγορίες τους και τη σημασία στο κατανεμημένο περιβάλλον. Οι μηχανισμοί συναίνεσης συζητούνται γενικά για ένα κατανεμημένο σύστημα και συγκεκριμένα για το blockchain. Συγκρίναμε μερικούς πρόσφατα προτεινόμενους αλγόριθμους συναίνεσης όσον αφορά τον αριθμό των παραμέτρων που έχουν σημαντικό αντίκτυπο στον αλγόριθμο συναίνεσης. Οι παράμετροι που προσδιορίστηκαν για σύγκριση καλύπτουν τόσο θέματα ασφάλειας όσο και πτυχές απόδοσης. Στη συνέχεια συζητούνται οι αλγόριθμοι μαζί με κάθε μία από τις προσδιορισμένες παραμέτρους. Εκτός από αυτά, μια σειρά άλλων πτυχών είναι επίσης σημαντικές που πρέπει να ληφθούν υπόψη. Τοπολογία δικτύου (π.χ. πλήρως συνδεδεμένο γράφημα), ποσοστό συναλλαγών, συνέπεια που επιτυγχάνεται με τη λύση συναίνεσης, έλεγχος ταυτόχρονης λειτουργίας, ταχύτητα επαλήθευσης συναλλαγών και πολυπλοκότητα γύρων (εάν ο αλγόριθμος συναίνεσης περιλάμβανε πολλούς γύρους ή φάσεις). Για μελλοντική έρευνα, αυτές οι παράμετροι μπορούν να ενσωματωθούν για μια πιο λεπτομερή σύγκριση.

Η τεχνολογία Blockchain και η εφαρμογή των τεχνολογιών στα συστήματα IoT έχουν κερδίσει μεγάλη προσοχή τόσο από τον ακαδημαϊκό όσο και από τη βιομηχανία. Ωστόσο, είναι ένα δύσκολο πρόβλημα η αποθήκευση και διαχείριση blockchain σε δίκτυα IoT, λόγω των τεράστιων δεδομένων που παράγονται από εφαρμογές IoT και των περιορισμένων πόρων στις υποδομές IoT. Αυτό το έγγραφο πρότεινε μια ιεραρχική δομή αποθήκευσης για την αποθήκευση της πλειοψηφίας του blockchain σε clouds και τη διατήρηση των πιο πρόσφατων μπλοκ που δημιουργήθηκαν σε ένα δίκτυο επικάλυψης blockchain.

Βιβλιογραφία

[1] Jingjing Gu, Binglin Sun, Xiaojiang Du, Jun Wang, Yi Zhuang, Ziwang Wang, "Consortium Blockchain-based Malware Detection in Mobile Devices", *Access IEEE*, vol. 6, σελ. 12118-12128, 2018. Εμφάνισηάρθρου Πλήρεςκείμενο: PDF (7778KB) Μελετητής Google

[2] Yu Nandar Aung, Thitinan Tantidham, "Review of Ethereum: Smart home case study", *Πληροφορική (INCIT) 2017 2οΔιεθνέςΣυνέδριο*, σελ. 1-4, 2017. Εμφάνισηάρθρου πλήρουςκειμένου: PDF (180 KB) Μελετητής Google

[3] Muhamed Turkanović, Marko Hölbl, Kristjan Košič, Marjan Heričko, Aida Kamišalić, "EduCTX: Μιαπιστωτικήπλατφόρματριτοβάθμιαςεκπαίδευσηςμεβάσητο Blockchain", *Access IEEE*, vol. 6, σελ. 5112-5127, 2018. Εμφάνισηάρθρου Πλήρεςκείμενο: PDF (2125KB) Μελετητής Google

[4] Felix Hartmann, Xiaofeng Wang, Maria Ilaria Lunesu, «Αξιολόγησητωναρχικώνπροσφορώνκρυπτογράφησης: ηκατάστασητηςπρακτικής», *Blockchain Oriented Software Engineering (IWBOSE) 2018 International Workshop on*, pp. 33-39, 2018. Εμφάνισηάρθρου πλήρουςκειμένου: PDF (240 KB) Μελετητής Google

[5] Tiago M. Fernández-Caramés, Paula Fraga-Lamas, "A Review on the Use of Blockchain for the Internet of Things", *Access IEEE*, vol. 6, σελ. 32979-33001, 2018. Εμφάνισηάρθρου Πλήρεςκείμενο: PDF (2722KB) Μελετητής Google

[6] Leonardo da Costa, André Neto, Billy Pinheiro, Roberto Araújo, Antônio Abelém, Weverton Cordeiro, "DLCP: Έναπρωτόκολλογιατηνεξασφάλισητηςλειτουργίαςελαφρούπελάτησε blockchains", *Network Operations and Management Symposium (NOMS) 2018 IEEE / IFIP*, pp. 1- 6, 2018. Εμφάνισηάρθρου Πλήρεςκείμενο: PDF (176KB) Google Μελετητής

[7] Wazen M. Shbair, Mathis Steichen, Jérôme François, Radu State, "Πλαίσιοενορχήστρωσηςκαιπειραματισμού Blockchain: Μιαμελέτηπερίπτωσηςτου KYC", *Συμπόσιολειτουργίαςκαιδιαχείρισηςδικτύου (NOMS) 2018 IEEE / IFIP*, σελ. 1-6, 2018. Εμφάνισηάρθρου Πλήρεςκείμενο: PDF (2233KB) Μελετητής Google

[8] Bin Wen, Ziqiang Luo, Yazhi Wen, "Evidence and Trust: IoT Collaborative Security Mechanism", *Information Science and Technology (ICIST) 2018 Eighth International Conference on*, pp. 98-9, 2018. Εμφάνισηάρθρου Πλήρεςκείμενο: PDF (555KB) Μελετητής Google

[9] Weiqi Dai, Jun Deng, Qinyuan Wang, Changze Cui, Deqing Zou, Hai Jin, "SBLWT: A Secure Blockchain Lightweight Wallet Based on Trustzone", *Access IEEE*, vol. 6, σελ. 40638-40648, 2018. Εμφάνισηάρθρου Πλήρεςκείμενο: PDF (5089KB) Google Μελετητής

[10] Woo-Suk Park, Dong-Yeop Hwang, Ki-Hyung Kim, "A Tentp-based Two Factor Authentication Scheme for Hyperledger Fabric Blockchain", *Ubiquitous and Future Networks (ICUFN) 2018 Tenth International Conference on*, pp. 817-819, 2018 .Εμφάνισηάρθρου Πλήρεςκείμενο: PDF (5517KB) Μελετητής Google

[11] Christopher Ehmke, Florian Wessling, Christoph M. Friedrich, "Proof-of-Property - A Lightweight and Scalable Blockchain Protocol", *Emerging Trends in Software Engineering for Blockchain (WETSEB) 2018 IEEE / ACM 1st International Workshop on* , pp. 48-51 , 2018. Εμφάνιση πλήρους άρθρου : PDF (286KB) Μελετητής Google

[12] Dorota Lang, Maxim Friesen, Marco Ehrlich, Lukasz Wisniewski, JïrgenJasperneite, "Pursuing the Vision of Industrie 4.0: Secure Plug-and-Produce by Means of the Asset Administration Shell and Blockchain Technology", *Industrial Informatics (INDIN) 2018 IEEE 16th International Συνέδριοστις* ,σελ. 1092-1097, 2018. Εμφάνισηάρθρου Πλήρεςκείμενο: PDF (325KB) Μελετητής Google

[13] Yue Hao, Yi Li, Xinghua Dong, Li Fang, Ping Chen, "Ανάλυσηαπόδοσηςτουαλγόριθμουσυναίνεσηςσε Private Blockchain", *Intelligent Vehicles Symposium (IV) 2018 IEEE*, pp. 280-285, 2018. Εμφάνισηάρθρου Πλήρεςκείμενο: PDF (607KB) Μελετητής Google

[14] Nuttapong Klaokliang, Padungpol Teawtim, Phet Aimtongkham, Chakchai So-In, Aimaschana Niruntasukrat, "A Novel IoT Authorization Architecture on Hyperledger Fabric With Optimal Consensus using Genetic Algorithm", *Student Project Conference (ICT-ISPC) 2018* 1ο *ICT International International* , pp. -5, 2018. Εμφάνισηάρθρου Πλήρεςκείμενο: PDF (513KB) Μελετητής Google

[15] KeltoumBendiab, Nicholas Kolokotronis, Stavros Shiaeles, Samia Boucherkha, "WiP: A Novel Blockchain-based Trust Model for Cloud Identity Management", *Dependable Autonomic and Secure Computing 16th Intl Conf on Pervasive Intelligence and Computing 4th Intl Conf on Big Data Intelligence and Computing και Cyber Science and Technology Congress (DASC / PiCom / DataCom / CyberSciTech) 2018 IEEE 16th Intl*, pp. 724-729, 2018. Εμφάνιση πλήρους άρθρου : PDF (476KB) Μελετητής Google

[16] Magnus Westerlund, Nane Kratzke, "Towards Distattered Clouds: A Review About the Evolution of Central Computing Cloud Computed Ledger Technologies and A Foresight on Unifying Opportunities and Security Implications", *High Performance Computing & Simulation (HPCS) 2018 International Conference on*, pp. 655 -663, 2018. Εμφάνισηάρθρου Πλήρεςκείμενο: PDF (791KB) Μελετητής Google

[17] Alessio Meloni, Syam Madanapalli, Sanil Kumar Divakaran, Steven F. Browdy, Ambika Paranthaman, Ajay Jasti, Nishant Krishna, Deepak Kumar, "Exploiting the IoT Potential of Blockchain in the IEEE P1931.1 ROOF Standard", *Communications Standards Magazine IEEE*, vol. 2, όχι. 3, σελ. 38-44, 2018. Εμφάνισηάρθρου Πλήρεςκείμενο: PDF (703KB) Μελετητής Google

[18] Pietro Ferraro, C. King, Robert Shorten, "Distolved Ledger Technology for Smart Cities the Sharing Economy and Social Compliance", *Access IEEE*, vol. 6, σελ. 62728-62746, 2018. Εμφάνισηάρθρου Πλήρεςκείμενο: PDF (10291KB) Google Μελετητής

[19] Meryam Essaid, Hyeon Woo Kim, Woo Guil Park, Ki Young Lee, Se Jin Park, Hong Taek Ju, "Network Usage of Bitcoin Full Node", *Information and Communication Technology Convergence (ICTC) 2018 International Conference on*, pp. 1286-1291, 2018. Εμφάνισηάρθρου Πλήρεςκείμενο: PDF (479KB) Μελετητής Google

[20] Marcello Cinque, Christian Esposito, "Πώςναααξιολογήσετετηναξιοπιστίατωνεφαρμογώνστηνκορυφήτου Blockchain: Novel Research Challenges", *Dependable Computing Conference (EDCC) 2018 14th European*, pp. 164-165, 2018. Εμφάνισηάρθρου Πλήρεςκείμενο: PDF (107KB) Google Μελετητής

[21] D. Mingxiao, M. Xiaofeng, Z. Zhe, W. Xiangwei and C. Qijun, "A review on consensus algorithm of blockchain", *Systems Man and Cybernetics*

(SMC) 2017 IEEE International Conference on, pp. 2567-2572, 2017. Show in Context View Article Full Text: PDF (400KB) Google Scholar

[22] M. Castro, B. Liskov et al., "Practical byzantine fault tolerance", *OSDI*, vol. 99, pp. 173-186, 1999. Show in Context Google Scholar

[23] L. Tseng, "Recent results on fault-tolerant consensus in message-passing networks" in International Colloquium on Structural Information and Communication Complexity, Springer, pp. 92-108, 2016. Show in Context CrossRef Google Scholar

[24] G. Wang, Z. J. Shi, M. Nixon and S. Han, "Smchain: a scalable blockchain protocol for secure metering systems in distributed industrial plants", *Proceedings of the International Conference on Internet of Things Design and Implementation*, pp. 249-254, 2019. Show in Context Google Scholar

[25] *Storj white paper v3.0*, [online] Available: https://storj.io/storj.pdf. Show in Context Google Scholar

[26] A. Dorri, S. S. Kanhere, R. Jurdak and P. Gauravaram, "Blockchain for iot security and privacy: The case study of a smart home", *Pervasive Computing and Communications Workshops (PerCom Workshops) 2017 IEEE International Conference on*, pp. 618-623, 2017. Show in Context View Article Full Text: PDF (612KB) Google Scholar

[27] J. Benet, *Ipfs-content addressed versioned p2p file system*, 2014, [online] Available: Show in Context Google Scholar

[28] C. Cachin, "Architecture of the hyperledger blockchain fabric", *Workshop on Distributed Cryptocurrencies and Consensus Ledgers*, 2016. Show in Context Google Scholar

[29] B. N. Levine, C. Shields and N. B. Margolin, A survey of solutions to the sybil attack, Amherst, MA: University of Massachusetts Amherst, vol. 7, pp. 224, 2006. Show in Context Google Scholar

[30] L. A. Linn and M. B. Koo, "Blockchain for health data and its potential use in health it and health care related research", *ONC/NIST Use of Blockchain for Healthcare and Research Workshop*, 2016. Show in Context Google Scholar

[31] G. Zyskind and Nathan, "Decentralizing privacy: Using blockchain to protect personal data", *Security and Privacy Workshops (SPW) 2015 IEEE*, pp. 180-184, 2015. Show in Context View Article Full Text: PDF (603KB) Google Scholar

[32] T. Hardjono and N. Smith, "Cloud-based commissioning of constrained devices using permissioned blockchains", *Proceedings of the 2nd ACM International Workshop on IoT Privacy Trust and Security*, pp. 29-36, 2016. Show in Context Google Scholar

[33] A. M. Antonopoulos, Mastering Bitcoin: unlocking digital cryptocurrencies, O'Reilly Media, Inc., 2014. Show in Context Google Scholar

[34] D. Johnson, A. Menezes and S. Vanstone, "The elliptic curve digital signature algorithm (ecdsa)", *International journal of information security*, vol. 1, no. 1, pp. 36-63, 2001. Show in Context CrossRef Google Scholar

[35] K. Khujamatov, K Ahmad, E. Reypnazarov and D. Khasanov, "Markov Chain Based Modeling Bandwith States of the Wireless Sensor Networks of Monitoring System", *International Journal of Advanced Science and Technology*, vol. 29, no. 4, pp. 4889-4903, 2020. Show in Context Google Scholar

[36] M. Agiwal, A. Roy and N. Saxena, "Next generation 5G wireless networks: A comprehensive survey", *IEEE Communications Surveys & Tutorials*, vol. 18, no. 3, pp. 1617-1655, 2016. Show in Context View Article Full Text: PDF (16653KB) Google Scholar

[37] N. Panwar, S. Sharma and A. K. Singh, "A survey on 5G: The next generation of mobile communication", *Physical Communication*, vol. 18, pp. 64-84, 2016. Show in Context CrossRef Google Scholar

[38] I. Ahmad, S. Shahabuddin, T. Kumar, J. Okwuibe, A. Gurtov and M. Ylianttila, "Security for 5G and beyond", *IEEE Communications Surveys & Tutorials*, 2019. Show in Context View Article Full Text: PDF (6052KB) Google Scholar

[39] K. Christidis and M. DevetsikIoTis, "Blockchains and smart contracts for the internet of things", *Ieee Access*, vol. 4, pp. 2292-2303, 2016. Show in Context View Article Full Text: PDF (2747KB) Google Scholar

[40] Z. Zheng, S. Xie, H. Dai, X. Chen and H. Wang, "An overview of blockchain technology: Architecture consensus and future trends", *2017 IEEE International Congress on Big Data (BigData Congress)*, pp. 557-564, 2017. Show in Context View Article Full Text: PDF (248KB) Google Scholar

[41] C. Thuemmler, C. Rolffs, A. Bollmann, G. Hindricks and W. Buchanan, "Requirements for 5G based telemetric cardiac monitoring", *2018 14th International Conference on Wireless and Mobile Computing Networking and Communications (WiMob)*, pp. 1-4, 2018. Show in Context View Article Full Text: PDF (225KB) Google Scholar

[42] *5G and blockchain: The building blocks of the shared economy*, [online] Available: https://www.ericsson.com/enlblog/2019/10/5Gblockchain-shared-economy. Show in Context Google Scholar

[43] M. Chaudhry, *Joint ieee spectrum and comsoc talk test and measurement virtualization and blockchain: Enablers for 5G networks*, Nov 2018. Show in Context Google Scholar

[44] H. L. Cech, M. Großmann and U. R. Krieger, "A fog computing architecture to share sensor data by means ofblockchain functionality", *2019 IEEE International Conference on Fog Computing (ICFC)*, pp. 31-40, 2019. Show in Context Google Scholar

[45] F. Jameel, Z. Hamid, F. Jabeen, S. Zeadall and M. A. Javed, "Asurveyof device-to-device communications: Research issues and challenges", *IEEE Commun. Surv. Tutorials*, vol. 20, no. 3, pp. 2133-2168, 2018. Show in Context View Article Full Text: PDF (4884KB) Google Scholar

[46] A. Ahad, M. Tahir and K.-L. A. Yau, "5G -based smart healthcare network: Architecture taxonomy challenges and future research directions", *IEEE Access*, vol. 7, pp. 100747-100762, 2019. Show in Context View Article Full Text: PDF (11603KB) Google Scholar

[47] K. Christidis and M. Devetsikiotis, "Blockchains and smart contracts for the internet of things", *Ieee Access*, vol. 4, pp. 2292-2303, 2016. Show in Context View Article Full Text: PDF (2747KB) Google Scholar

[48] J. L. Zhao, S. Fan and J. Yan, *Overview of business innovations and research opportunities in blockchain and introduction to the special issue*, 2016. Show in Context Google Scholar

[49] M. Crosby, P. Pattanayak, S. Verma and V. Kalyanaraman, "Blockchain technology: Beyond bitcoin", *Applied Innovation*, vol. 2, pp. 6-10, 2016. Show in Context Google Scholar

[50] D. Yermack, "Corporate governance and blockchains", *Review of Finance*, vol. 21, no. 1, pp. 7-31, 2017. Show in Context CrossRef Google Scholar

[51] T. J. MacDonald, D. W. Allen and J. Potts, "Blockchains and the boundaries of self-organized economies: Predictions for the future of banking" in Banking Beyond Banks and Money., Springer, pp. 279-296, 2016. Show in Context CrossRef Google Scholar

[52] M. Pilkington, "11 blockchain technology: principles and applications", *Research handbook on digital transformations*, pp. 225, 2016. Show in Context CrossRef Google Scholar

[53] T. McConaghy, "Blockchain throughput and big data" in Bitcoin Startups, Berlin, vol. 28, Oct 2014. Show in Context Google Scholar

[54] D. Brandon, "The blockchain: The future of business information systems", *International Journal of the Academic Business World*, vol. 10, no. 2, pp. 33-40, 2016. Show in Context Google Scholar

[55] J. Mattila et al., "The blockchain phenomenon-the disruptive potential of distributed consensus architectures", *The Research Institute of the Finnish Economy Tech. Rep.*, 2016. Show in Context Google Scholar

[56] H. Watanabe, S. Fujimura, A. Nakadaira, Y. Miyazaki, A. Akutsu and J. J. Kishigami, "Blockchain contract: A complete consensus using blockchain", *Consumer Electronics (GCCE) 2015 IEEE 4th Global Conference on.*, pp. 577-578, 2015. Show in Context View Article Full Text: PDF (55KB) Google Scholar

[57] L. Luu, V. Narayanan, C. Zheng, K. Baweja, S. Gilbert and P. Saxena, "A secure sharding protocol for open blockchains", *Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security.*, pp. 17-30, 2016. Show in Context Google Scholar

[58] J. DESJARDINS, It's official: Bitcoin was the top performing currency of 2015, 2016. URL http://money.visualcapitalist.com/its-official-bitcoin-was-the-top-performing-currency-of-2015/. Google Scholar

[59] J. Adinolfi, and 2016's best-performing commodity is ... bitcoin? 2016. URL http://www.marketwatch.com/story/and-2016s-best-performing-commodity-is-bitcoin-2016-12-22 . Google Scholar

[60] blockchain.info, Confirmed transactions per day, 2017. URL https://blockchain.info/charts/n-transactions?timespan=all/#. Google Scholar

[61] A. Ekblaw, A. Azaria, J.D. Halamka, A. Lippman, A case study for blockchain in healthcare: medrec prototype for electronic health records and medical research data, 2016. URL https://www.media.mit.edu/publications/medrec-whitepaper/. Google Scholar

[62] A. Azaria, A. Ekblaw, T. Vieira, A. Lippman, Medrec: Using blockchain for medical data access and permission management, in: International Conference on Open and Big Data, OBD, 2016, pp. 25–30. Google Scholar

[63] Yue X., Wang H., Jin D., Li M., Jiang W. **Healthcare data gateways: Found healthcare intelligence on blockchain with novel privacy risk control** J. Med. Syst. (2016), p. 218 View Record in ScopusGoogle Scholar

[64] Huckle S., Bhattacharya R., White M., Beloff N. **Internet of things, blockchain and shared economy applications** Proc. Comput. Sci., 98 (2016), pp. 461-466 ArticleDownload PDFView Record in ScopusGoogle Scholar

[65] P. Bylica, Ł. Gleń, P. Janiuk, A. Skrzypczak, A. Zawłocki, A probabilistic nanopayment scheme for golem, 2015. URL http://golemproject.net/doc/GolemNanopayments.pdf. Google Scholar
[66] Hurich P. **The virtual is real: An argument for characterizing bitcoins as private property** Banking & Finance Law Review, Vol. 31, Carswell Publishing (2016), p. 573 View Record in ScopusGoogle Scholar
[67] A. Dorri, S.S. Kanhere, R. Jurdak, P. Gauravaram, Blockchain for iot security and privacy: The case study of a smart home, in: IEEE Percom Workshop on Security Privacy and Trust in the Internet of Thing, 2017. Google Scholar
[68] Zhang Y., Wen J. **The IoT electric business model: Using blockchain technology for the internet of things** Peer-to-Peer Netw. Appl. (2016), pp. 1-12 CrossRefView Record in ScopusGoogle Scholar
[69] Sun J., Yan J., Zhang K.Z. **Blockchain-based sharing services: What blockchain technology can contribute to smart cities** Financ. Innov. (2016), p. 26 CrossRefView Record in ScopusGoogle Scholar
[70] X. Xu, C. Pautasso, L. Zhu, V. Gramoli, A. Ponomarev, A.B. Tran, S. Chen, the blockchain as a software connector, in: The 13th Working IEEE/IFIP Conference on Software Architecture, WICSA, 2016. Google Scholar
[71] Nordström E. (Master's thesis) Personal Clouds: Concedo, Lulea University of Technology (2015) Google Scholar
[72] J.S. Czepluch, N.Z. Lollike, S.O. Malone, The use of block chain technology in different application domains, in: The IT University of Copenhagen, 2015, Copenhagen. Google Scholar
[73] Ethereum, Etherscan: The ethereum block explorer, 2017. URL https://www.ethereum.org/. Google Scholar
[74] L. Luu, D.-H. Chu, H. Olickel, P. Saxena, A. Hobor, Making smart contracts smarter, in: The 2016 ACM SIGSAC Conference on Computer and Communications Security, 2016, pp. 254–269. Google Scholar
[75] V. Buterin, Critical update re: Dao vulnerability, 2016. URL https://blog.ethereum.org/2016/06/17/critical-update-re-dao-vulnerability/. Google Scholar
[76] J. Adelstein, Behind the biggest bitcoin heist in history: Inside the implosion of mt.gox, 2016. URL http://www.thedailybeast.com/articles/2016/05/19/behind-the-biggest-bitcoin-heist-in-history-inside-the-implosion-of-mt-gox.html . Google Scholar
[77] N. Atzei, M. Bartoletti, T. Cimoli, A survey of attacks on ethereum smart contracts (sok), in: International Conference on Principles of Security and Trust, 2017, pp. 164–186. Google Scholar
[78] Zheng Z., Xie S., Dai H.-N., Wang H. **Blockchain challenges and opportunities: A survey** Internat. J. Web Grid Serv. (2016)Google Scholar
[79] M. Ghosh, M. Richardson, B. Ford, R. Jansen, A torpath to torcoin, proof-of-bandwidth altcoins for compensating relays, 2014. URL https://www.smithandcrown.com/open-research/a-torpath-to-torcoin-proof-of-bandwidth-altcoins-for-compensating-relays/. Google Scholar
[80] Intel, Proof of elapsed time (poet), 2017. URL http://intelledger.github.io/ . Google Scholar
[81] P. technologies, Proof of Authority Chains, 2017. URL https://github.com/paritytech/parity/wiki/Proof-of-Authority-Chains. Google Scholar

[82] E. community, Kovan - Stable Ethereum Public Testnet, 2017. https://github.com/kovan-testnet/proposal. Google Scholar
[83] L. Luu, Y. Velner, J. Teutsch, P. Saxena, Smart pool: Practical decentralized pooled mining, in: USENIX Security Symposium, 2017. Google Scholar
[84] Karl (Ph.D. thesis Security of Blockchain Technologies, Swiss Federal Institute of Technology (2016) Google Scholar
[85] Karl, Ethereum eclipse attacks, 2016. URL http://e-collection.library.ethz.ch/view/eth:49728Google Scholar
[86] A. Gervais, G.O. Karame, K. Wüst, V. Glykantzis, H. Ritzdorf, S. Capkun, On the security and performance of proof of work blockchains, in: The 2016 ACM SIGSAC Conference on Computer and Communications Security, 2016, pp. 3–16. Google Scholar
[87] CoinMarketCap, CryptoCurrency market capitalizations, 2017. URL https://coinmarketcap.com/. Google Scholar
[88] Swan M. Blockchain: Blueprint for a New Economy, O'Reilly Media (2015) Google Scholar
[89] B.L.S.A., Bitcoin wallet, 2017. URL https://blockchain.info/wallet/#/. Google Scholar
[90] BlockGeeks, what is cryptocurrency: Everything you need to know, 2016. URL https://blockgeeks.com/guides/what-is-cryptocurrency/. Google Scholar
[91] M. Bartoletti, L. Pompianu, an empirical analysis of smart contracts: Platforms, applications, and design patterns, in: 1st Workshop on Trusted Smart Contracts, 2017. Google Scholar
[92] BlockGeeks, Smart contracts: The blockchain technology that will replace lawyers, 2016. URL https://blockgeeks.com/guides/smart-contracts/. Google Scholar
[93] M. Iansiti and K. Lakhani, *The Truth About Blockchain" Harvard Business Review*, [online] Available: https://hbr.org/2017/01/the-truth-about-blockchain. Show in Context Google Scholar
[94] S. Nakamoto, *Bitcoin: A Peer-to-peer Electronic Cash System*, [online] Available: https://bitcoin.org/bitcoin.pdf. Show in Context Google Scholar
[95] G. Karame and E. Androulaki, Bitcoin and Blockchain Security, Norwood, MA: Artech House, 2016. Show in Context Google Scholar
[96] L. Lamport, R. Shostak and M. Pease, "The Byzantine Generals Problem", *ACM Transactions on Programming Languages and Systems*, vol. 4, no. 3, pp. 382-401, 1982. Show in Context Google Scholar
[97] M. Castro and B. Liskov, "Practical Byzantine Fault Tolerance and Proactive Recovery", *ACM Transactions on Computer Systems*, vol. 20, no. 4, pp. 398-461, 2002. Show in Context Google Scholar
[98] M. Correia, G. Veronese and L. Lung, "Asynchronous Byzantine consensus with 2f+1 processes", *Proc. 2010 ACM Symposium on Applied Computing - SAC '10*, 2010. Show in Context Google Scholar
[99] *NEO White Paper*, [online] Available: http://docs.neo.org/en-us/. Show in Context Google Scholar
[100] S. David, Y. Noah and B. Arthur, The Ripple Protocol Consensus Algorithm, Ripple Labs Inc. Show in Context Google Scholar
[101] S. King and S. Nadal, *PPCoin: Peer-to-Peer Crypto-Currency with Proof-of-Stake*, [online] Available: https://peercoin.net/assets/paper/peercoin-paper.pdf. Show in Context Google Scholar

[102] P. Vasin, BlackCoin's Proof-of-Stake Protocol v2, Blackcoin.co. Show in Context Google Scholar

[103] Kiayias, A. Russell, B. David and R. Oliynykov, "Ouroboros: A Provably Secure Proof-of-Stake Blockchain Protocol", *Advances in Cryptology - CRYPTO 2017*, pp. 357-388, 2017. Show in Context CrossRef Google Scholar

[104] D. Mazieres, *The Stellar Consensus Protocol: A Federated Model for Internet-Level Consensus" draft Stellar Development Foundation*, [online] Available: https://www.stellar.org/papers/stellar-consensus-protocol.pdf. Show in Context Google Scholar

[105] L.S. Sankar, M. Sindhu and M. Sethumadhavan, "Survey of consensus protocols on blockchain applications", *2017 4th International Conference on Advanced Computing and Communication Systems (ICACCS)*, 2017. Show in Context Google Scholar