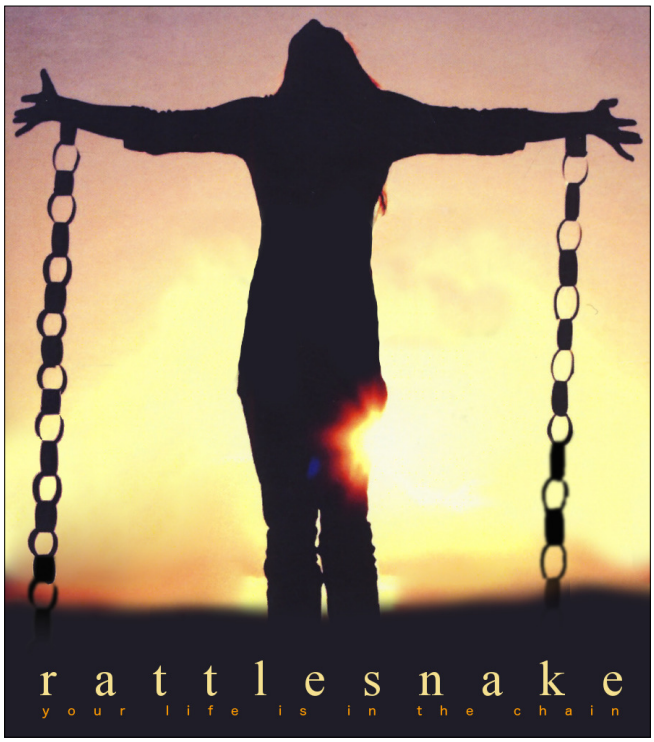
Rattlesnake

- your life is the chain -



DRAFT - White Paper

Preparato per: https://github.com
Preparato da: Mikro Varzè
14 gennaio 2018

PRESENTAZIONE

Cos'è Rattlesnake

Rattlesnake è la blockchain personale che tiene il segno dei momenti importanti della propria vita.

Obiettivo

Rendere reperibili ad ogni occorrenza dati relativi alla nostra salute, al percorso di studi, al curriculum lavorativo e tanti altri dati, privati o pubblici, senza dare limiti alla fantasia. Rendere possibile e inequivocabile l'identificazione personale rendendo di fatto impossibile la clonazione delle nostre identità. Portare la storia della nostra vita sempre con noi poiché è la storia della nostra vita che ci rende quello che siamo.

*****

Ogni blocco della propria catena contiene riferimenti ad almeno un'altra catena coinvolta che potrebbe essere anche referenziale (catena personale privata) il concatenamento tra catene avviene facendo riferimento a delle chiavi racchiuse nei blocchi referenziali di altre catene. Esplicitando: nel momento in cui inserisco nella mia catena un riferimento al mio stato di salute posso coinvolgere altre catene inserendo il codice referenziale del mio dottore personale o della ASUR che mi segue, oppure se registro la ricevuta di pagamento della farmacia posso coinvolgere il serve dell'agenzia delle entrate (per poter scaricare la spesa) e il mio dottore per confermare l'acquisto del medicinale, altro esempio il datore di lavoro che paga uno stipendio potrebbe coinvolgere il dipendente, la banca e l'INPS.

*****

Soluzione

L'utilizzo della tecnologia Blockchain unita ai vantaggi della piattaforma decentralizzata Ethereum e dell'archiviazione criptata dei dati nel cloud sono la soluzione adeguata in termini di sicurezza e irreversibilità dei dati.

Struttura del progetto e core dell'applicazione

Inserimento dati

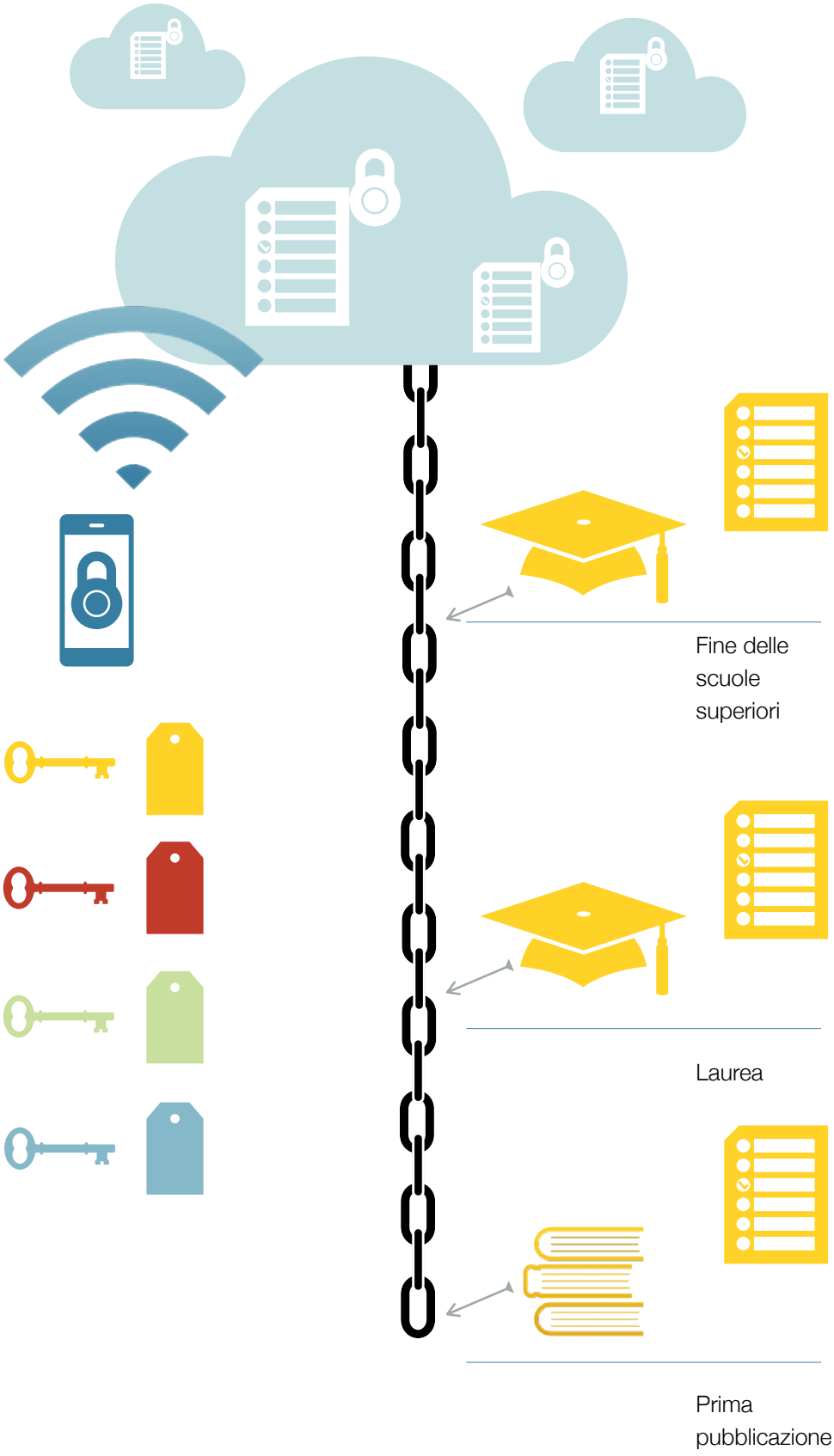
Attraverso un'applicazione posso inserire elementi nella mia personale blockchain.

Inserisco ogni evento attribuendo uno o più **TAG**.

Gli eventi possano essere di interesse pubblico o privato. Nel momento dell'archiviazione vengono criptati con chiavi diverse per ogni tipo di TAG.

Ogni inserimento sarà un anello della catena della mia storia.

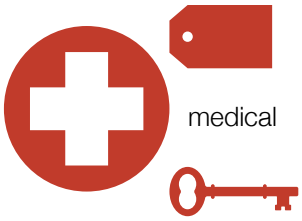
I miei studi e le mie pubblicazioni formeranno il mio curriculum che si aggiorna ogni qual volta inserisco nuovi eventi riguardanti la mia carriera.

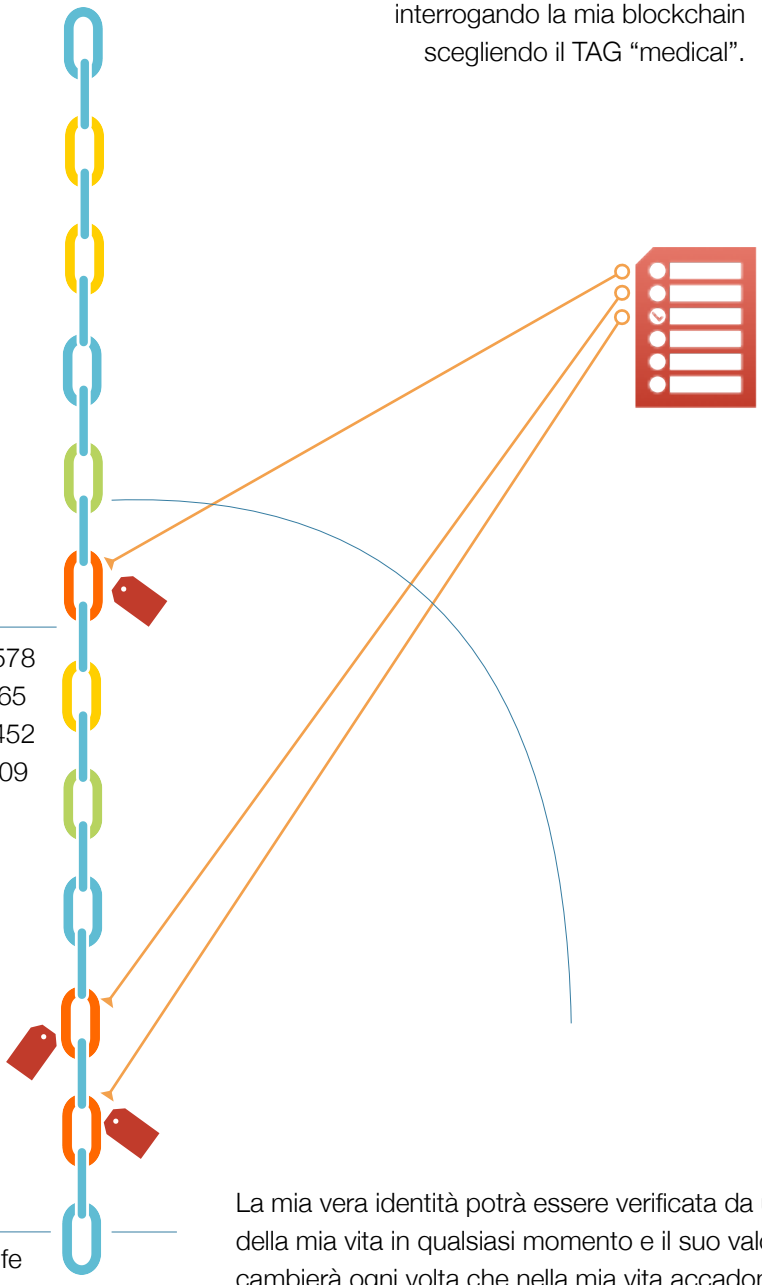


Ricerca dati

4179bfaf1
74de35ac
247edf3f8
4942f

Gli esami del sangue, le malattie sostenute, i vaccini, le allergie formeranno il mio stato sanitario, gli eventi relativi alla mia salute possono essere facilmente recuperati interrogando la mia blockchain scegliendo il TAG “medical”.





Verifica identità

ba215578
6f1bec65
52ba7452
19509f09

Verifica identità

8dd3b1fe
3da8ff308
a0a81fa98
524dd8

La mia vera identità potrà essere verificata da un Hash della mia vita in qualsiasi momento e il suo valore cambierà ogni volta che nella mia vita accadono nuovi eventi importanti

Funzionamento

esempio di caricamento di un nuovo blocco con nuovo documento da archiviare nella personale blockchain

in pratica:

aprire l'applicazione e selezionare nuovo Blocco

Tipo:

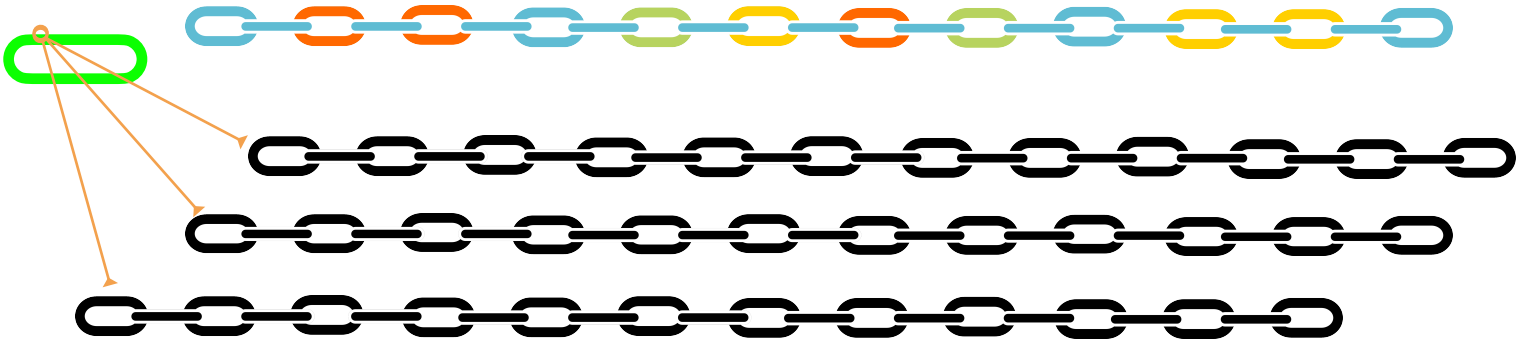
- nuovo documento

Seleziona/Carica:

- cerca documento o carica nuovo documento (.pdf, .odt, .jpg, .png, …)
- confermare hash del documento

Agganciare ancore:

- selezionare ancore alle Blockchain più comuni o individuare quelle personalizzate tramite la sezione ancore di riferimento.



Mining e archiviazione del Blocco (*)

- aggiungere il blocco alla Blockchain richiedendo il mining ai miner collaboratori (opzionale a pagamento l'archivio del documento nel cloud)

Mining e archiviazione del Blocco (*)

Prerequisiti

miner

il modello di mining si ispira al Proof-of-Work classico ma a bassi consumi, misto con delegated Proof-of-Stake in Trusted Network e delegated Byzantine Fault Tolerance.

i miner nella propria rubrica possono essere:

- soggetti singoli come amici o conoscenti che hanno l'applicazione installata e attiva sul telefono ed hanno acconsentito a partecipare al mining con i propri amici. Soggetti con hardware poco potente (a)(Trusted Network)
- gruppi di soggetti singoli ovvero amici che si uniscono in un gruppo, con hardware poco potente (a1)(Trusted Network). L'unirsi in un grippo permette di partecipare a ricompense più alte poiché in gruppo la potenza di calcolo aumenta e di conseguenza aumenta la difficoltà del blocco.
- singoli server delegati con hardware molto potente (b)(delegated Proof-of-Stake)
- gruppi di server delegati con hardware molto potente (b1)(delegated Proof-of-Stake)
- rete mista (a/b) (a1/b1) (a1/b) (a/b1)

fee

sono previste commissioni per blocchi superiori a un limite di MB stabilito e commissioni per l'archiviazione di documenti se richiesta, proporzionali al peso dei documenti archiviati. Non sono previste commissioni per il mining di blocchi classici con soli riferimenti (ancore) esterni ad altre Blockchain.

difficulty

Il codice del Core, una volta pronto il blocco da minare, controlla la lista dei possibili miner disponibili e in base alla capacità di calcolo a disposizione decide il valore di **difficoltà** del blocco

rewards

in base alla difficoltà del blocco in maniera proporzionale aumenta la **ricompensa** che viene data al miner che individua per primo il nonce.

Mining (the Core)

guida al codice del Core

Preparato il blocco da inserire nella Blockchain il core individua i contatti online che rispondono con un feedback positivo e con un parametro che indica la potenza di calcolo messa a disposizione.

In base alla quantità di potenza a disposizione nel trusted network, Il core calcola la difficoltà possibile e ragionevole da richiedere per minare il blocco (quantità di zeri iniziali nell'hash di convalida del blocco)

prima sezione di mining

In base all'esperienza pregressa viene indicato un valore minimo e un valore massimo per il nonce e viene diviso a blocchi per il numero di miner disponibili.

esempio di difficoltà 1 nonce minimo 0 fino a massimo 100 diviso per 5 miner disponibili:

progressive nonce : 1
progressive nonce : 2
progressive nonce : 3
progressive nonce : 4
progressive nonce : 5
progressive nonce : 6
progressive nonce : 7
progressive nonce : 8
progressive nonce : 9
progressive nonce : 10
progressive nonce max in this block: 10
last mining nonce 10
array random nonce: 11
array random nonce: 14
array random nonce: 12
array random nonce: 13
array random nonce: 18
array random nonce: 20
array random nonce: 19
array random nonce: 16
array random nonce: 17
array random nonce: 15
block random nonce from 10 to 20
[15, 17, 16, 19, 20, 18, 13, 12, 14, 11]
last mining random nonce 15
progressive nonce : 21
progressive nonce : 22
progressive nonce : 23
progressive nonce : 24
progressive nonce : 25
progressive nonce : 26
progressive nonce : 27
progressive nonce : 28
progressive nonce : 29
progressive nonce : 30
progressive nonce max in this block: 30
last mining nonce 30
array random nonce: 38
array random nonce: 37
array random nonce: 33
array random nonce: 39
array random nonce: 36
array random nonce: 35
array random nonce: 40
array random nonce: 34
array random nonce: 32
array random nonce: 31
block random nonce from 30 to 40
[31, 32, 34, 40, 35, 36, 39, 33, 37, 38]
last mining random nonce 31
progressive nonce : 41
progressive nonce : 42
progressive nonce : 43
progressive nonce : 44
progressive nonce : 45
progressive nonce : 46
progressive nonce : 47
progressive nonce : 48
progressive nonce : 49
progressive nonce : 50
progressive nonce max in this block: 50
last mining nonce 50
array random nonce: 51
array random nonce: 60
array random nonce: 54
array random nonce: 57
array random nonce: 56
array random nonce: 55
array random nonce: 59
array random nonce: 53
array random nonce: 52
array random nonce: 58
block random nonce from 50 to 60
[58, 52, 53, 59, 55, 56, 57, 54, 60, 51]
last mining random nonce 58
progressive nonce : 61
progressive nonce : 62
progressive nonce : 63
progressive nonce : 64
progressive nonce : 65
progressive nonce : 66
progressive nonce : 67
progressive nonce : 68
progressive nonce : 69
progressive nonce : 70
progressive nonce max in this block: 70
last mining nonce 70
array random nonce: 76
array random nonce: 72
array random nonce: 73
array random nonce: 75
array random nonce: 71
array random nonce: 78
array random nonce: 77
array random nonce: 74
array random nonce: 79
array random nonce: 80
block random nonce from 70 to 80
[80, 79, 74, 77, 78, 71, 75, 73, 72, 76]
last mining random nonce 80
progressive nonce : 81
progressive nonce : 82
progressive nonce : 83
progressive nonce : 84
progressive nonce : 85
progressive nonce : 86
progressive nonce : 87
progressive nonce : 88
progressive nonce : 89
progressive nonce : 90
progressive nonce max in this block: 90
last mining nonce 90
array random nonce: 93
array random nonce: 95
array random nonce: 94
array random nonce: 100
array random nonce: 92
array random nonce: 96
array random nonce: 98
array random nonce: 99
array random nonce: 91
array random nonce: 97
block random nonce from 90 to 100
[97, 91, 99, 98, 96, 92, 100, 94, 95, 93]
last mining random nonce 97
break into blocks of 20 elements
array: 5,1,20,21,40,41,60,61,80,81,100
array: [0][0] value undefined
array: [0][1] value undefined
array: [1][0] value 1
array: [1][1] value 20
array: [2][0] value 21
array: [2][1] value 40
array: [3][0] value 41
array: [3][1] value 60
array: [4][0] value 61
array: [4][1] value 80
array: [5][0] value 81
array: [5][1] value 100

Nella prima sezione di mining il core individua i miner disponibili (5 in questo caso a bassa potenza) , quindi imposta difficoltà a 1 e i un range di nonce possibili, in base alle esperienze pregresse (nonce usati su ultimi blocchi con stesso livello di difficoltà) in questo caso per difficoltà 1, numeri nonce compresi tra 1 e 100 possono essere i più idonei ad essere provati per primi. Si divide il numero totale dei nonce probabili 100 in 5 blocchi da 20 numeri che vengono passati ai miner in modo random.

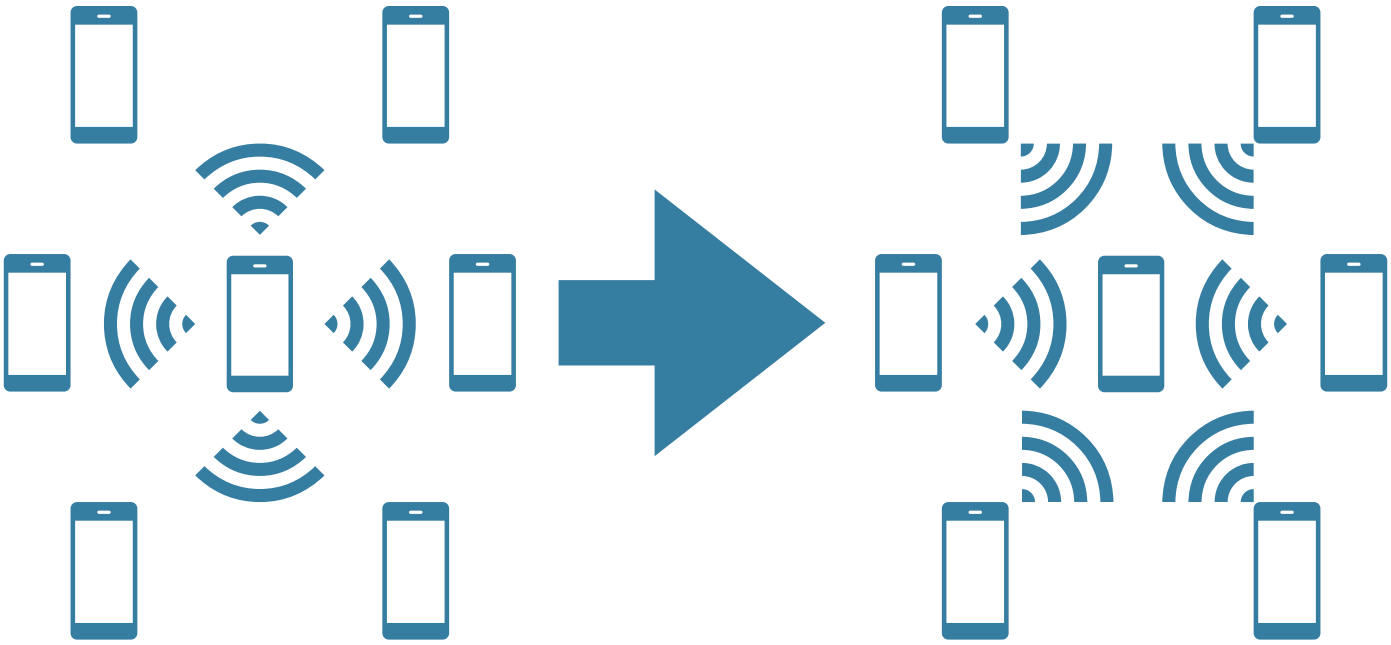
(*) Il miner che riceve il blocco a sua volta individua miner disponibili e suddivide il lavoro se molto oneroso.

Il gruppo di 20 numeri acquisito dal miner viene suddiviso a sua volta in 2 blocchi. Uno ordinato in modo crescente, verrà usato progressivamente aumentando il nonce di una unità per ogni ciclo di calcolo dell'hash e la restante metà verrà randomizzata. Per ogni nonce progressivo testato si testa anche uno nonce preso dall'array random. In questa maniera si possono ottenere risultati inaspettatamente più veloci nella risoluzione dell'hash.

(*) Nel caso la prima sezione di mining non ritorna la soluzione dell'hash si preparano nuovi blocchi progressivi e si inviano alla rete di miner fino alla risoluzione dellhash.

invio dei blocchi di nonce da provare

risposta dei miner



esempio di esperienza pregressa su blocchi da difficoltà 5

esempio dobbiamo minare il blocco 4 e abbiamo disponibili 3 amici in linea con hardware di tipo (a), essendo la potenza di calcolo a disposizione molto bassa il core decide per una difficoltà bassa pari a 5 (cinque zeri iniziali nell'hash di convalida del blocco) e una ricompensa adeguata al lavoro svolto


```
"index": 4,
        "timestamp": "01/05/2020",
        "data": {
            "type": "made in Italy"
        },
        "guna": {
            "tamas": [
                "Brioni",
                "Visa",
                "Certificato"
            ],
            "rajas": [
                "griffe",
                "pagamento",
                "made in check"
            ],
            "sattva": [
                "0xjkahdlgkjd",
                "0xdghjkgdahg20",
                "0xfd628417"
            ]
        },
        "previousHash":
"00000b49c15523199310d693a9813cc27d91f0afa67433f48cd5edae1c20888
73a8e39438b676828c056a44c7aa3325548359d8ab9f890f50b522cc218aa494
1",
        "hash":
"00000845a2cd8bfcd2d729e7af50854ae0e19d4a6b2e72b663bc2d983844679
e29858f42ebcf0a22a2a417f0321c167c0539a2ea0b11f34f2f346e10fc20f844",
        "nonce": 1788143
    }
],
"difficulty": 5
```