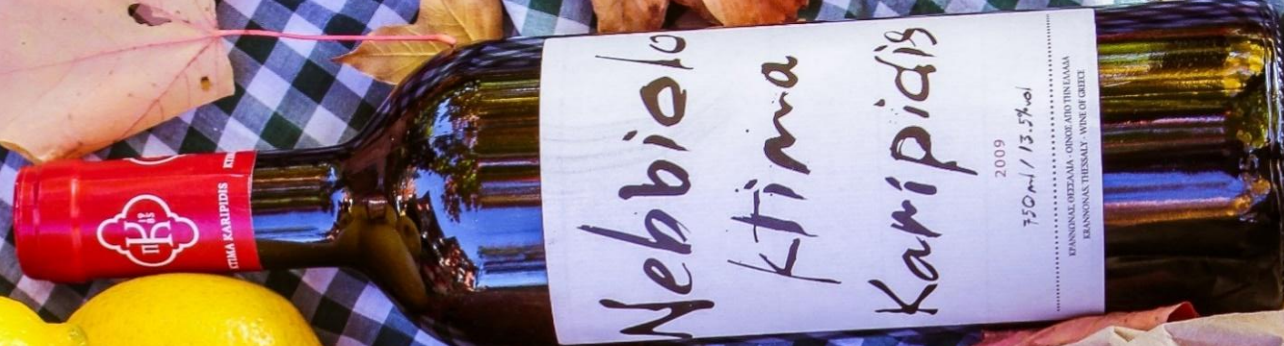




FOODCHAIN®
BLOCKCHAIN TECHNOLOGY FOR FOOD
SPA



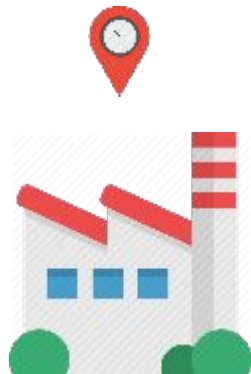
Chi siamo

Nel 2012 si avvia la fase di ricerca e sviluppo per ottenere una tecnologia digitale in grado di tracciare e rintracciare materie e prodotti, basata sulla blockchain.

Oggi, 2016, è nata la società **Foodchain spa** che lavora ogni giorno per raccontare la **storia** di ogni **prodotto alimentare**, utilizzando la tecnologia blockchain reingegnerizzata e messa a punto.

Cosa facciamo

Tracciamo e rintracciamo, attraverso la tecnologia blockchain, **materie e prodotti alimentari** raccogliendo **informazioni** da tutti gli **attori** che intervengono nelle filiere produttive.



Ogni **informazione** della filiera è coinvolta nel processo di tracciabilità ed è **resa disponibile via web e mobile senza dover ricorrere ad implementazioni onerose dei sistemi informativi interni**.

Come lo facciamo

Le **informazioni** inserite possono avere **diverse forme e senza limiti di dimensione** (immagini, documenti, video...)

Una volta immesse le informazioni **non possono essere più alterate o cancellate.**

Attraverso la nostra piattaforma web e la app mobile le **informazioni** possono essere rese **pubbliche all'intera filiera, condivise solo con alcuni operatori** della filiera o **private.**

Perché lo facciamo

Trasparenza

Univocità

Certezza

Inalterabilità

Sicurezza interna del prodotto

Sono i **principi fondamentali** che ispirano e alimentano il core business della società.

Vantaggi della tracciabilità

Il 47,6% delle aziende afferma che il fatto di possedere delle certificazioni impatta oltre l'80% sul fatturato registrato e riconosce il fatto che avere delle certificazioni aiuti molto a migliorare la reputazione aziendale, valorizzando i prodotti e migliorandone il controllo e la qualità.

Utilizzare **Foodchain** significa dotare la propria azienda di un **potente strumento ad alto valore aggiunto** in grado di ottenere grandi vantaggi atti al raggiungimento di **migliori risultati economici**.

Vantaggi della tracciabilità

Vantaggi derivati dalla tracciabilità:

aumento
dell'efficienza del
sistema produttivo

differenziazione dei prodotti e
creazione di valore aggiunto grazie
ad alti livelli di qualità e sicurezza

migliore gestione di
tutta la catena di
distribuzione

possibilità per azienda di
rendere alcuni dati
sensibili non visibili
all'intera filiera

facilità nel
controllo
qualità

facilità nel risalire
a prodotti non
conformi

aumento del
controllo di
produzione

Vantaggi della rin-tracciabilità

E' fondamentale ricordare che almeno la metà dei consumatori italiani è oggi disposta a pagare fino al 20% in più per avere un prodotto Made in Italy, e ci sarebbe anche un 12% che è pronto a spendere ancora di più pur di avere la garanzia dell'origine nazionale.

Utilizzare **Foodchain** significa dotare la propria azienda di un **potente strumento ad alto valore aggiunto** in grado di ottenere grandi vantaggi anche **verso i consumatori finali**.

Vantaggi della rin-tracciabilità

Vantaggi derivati dalla rin-tracciabilità:

Trasparenza dei prodotti
verso il consumatore finale

Impiego personalizzato di
marketing e politiche di marchio,
valorizzando le caratteristiche del
proprio prodotto

Percezione di un
comportamento etico
dell'azienda da parte del
consumatore

Razionalizzazione
della logistica

Fidelizzazione della
clientela

La tecnologia



La **catena a blocchi, Blockchain**, è la più recente, innovativa e sicura tecnologia di database. Nella Blockchain creata da Foodchain la memorizzazione di un qualsiasi dato implica la firma digitale dello stesso. In questo modo vengono garantiti autenticità e non modificabilità delle informazioni salvate.

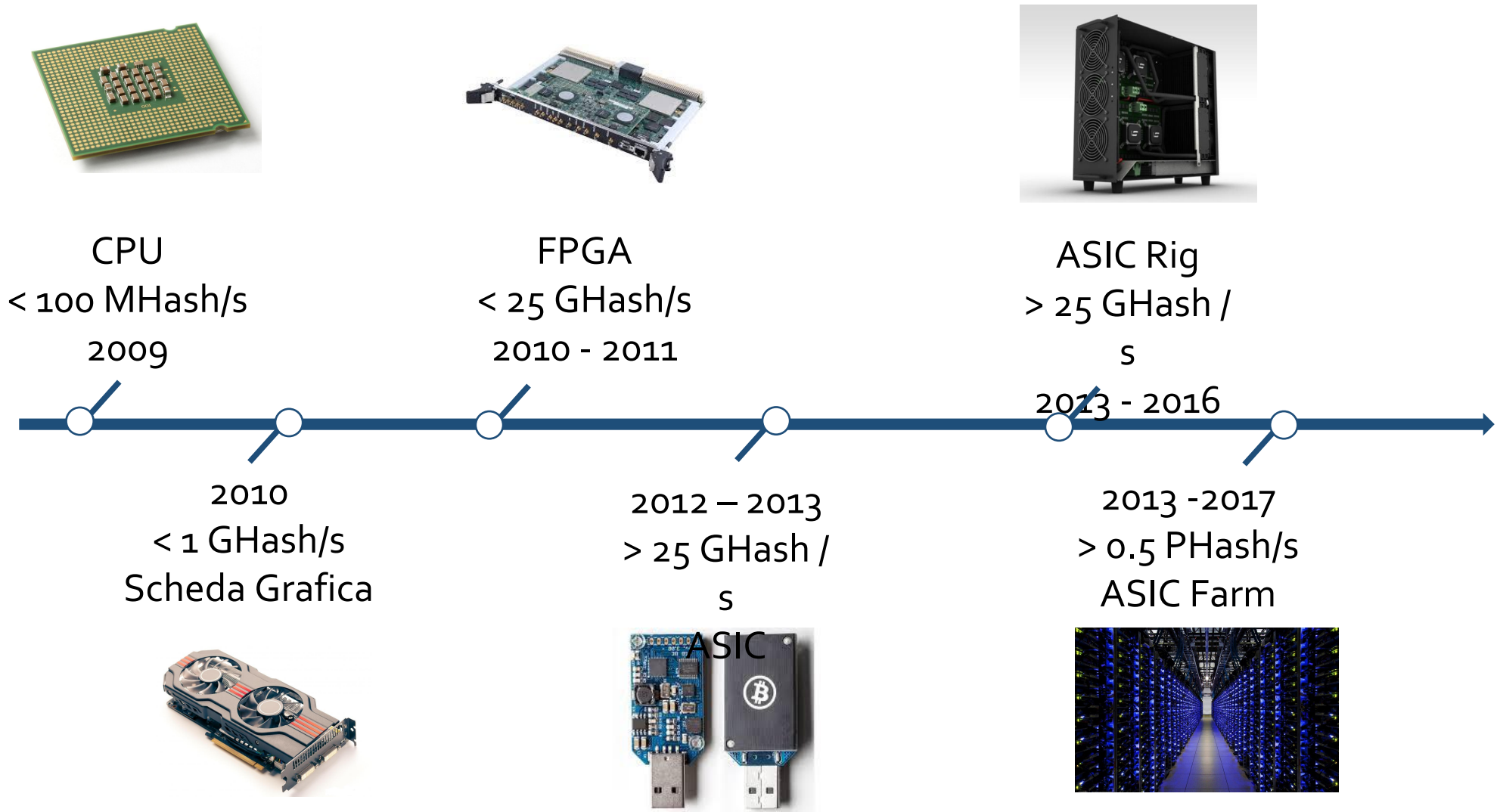


I **Validatori** sono dispositivi hardware che mantengono e aggiornano la Blockchain. Utilizzano la cifratura asimmetrica e forniscono il maggior livello di sicurezza informatica attualmente disponibile, superiore anche a quello bancario.



La **App Mobile** permette la lettura delle informazioni memorizzate nel database Foodchain. E' sufficiente avvicinare la fotocamera dello smartphone al QrCode del prodotto interessato per visualizzarne l'etichetta digitale.

Evoluzione SHA-256 PoW



Evoluzione SHA-256 PoW

Il consenso, decentralizzazione

- Il mining è il fondamento del meccanismo del consenso
- Le cryptovalute hanno dimostrato che una PoW dove il **bottleneck** è espressione di potenza di calcolo comporta una parziale centralizzazione del consenso
- Se viene a mancare il consenso distribuito è possibile 50% + 1 attacco



Alternative

1. Ethash PoW: algoritmo basato sulla velocità di accesso in memoria
2. Proof of Stake: il consenso è riposto nelle mani di chi possiede lo «stake», i **forgers**

Proof of Stake

“Proof-of-work is a really good system, but there’s probably going to be something better.”

Juan Benet - CEO of Protocol Labs

VANTAGGI:

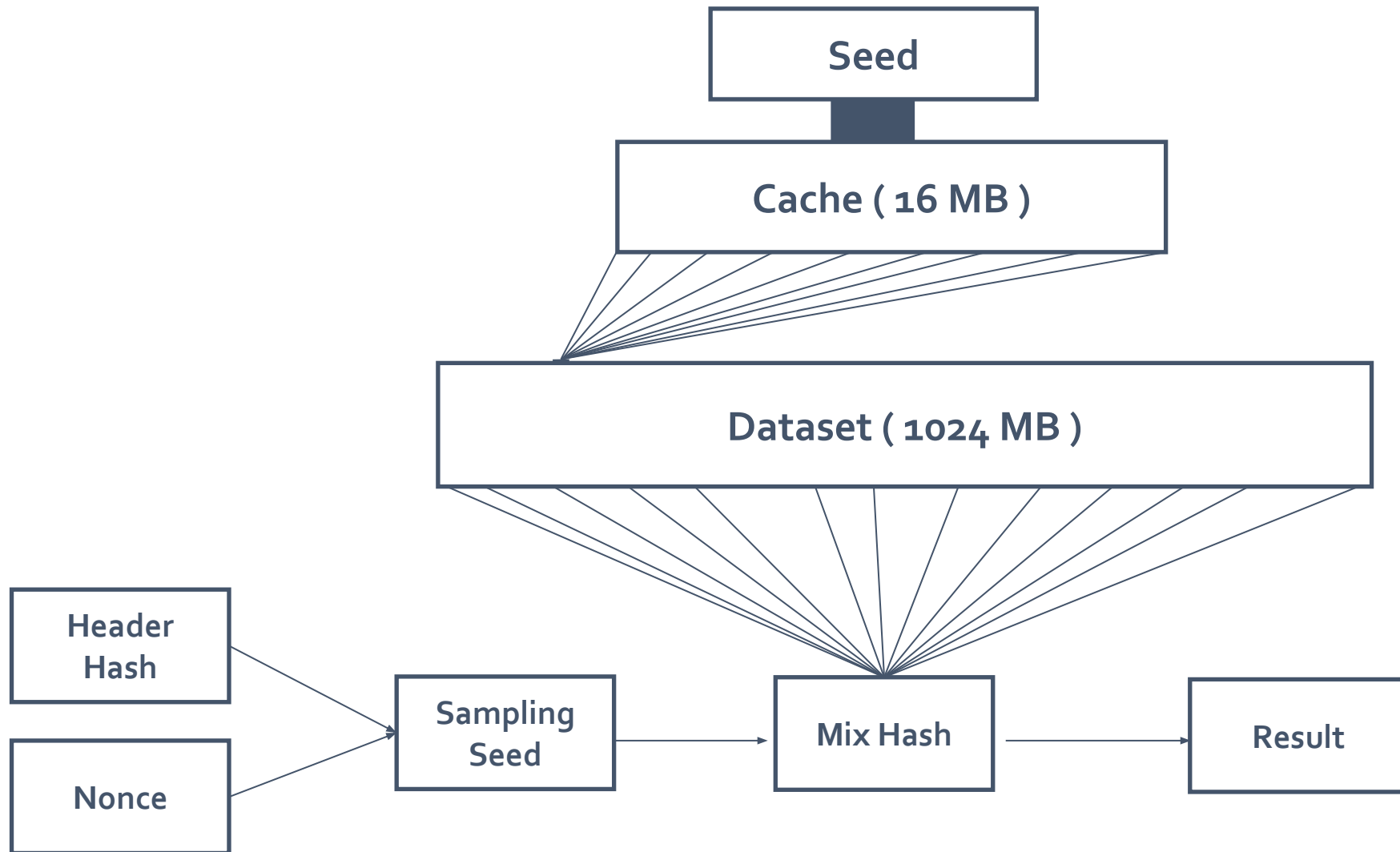
1. Riduce i consumi di energia (nel 2020 Bitcoin PoW consumerà come l’intera Danimarca)
2. Non necessita di hardware dedicato

SVANTAGGI:

1. Prevede una parte di controllo centralizzato a checkpoint sui blocchi
2. Solo chi possiede lo «stake» può «forgiare» nuova moneta
3. Sono tuttora in corso di discussione la resilienza a l’affidabilità per alcune tipologie di attacco

<http://www.coindesk.com/rethinking-proof-of-work-the-quest-to-improve-bitcoin-heats-up/>

Mining Ethash - Diagramma



Ethash PoW – Mining Cycle

GENEREAZIONE DAG

per minare in maniera efficiente il DAG deve essere pre-generato

1. Dato un blocco si procede al calcolo de **Seed** risalendo a tale blocco tramite gli **headers**
2. Dal seed si procede al calcolo della pseudorandom Cache 16MB tramite una *Strict Memory Hard Hashing Function*.
3. Dalla 16MB Cache si genera il **Dataset 1024 MB** , in parallelo. Ogni slice viene calcolata a partire da **256 parents** dalla 16MB Cache.

MINING

1. A partire dal Nonce e dall'Header Hash generare il Seed
2. Scegliere 64 random slice dal **Dataset** e calcolare il Mixhash per ottenere il risultato
3. Confrontare il risultato

Ethash PoW – Punti di forza

Resistente ad ASIC

sposta il *bottleneck* della potenza di calcolo sull'accesso in memoria. Di fatto rende meno probabile lo sviluppo di una tecnologia dedicata a questo scopo, dato che ci sono decine di aziende che già investono Mld di dollari in questa ricerca.

Alta Velocità di avvio

permette ad un Light Client di essere completamente operativo in meno di un minuto

Minatore facilmente reperibile

per partecipare al mining è sufficiente una scheda Grafica con almeno 2 GB GDDR5

Facile verifica per Light Client

permette ad un light client (che non ha a disposizione l'intera blockchain per effettuare la verifica di un round di mining) di verificare la validità di una transazione in qualche decimo di secondo anche con pochi MB di memoria a disposizione (seppur sempre crescente col crescere della dimensione della blockchain)