Panoramica su Alcune Attività di Ricerca in Cifrischain

Cifrischain 2018

Prof. Daniele Venturi
Dipartimento di Informatica

SAPIENZA
UNIVERSITÀ DI ROMA

Roma, 17 Dicembre 2018

Chi di noi fa Ricerca su Blockchain?

- Contributi raccolti:

UNIVERSITÀ DI TRENTO

Dipartimento di Matematica

UNIVERSITÀ DEGLI STUDI DI CAGLIARI

Dipartimento di Matematica e di Informatica

UNIVERITÀ DEGLI STUDI DI SALERNO

Dipartimento di Ingegneria dell'Informazione ed Elettrica e Matematica Applicata

SAPIENZA UNIVERSITÀ DI ROMA

Dipartimento di Informatica

Chiavi Segrete Deboli in Bitcoin

Generazione di Chiavi Segrete

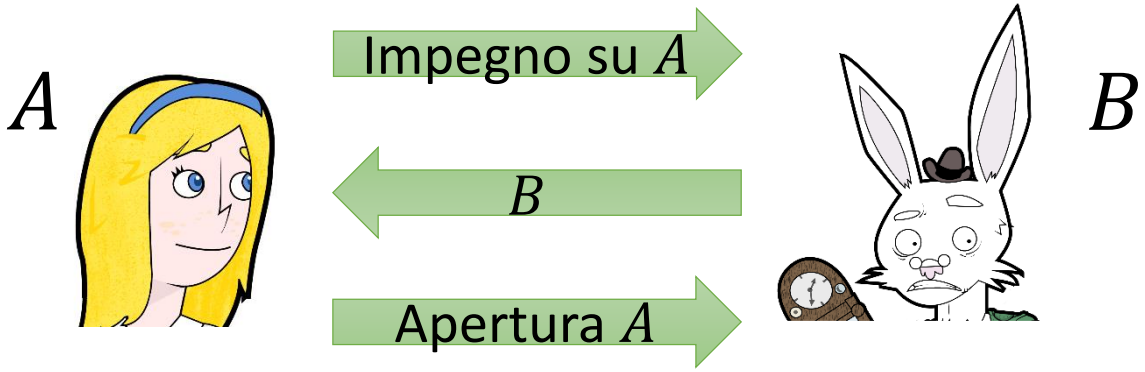
- Le transazioni Bitcoin sfruttano le firme digitali per trasferire crittovaluta tra diversi indirizzi
- Schema di firma usato: Elliptic Curve Digital Signature Algorithm (ECDSA)
  - Sicurezza basata sul problema del logaritmo discreto
- Chiavi algebraicamente deboli?
  - Individuate sfruttando alcune proprietà del gruppo moltiplicativo del campo finito dei coefficienti
  - Trovate 4 chiavi!

Lotterie Giuste Distribuite

Pubblicazioni:

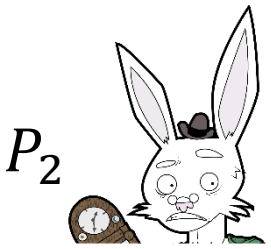
- Massimo Bartoletti, Roberto Zunino. "Constant-Deposit Multiparty Lotteries on Bitcoin". Financial Cryptography Workshops, 2017

Lancio di Moneta al Telefono



- Impegno digitale con hash: $\mathbf{H}(A||R)$ con R casuale
  - **Celante:** Non rivela informazione su A
  - **Vincolante:** Non può essere aperto con $A' \neq A$
- Mancanza di giustizia
  - Alice può rifiutarsi di aprire l'impegno

Specificare Condizioni in Bitcoin



P_2

$T_2 =$ | T_1 | 1 BTC | Condizione C_2 per spendere T_2 | Indizio W_2 |

Una funzione booleana

P_3

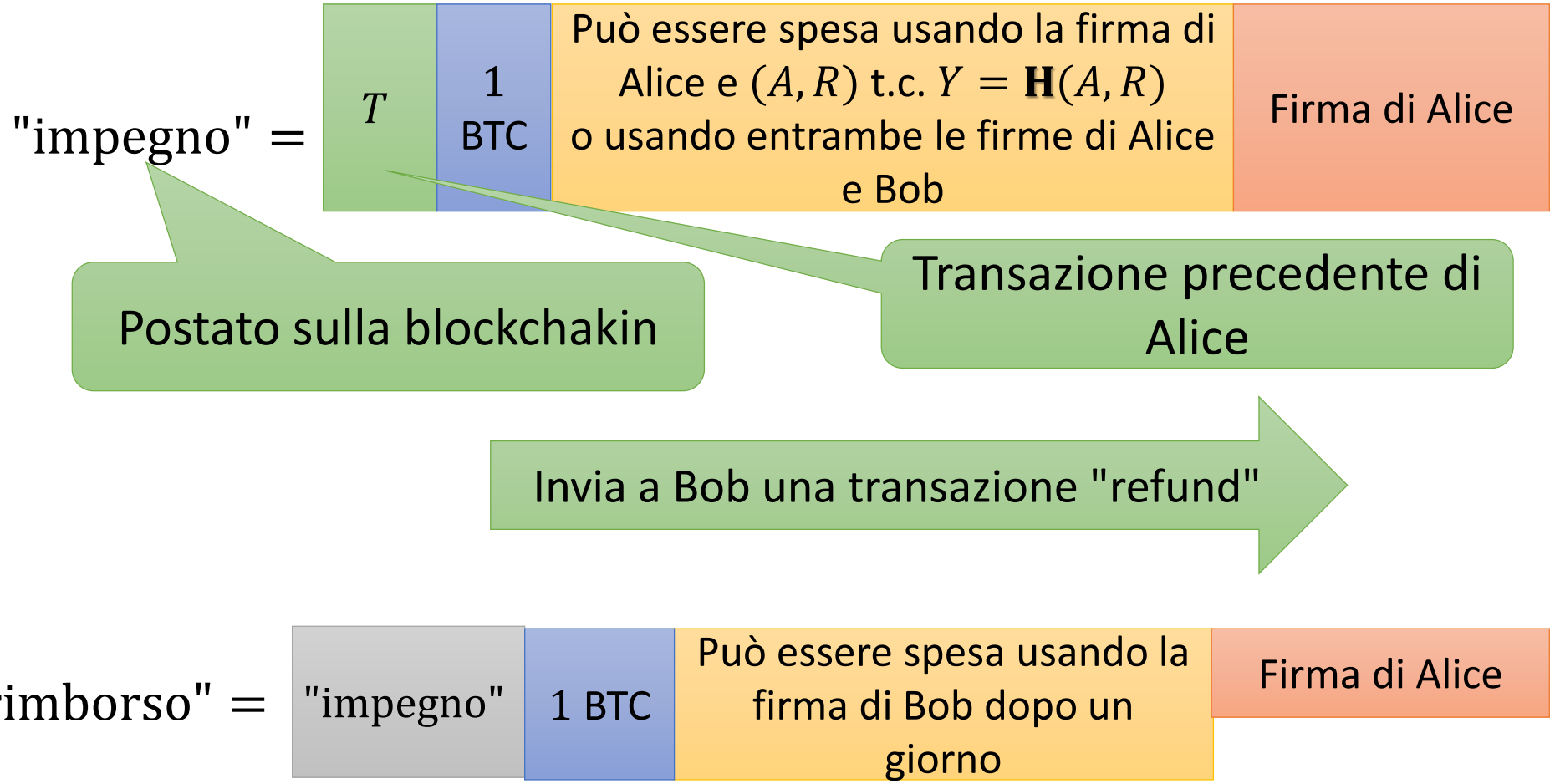
$[T_3]$

$T_3 =$ | T_2 | 1 BTC | Condizione C_3 per spendere T_3 | Indizio W_3 |

- T_3 redime T_2 se C_2 ritorna vero su input $([T_3], W_3)$
- Transazioni classiche:

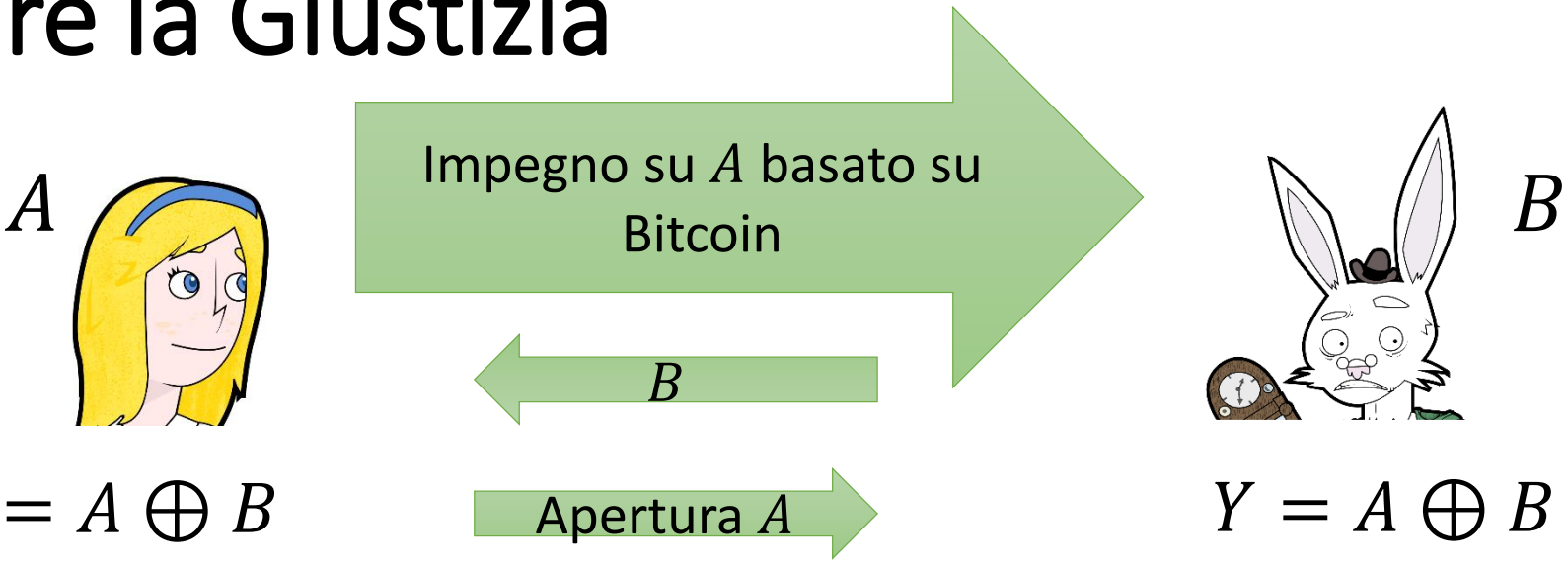
$$C_2([T_3], W_3) = \mathbf{V}(pk_2, [T_3], W_3)$$

Impegno basato su Bitcoin



SAPIENZA UNIVERSITÀ DI ROMA

Assicurare la Giustizia



- Se Alice non apre l'impegno entro un giorno, Bob ottiene 1BTC postando la transazione "rimborso"
- Altrimenti Alice riottiene 1BTC

Il Caso delle Lotterie: Risultati

	Andrychowicz & al. 2014	Bentov & Kumaresan 2014	Miller & Bentov 2017 v1	Miller & Bentov 2017 v2	Bartoletti & Zunino
Deposito	$N(N-1)$	$O(N^2)$	0	0	$d \geq 0$
Tempo	$O(1)$	$O(N)$	$O(\log N)$	$O(\log N)$	O(log N)
Transazioni "off-chain"	$O(N^2)$	-	$O(2^N)$	$O(N^2)$	$O(N^2)$
Transazioni "on-chain"	$O(N)$	$O(N^2)$	$O(N^2)$	$O(N)$	$O(N)$
Caratteristiche Bitcoin			SegWit	SegWit **MULTIINPUT** *(no interferences)*	SegWit **in-malleability**

Blockchain Riscrivibile

Pubblicazioni:

- Giuseppe Ateniese, Bernardo Magri, Daniele Venturi, Ewerton Andrade. "Redactable Blockchain – or – How to Rewrite History in Bitcoin and Friends". IEEE Euro S&P, 2017

Brevetti (con Accenture spa):

- Hybrid Blockchain, Patent n. 9959065, May 2018.
- Distributed Key Secret for Rewritable Blockchain, Patent n. 9774578, September 2017.
- Multiple-Link Blockchain, Patent n. 9785369, October 2017.

Perché Riscrivere la Blockchain?

- Per rimediare ad errori umani
  - Rispettare regolamenti legislativi e risolvere "bachi"
- "General Data Protection Regulation" (GDPR)
  - Le violazioni della privacy comportano multe salate: 4% dei ricavati annuali o 20 MLN EURO
- Gli "smart contracts" richiedono flessibilità
  - Vedere incidente DAO con 60 MLN USD rubati
- Scalabilità

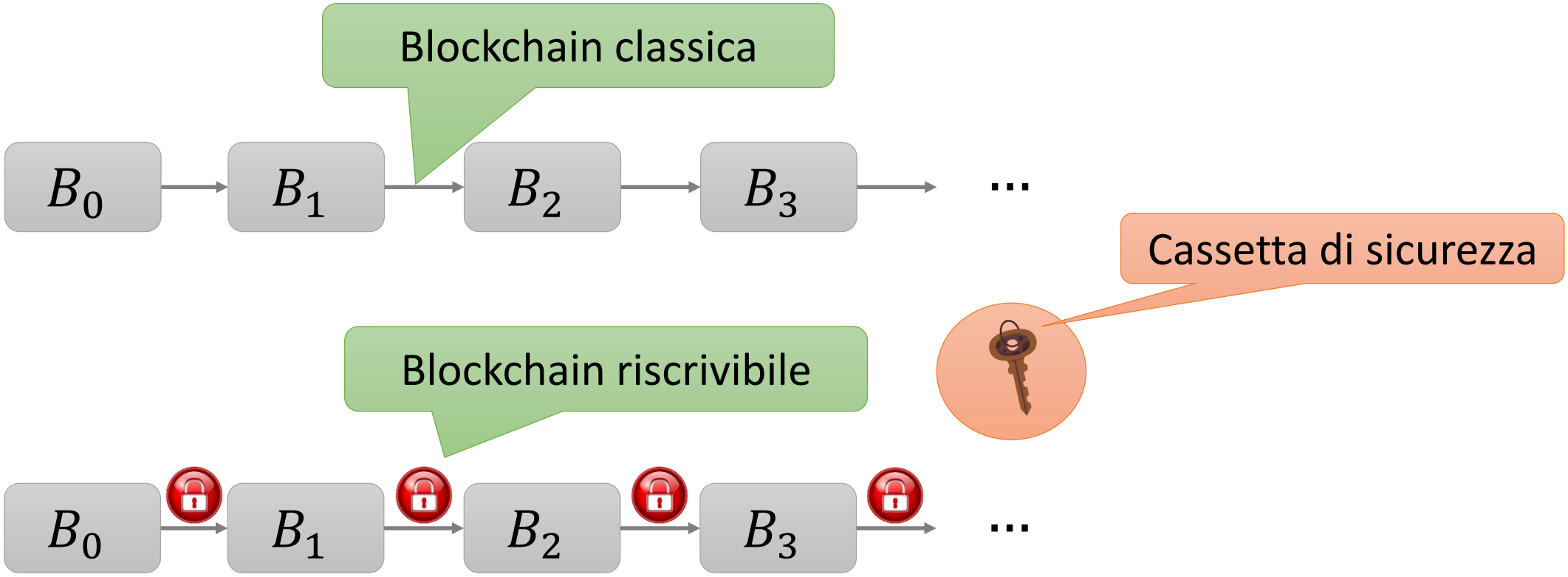
Una Soluzione Semplice?

- Effettuare il "chaining" solo tra gli hash dei dati; la rimozione dei dati non disturba quindi il "chaining"
- Non funziona! La blockchain non è solo un deposito di dati
  - Hash come prova di esistenza
  - L'esecuzione di "smart contract" richiede una evoluzione di stati correlati
  - L'integrità non deriva solo dal "chaining" ma anche dai dati stessi
- Necessità di riscrivere il blocco nella sua interezza

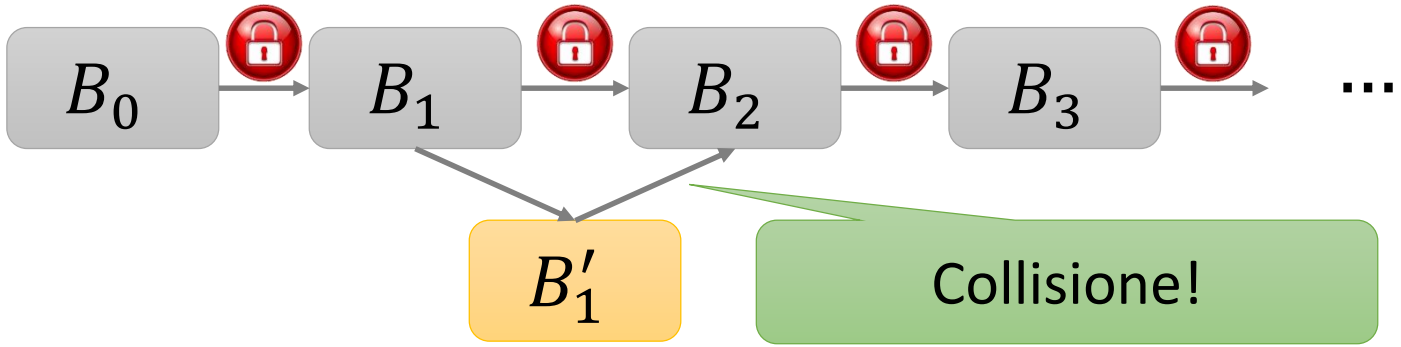
Blockchain Private e Pubbliche

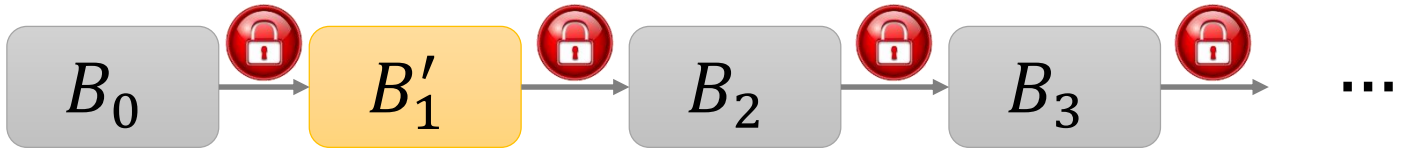
- La blockchain riscrivibile resta decentralizzata ed immutabile
  - Nessun server centralizzato
  - Utenti maliziosi non sono in grado di riscrivere blocchi
- Blockchain private ("permissioned")
  - Amministratori fidati possono riscrivere o rimuovere blocchi sulla base di regole di governance ben precise
- Blockchain pubbliche ("permissionless")
  - Più complicato capire chi può fare modifiche nel caso in cui chiunque possa aggiungersi al sistema

Il Caso di Blockchain Privata

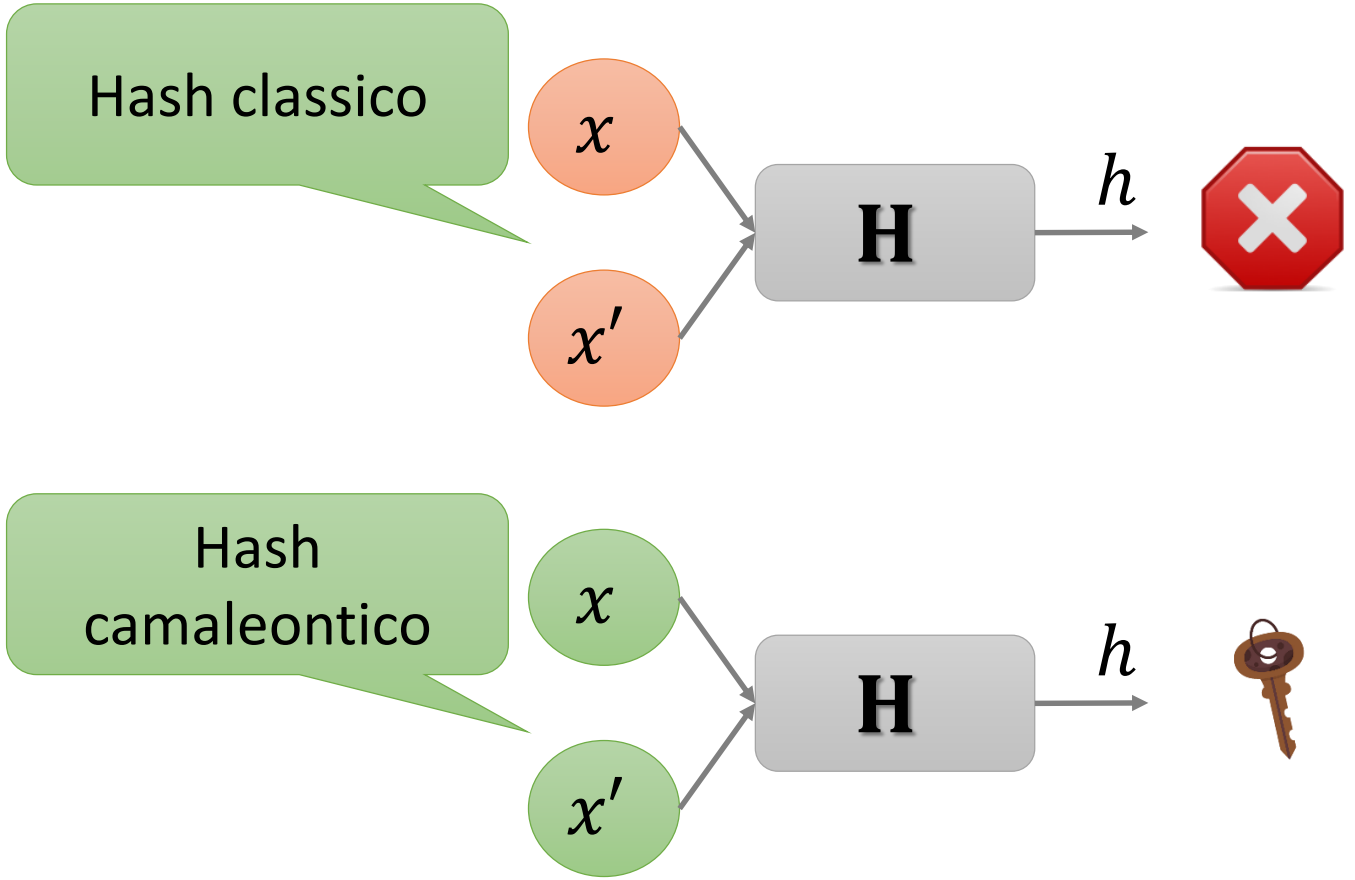


Cambiare un Blocco

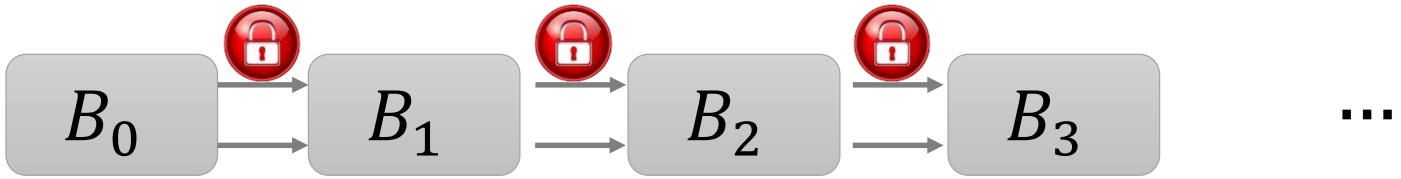


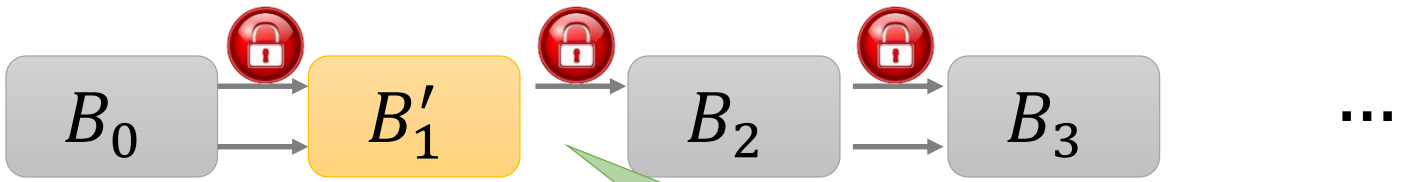


Hash Camaleontico



Lasciare una Cicatrice Incancellabile





Collegamento mancante!

Una Soluzione Alternativa

- Idea: Sfruttare le firme digitali di una maggioranza delle organizzazioni del consorzio
- Firme raccolte per validare ogni blocco
  - Ogni blocco include il valore di un contatore
- Sovrascrivere un blocco significa ricalcolarlo e questo non ha impatto sui blocchi successivi
  - Il "chaining" viene dagli identificativi dei blocchi e dalla certificazione fornita dalle firme

Il Caso di "Hyperledger Fabric"

- Si può invalidare un blocco aggiornando dei metadati
- Interpretazione della GDPR secondo cui i dati privati non più necessari non devono essere "logicamente" disponibili
  - I dati "logicamente" rimossi non sono più disponibili agli "smart contracts" ed alle altre applicazioni che accedono alla blockchain
  - Eccetto quelle coinvolte nel processo di consenso

Il Caso di Blockchain Pubblica

- Impossibile in generale
  - Contraddirebbe la dinamicità delle blockchain pubbliche
  - I nuovi partecipanti devono essere in grado di verificare l'intera blockchain
- Tuttavia esaminando casi specifici (es. Bitcoin) modifiche ad-hoc possono evitare l'inserimento di dati arbitrari
  - Prevenire è possibile
  - Chaining più complesso che permetta di eliminare gli eventuali dati privati apparsi in una transazione, lasciando tuttavia in piedi la logica della stessa

Progetto PRIViLEDGE

- Privacy-Enhancing Cryptography in Distributed Ledgers
- Progetto H2020
  - Dal 2018 al 2020
  - Circa 4.5M EUR (10 partner)
  - U. Salerno, IBM Zurich, Guardtime, IOHK, U. Edinburgh, TUE, ...
- U. Salerno è workpackage leader per "Privacy-enhancing cryptography"
  - "Zero-knowledge proofs", "publicly verifiable proofs", "verifiable secure computation", ...

Didattica

Università di Trento e FBK

- Università di Trento
  - Corsi di formazione per le aziende e per le banche dal 2013
  - Evento "Bitcoin e Altcoin: Applicazioni e Limitazioni", 2015
  - Workshop su "Trusted Smart Contracts", FC 2017
- Fondazione Bruno Kessler
  - Workshop su Blockchain per il corso "Introduction to computer and network security" al DISI
  - Lezioni su Blockchain, Dipartimento di Sociologia e Facoltà di Legge, Università di Trento

Accenture

- Partecipazione alla "London Blockchain Week" 2018
- Partecipazione al "Security Blockchain Workshop" 2018 (Dublino)
- Speaker su tematiche Blockchain al "Campus Party" 2018
- Blockchain Speech e Workshop alle Università
  - Federico II, Statale di Milano (sede Crema), Università della Calabria, Università di Padova, Università di Pisa per le Facoltà di Informatica/Ingegneria Informatica/Sicurezza Informatica

Eustema

- Attività di formazione come membro del gruppo di lavoro volontario sulla tecnologia blockchain nei processi dell'Amministrazione Comunale di Napoli
- Partecipazione ed eventi di divulgazione tecnico-scientifica (es. evento DeCifris presso Università di Salerno)
- Partecipazione a tavoli di associazioni pubblico-private per favorire il trasferimento tecnologico (es. ANITEC, CDTI, Canova Digitale, ecc.)

Università di Cagliari

- Corso in Cybersecurity della Laurea Magistrale in Informatica
  - Crittovalute e "smart contracts"
- "Summer school" su "distributed ledger technologies" (Giugno 2018)
  - Polo tecnologico di Pula, Sardegna
  - http://www.crs4.it/news-view/blockchain-and-distributed-ledger-technology-school/

Università di Milano

- Corso di Crittografia 1 (A.A. 2018/2019)
  - Argomenti trattati: Cryptocurrencies, Blockchain, e applicazioni varie (6 ore)
- Corso di perfezionamento UniMI (Aprile 2019)
  - Argomenti trattati: Blockchain technology (15 ore)

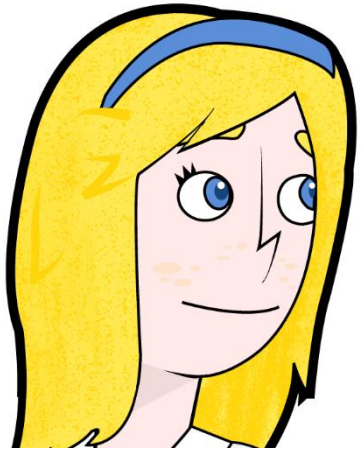
Università di Salerno

- Laurea Magistrale in Ingegneria Informatica
  - Corso: Sicurezza Informatica
  - Docente: Ivan Visconti per 3 CFU (24 ore)
- Argomenti trattati:
  - Blockchain permissionless, Bitcoin, Ethereum, Smart Contracts, Blockchain permissioned, Hyperldger Fabric

Sapienza Università di Roma

- Laurea Magistrale in Data Science
  - Corso "Data Privacy and Security" (6 CFU)
- Laurea Magistrale in Cybersecurity
  - Corso "Secure Computation" (6 CFU)
- Argomenti trattati:
  - Bitcoin, Smart contracts, Algorand, Spacemint, Zerocash

Grazie!



Per approfondire:

http://danieleventuri.altervista.org/

Recent Developments

- The "right to be forgotten"
  - A real case has stalled after the European Court of Justice found a Dutch man's identity information was uploaded on the Bitcoin blockchain
- The Open Data Institute (ODI) Report:
  - "Immutable data storage in blockchains may be incompatible with legislation which requires changes to the official truth"
  - "Even if personal data is not stored on a blockchain, metadata can be sufficient to reveal information"

SAPIENZA UNIVERSITÀ DI ROMA

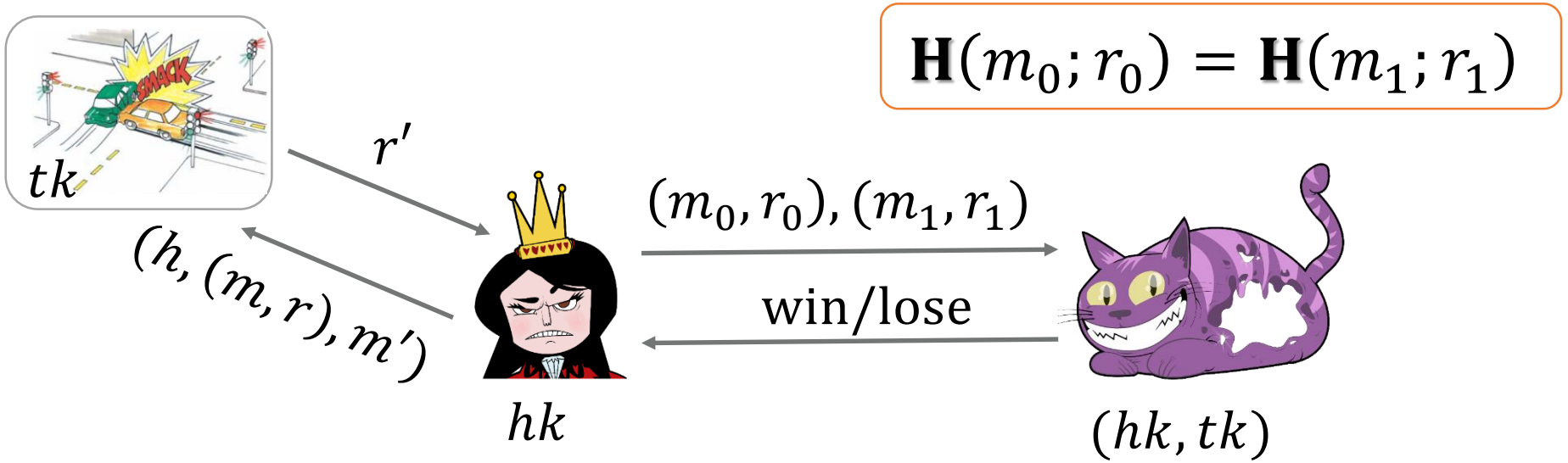
Recent Developments

- The European Union Agency for Network and Information Security (ENISA) Report:
  - "Define what to be kept confidential in order to remain compliant with regulatory requirements"
  - "Identify or develop standard methods for removing data from a ledger"

Recent Developments

- The European Securities and Markets Authority (ESMA) Report:
  - "The DLT that was originally designed for Bitcoin created immutable records, meaning that transactions once validated cannot be modified, cancelled or revoked"
  - "While this immutability had clear benefits in a permissionless DLT framework, it appears ill-suited to securities markets, e.g., operational errors may necessitate the cancellation of some transactions"

Enhanced Collision Resistance



- Hard to find collisions even after seeing polynomially many collisions
  - Computed using the trapdoor key
- Previous constructions did not have this property or could only be proven secure in idealized models

SAPIENZA UNIVERSITÀ DI ROMA