Blockchain, Applicazioni Finanziarie, Soluzioni Crittografiche privacy-preserving

I requisiti del consumatore

Dr. Simone Cortese

Menu

0. Obiettivi del talk
1. Introduzione
2. Blockchain 101
3. Infrastruttura Finanziaria 101
4. Potenziale e Rischi
5. “Yes, but why?” 3 domande chiave
6. Applicazioni: retail CBDC
7. Applicazioni: cosa proteggere
8. I requisiti minimi per il consumatore
9. A Very Brief Privacy Panorama
10. Conclusione: There is no one to rule them all

_0. Obiettivi del Talk

Questo Talk non ruota attorno a nessuna tecnica crittografica specifica. Ne tenta di “venderne” alcuna nuova.

_0. Obiettivi del Talk

Questo Talk non ruota attorno a nessuna tecnica crittografica specifica. Ne tenta di “venderne” alcuna nuova.

Questa presentazione nasce però dall’esperienza legata alle Public Blockchains, il dibattito su “Central Bank Digital Currencies” e dalle pressoche’ illimitate discussioni su un argomento “caldo” quale e’ “Privacy”.

_0. Obiettivi del Talk

Questo Talk non ruota attorno a nessuna tecnica crittografica specifica. Ne tenta di “venderne” alcuna nuova.

Questa presentazione nasce però dall’esperienza legata alle Public Blockchains, il dibattito su “Central Bank Digital Currencies” e dalle pressoche’ illimitate discussioni su un argomento “caldo” quale e’ “Privacy”.

Gli obiettivi di questo talk sono quindi tre:

_0. Obiettivi del Talk

Questo Talk non ruota attorno a nessuna tecnica crittografica specifica. Ne tenta di “venderne” alcuna nuova.

Questa presentazione nasce però dall’esperienza legata alle Public Blockchains, il dibattito su “Central Bank Digital Currencies” e dalle pressoche’ illimitate discussioni su un argomento “caldo” quale e’ “Privacy”.

Gli obiettivi di questo talk sono quindi tre:

- Comunicare che non vi e’ una “flat solution” per il “problema privacy”. Vi sono solo requisiti e soluzioni piu’ o meno calzanti per tali requisiti.

_0. Obiettivi del Talk

Questo Talk non ruota attorno a nessuna tecnica crittografica specifica. Ne tenta di “venderne” alcuna nuova.

Questa presentazione nasce però dall’esperienza legata alle Public Blockchains, il dibattito su “Central Bank Digital Currencies” e dalle pressoche’ illimitate discussioni su un argomento “caldo” quale e’ “Privacy”.

Gli obiettivi di questo talk sono quindi tre:

- Comunicare che non vi e’ una “flat solution” per il “problema privacy”. Vi sono solo requisiti e soluzioni piu’ o meno calzanti per tali requisiti.
- Fornire un semplicissimo framework (“forma mentis”) che permetta a chiunque - ingegneri, crittografi, product managers e analisti - di pensare e progettare una soluzione basandosi davvero sui bisogni del consumatore.

_0. Obiettivi del Talk

Questo Talk non ruota attorno a nessuna tecnica crittografica specifica. Ne tenta di “venderne” alcuna nuova.

Questa presentazione nasce però dall’esperienza legata alle Public Blockchains, il dibattito su “Central Bank Digital Currencies” e dalle pressoche’ illimitate discussioni su un argomento “caldo” quale e’ “Privacy”.

Gli obiettivi di questo talk sono quindi tre:

- Comunicare che non vi e’ una “flat solution” per il “problema privacy”. Vi sono solo requisiti e soluzioni piu’ o meno calzanti per tali requisiti.
- Fornire un semplicissimo framework (“forma mentis”) che permetta a chiunque - ingegneri, crittografi, product managers e analisti - di pensare e progettare una soluzione basandosi davvero sui bisogni del consumatore.
- Iniziare un dialogo, “outcome focused and consumer centric”

_I. Chi sono

Simone Cortese, PhD (University of Southampton, UK)

_I. Chi sono

Simone Cortese, PhD (University of Southampton, UK)

Attualmente:

_I. Chi sono

Simone Cortese, PhD (University of Southampton, UK)

Attualmente:

- Product Manager, Fnality International

_I. Chi sono

Simone Cortese, PhD (University of Southampton, UK)

Attualmente:

- Product Manager, Fnality International
- Visiting Lecturer, University of West London
    - (Blockchain and DLT for Finance module)

_I. Chi sono

Simone Cortese, PhD (University of Southampton, UK)

Attualmente:

- Product Manager, Fnality International
- Visiting Lecturer, University of West London
  - (Blockchain and DLT for Finance module)
- Mentor

_I. Chi sono

Simone Cortese, PhD (University of Southampton, UK)

Attualmente:

- Product Manager, Fnality International
- Visiting Lecturer, University of West London
  - (Blockchain and DLT for Finance module)
- Mentor

Aree di interesse:

- **Infrastrutture dei Mercati Finanziari** (FMIs, Sistemi di Pagamento, CCPs etc)

_I. Chi sono

Simone Cortese, PhD (University of Southampton, UK)

Attualmente:

- Product Manager, Fnality International
- Visiting Lecturer, University of West London
  - (Blockchain and DLT for Finance module)
- Mentor

Aree di interesse:

- **Infrastrutture dei Mercati Finanziari** (FMIs, Sistemi di Pagamento, CCPs etc)
- **Blockchain, DLT** e applicativi nei Mercati Finanziari (dFMI, CBDC) attraverso l'intera "Trade" *Value Chain*

_I. Chi sono

Simone Cortese, PhD (University of Southampton, UK)

Attualmente:

- Product Manager, Fnality International
- Visiting Lecturer, University of West London
  - (Blockchain and DLT for Finance module)
- Mentor

Aree di interesse:

- **Infrastrutture dei Mercati Finanziari** (FMIs, Sistemi di Pagamento, CCPs etc)
- **Blockchain, DLT** e applicativi nei Mercati Finanziari (dFMI, CBDC) attraverso l'intera "Trade" *Value Chain*
- **Regulatory Landscape** relativo a nuove tecnologie

_I. Chi sono

Simone Cortese, PhD (University of Southampton, UK)

Attualmente:

- Product Manager, Fnality International
- Visiting Lecturer, University of West London
  - (Blockchain and DLT for Finance module)
- Mentor

Aree di interesse:

- **Infrastrutture dei Mercati Finanziari** (FMIs, Sistemi di Pagamento, CCPs etc)
- **Blockchain, DLT** e applicativi nei Mercati Finanziari (dFMI, CBDC) attraverso l'intera "Trade" *Value Chain*
- **Regulatory Landscape** relativo a nuove tecnologie
- **Crittografia "dal punto di vista del consumatore"**

_I. Chi sono

Simone Cortese, PhD (University of Southampton, UK)

Attualmente:

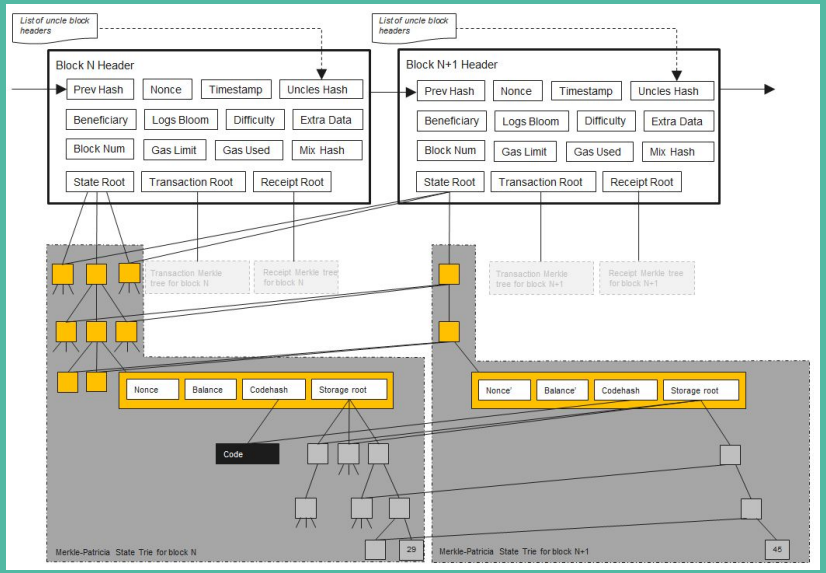
- Product Manager, Fnality International
- Visiting Lecturer, University of West London
  - (Blockchain and DLT for Finance module)
- Mentor

Aree di interesse:

- **Infrastrutture dei Mercati Finanziari** (FMIs, Sistemi di Pagamento, CCPs etc)
- **Blockchain, DLT** e applicativi nei Mercati Finanziari (dFMI, CBDC) attraverso l'intera "Trade" *Value Chain*
- **Regulatory Landscape** relativo a nuove tecnologie
- ***Crittografia "dal punto di vista del consumatore"***

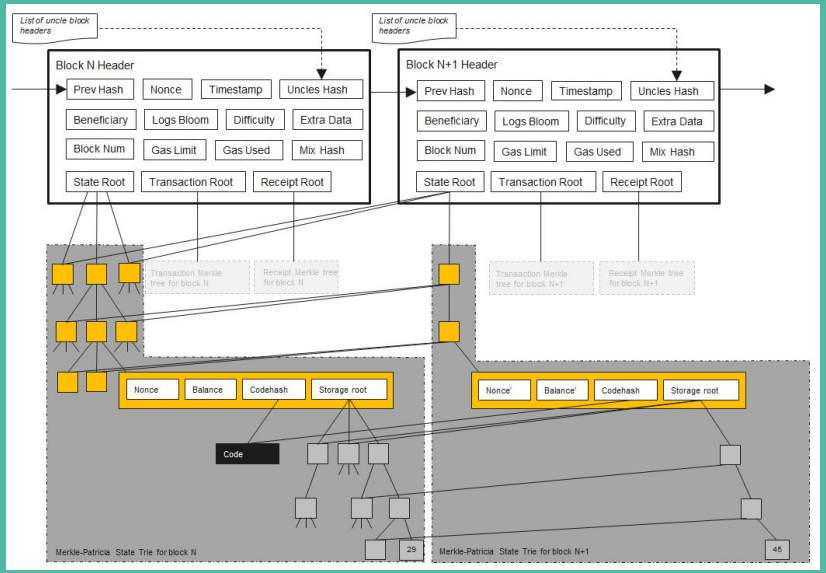
_II. Blockchain 101

_II. Blockchain 101



_II. Blockchain 101

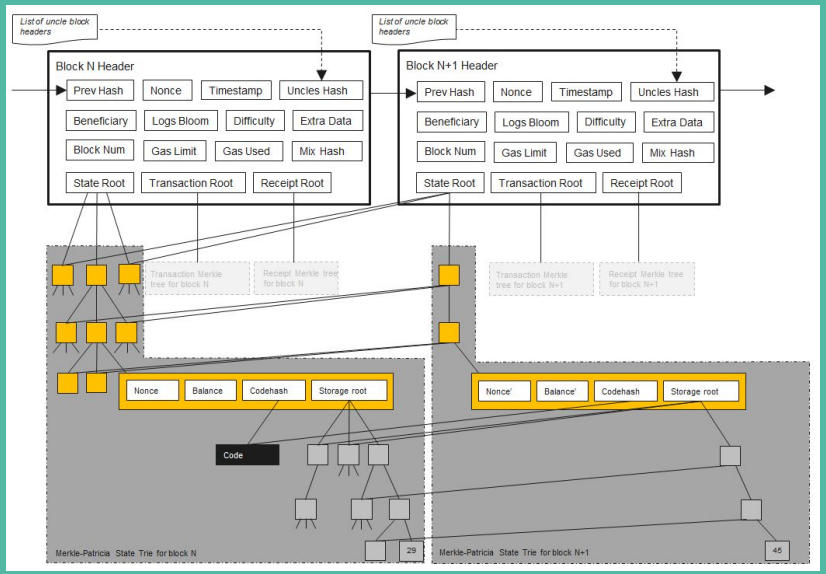
Registro distribuito egualmente tra tutti i partecipanti in una comunita'. Gli updates di questo registro non vengono controllati da nessuna autorita' ma sono aggiunti seguendo una ben definita serie di step **("Consensus").**



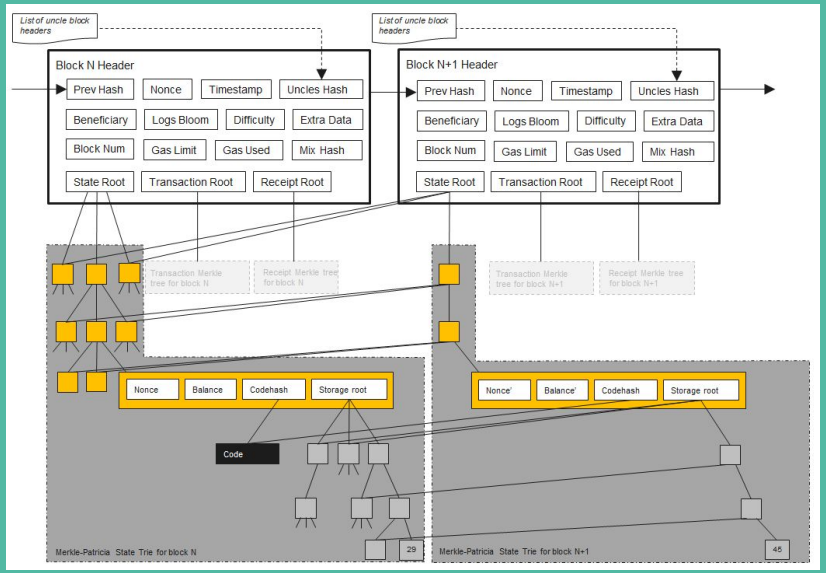
_II. Blockchain 101

Registro distribuito egualmente tra tutti i partecipanti in una comunita'. Gli updates di questo registro non vengono controllati da nessuna autorita' ma sono aggiunti seguendo una ben definita serie di step **("Consensus").**

Gli updates di questo registro vengono applicati in "Batches" i.e. **Blocchi,** i quali sono a loro volta collegati ai precedenti Blocchi tramite l'inclusione dell'**Hash del blocco precedente.**

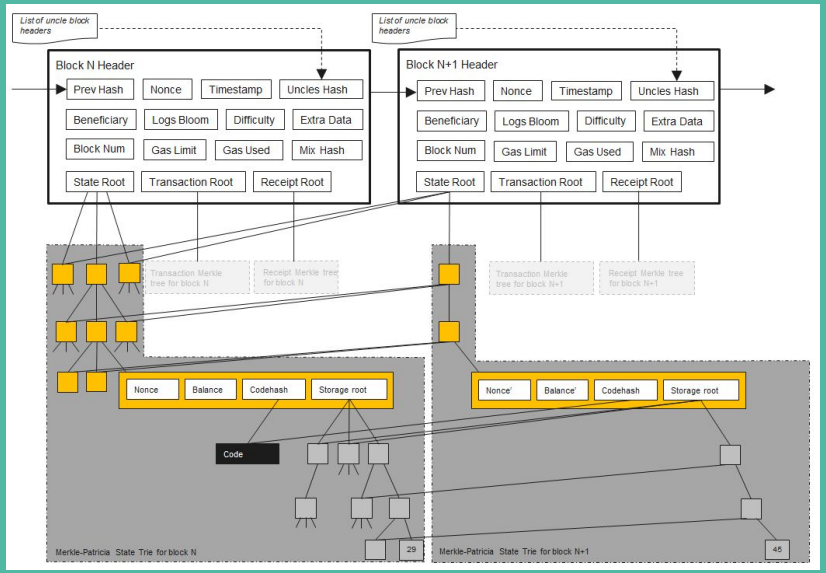


_II. Blockchain 101 - Punti chiave



_II. Blockchain 101 - Punti chiave

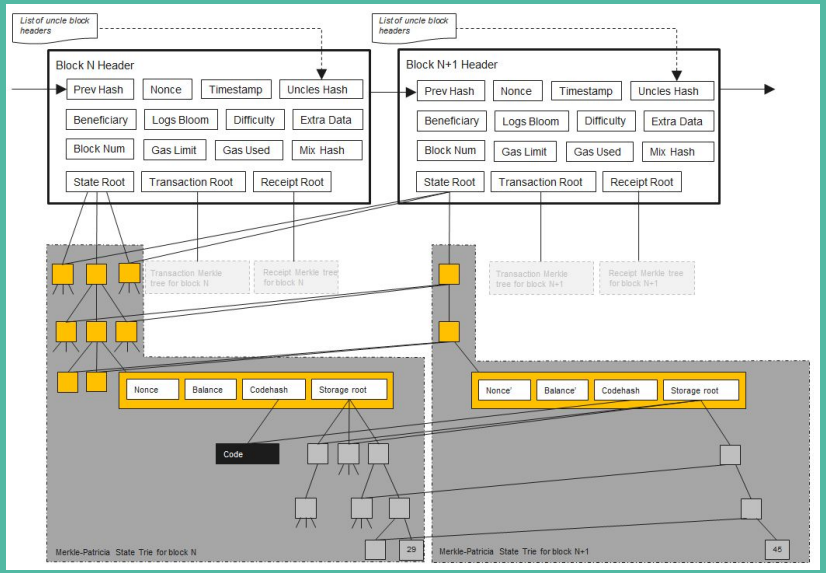
- “**Centralizzazione logica**” dei dati: non piu’ differenti database da allineare continuamente ma un solo punto di vista per ogni partecipante.



_II. Blockchain 101 - Punti chiave

- “**Centralizzazione logica**” dei dati: non piu’ differenti database da allineare continuamente ma un solo punto di vista per ogni partecipante.

- L’architettura complessiva (inherently replicated) garantisce livelli di **resilienza** estremamente elevati.

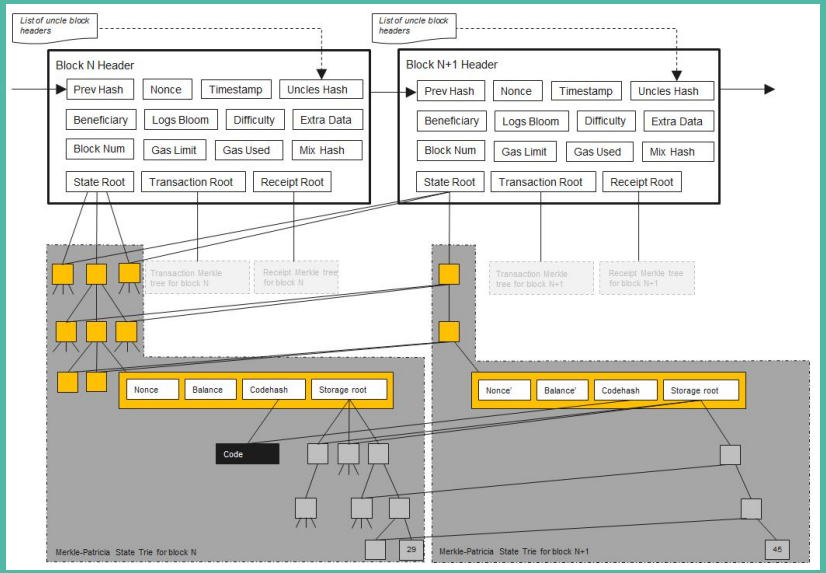


_II. Blockchain 101 - Punti chiave

- “**Centralizzazione logica**” dei dati: non piu’ differenti database da allineare continuamente ma un solo punto di vista per ogni partecipante.

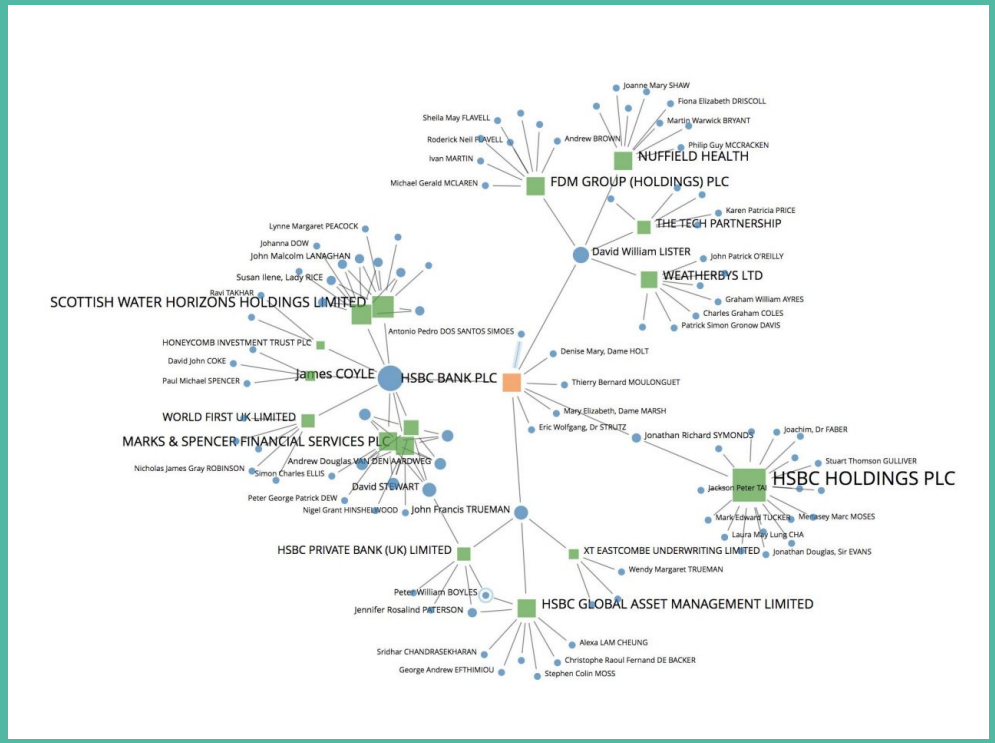
- L’architettura complessiva (inherently replicated) garantisce livelli di **resilienza** estremamente elevati.

- Il regolamento di conti e’ realmente “Peer-to-Peer”, senza alcun intermediario.



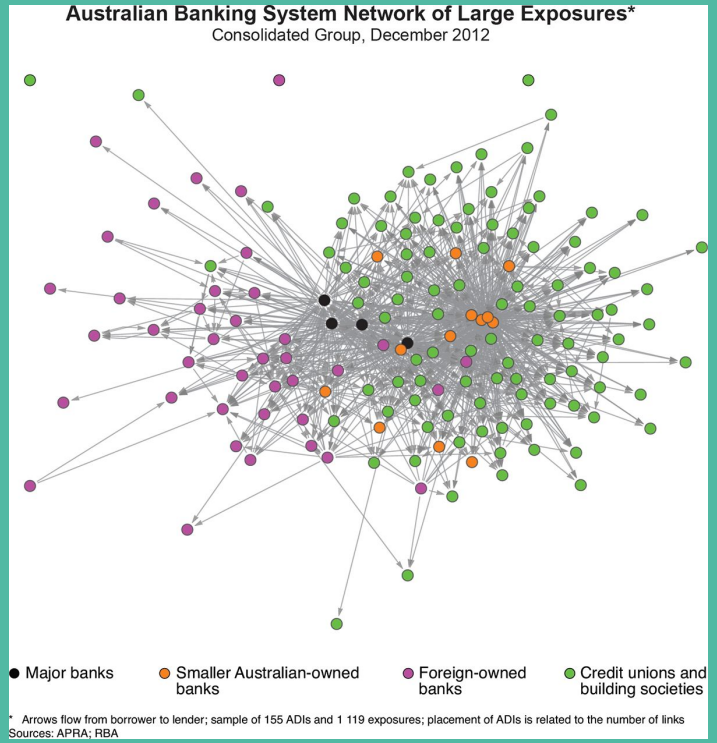
_III. Infrastruttura Finanziaria 101

_III. Infrastruttura Finanziaria 101



[1] Kimmo Soramaki, *BIS IFC – Bank Indonesia International Workshop and Seminar on "Big Data for Central Bank Policies / Building Pathways for Policy Making with Big Data"*, 2018

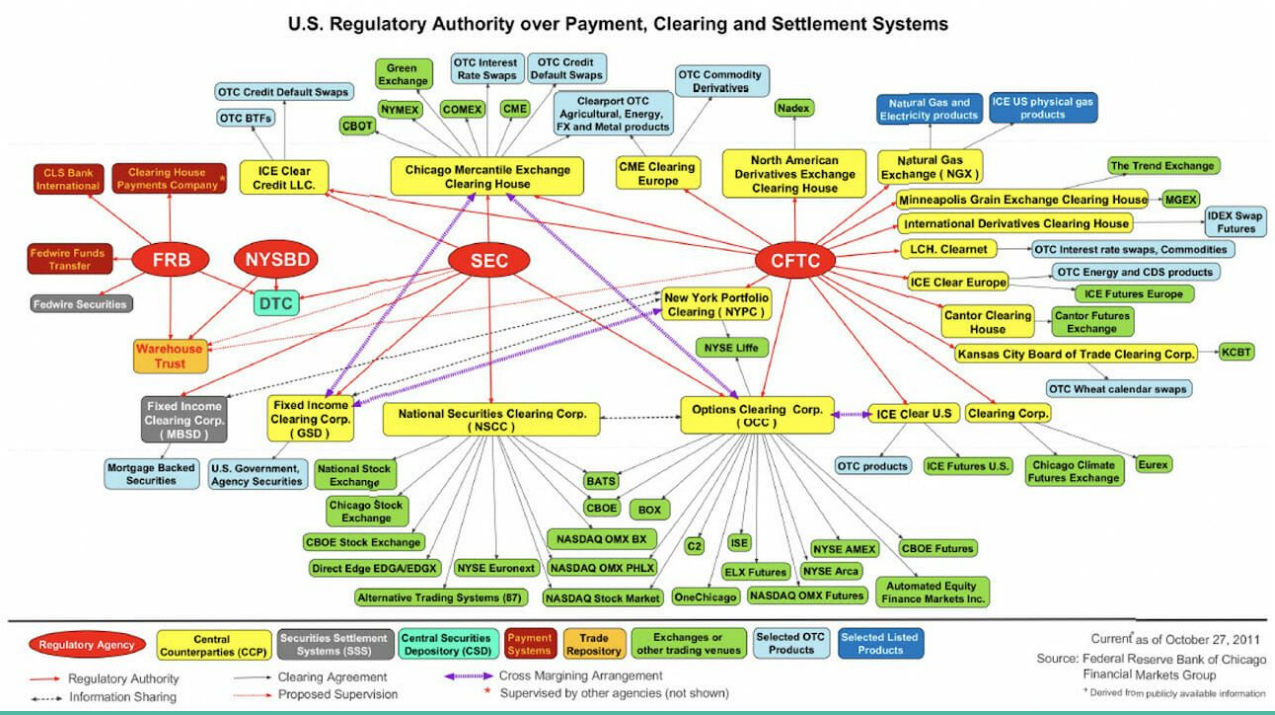
_III. Infrastruttura Finanziaria 101



[1] Kimmo Soramaki, *BIS IFC – Bank Indonesia International Workshop and Seminar on "Big Data for Central Bank Policies / Building Pathways for Policy Making with Big Data"*, 2018

_III. Infrastruttura Finanziaria 101

BUILDING FINANCIAL PRODUCTS — REGULATORY ENVIRONMENT



_IV. Potenziale & Rischi

_IV. Potenziale & Rischi

- **Potenziale: un singolo punto di vista condiviso** dal mercato aumenta l'efficienza, riduce costi e tempi, aumenta la resilienza del sistema**[2]**.

[2] Oliver Wyman, "Blockchain in Capital Markets", 2016.

_IV. Potenziale & Rischi

- **Potenziale: un singolo punto di vista condiviso** dal mercato aumenta l'efficienza, riduce costi e tempi, aumenta la resilienza del sistema**[2]**.
- **Rischi: quali dati vengono condivisi?** Chi ha accesso a tali dati?

[2] Oliver Wyman, "Blockchain in Capital Markets", 2016.
[3] ECB, "Eurosystem Report on the public consultation on digital euro", 2021

_IV. Potenziale & Rischi

- **Potenziale: un singolo punto di vista condiviso** dal mercato aumenta l'efficienza, riduce costi e tempi, aumenta la resilienza del sistema**[2]**.
- **Rischi: quali dati vengono condivisi?** Chi ha accesso a tali dati?

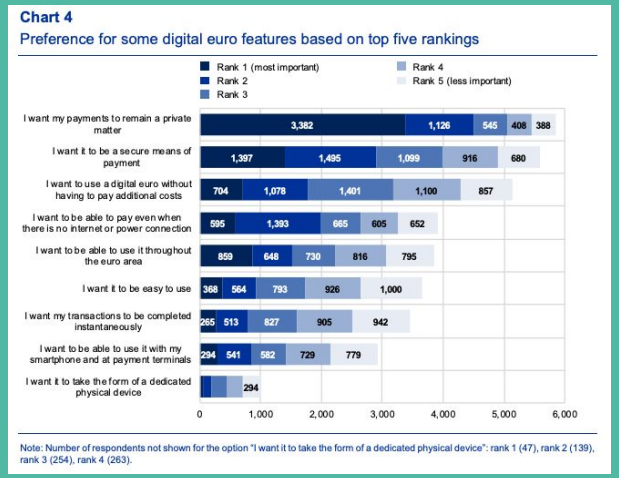
Tale rischio e' particolarmente percepito per gli utenti retail.**[3]**

[2] Oliver Wyman, "Blockchain in Capital Markets", 2016.
[3] ECB, "Eurosystem Report on the public consultation on digital euro", 2021

_IV. Potenziale & Rischi

- **Potenziale: un singolo punto di vista condiviso** dal mercato aumenta l'efficienza, riduce costi e tempi, aumenta la resilienza del sistema**[2]**.
- **Rischi: quali dati vengono condivisi?** Chi ha accesso a tali dati?

Tale rischio e' particolarmente percepito per gli utenti retail.**[3]**

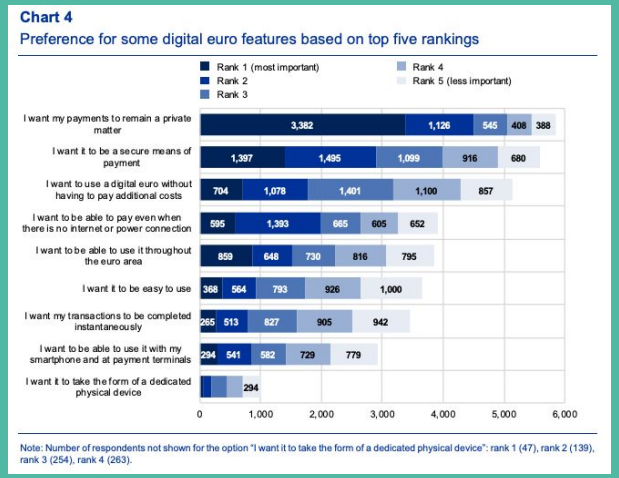


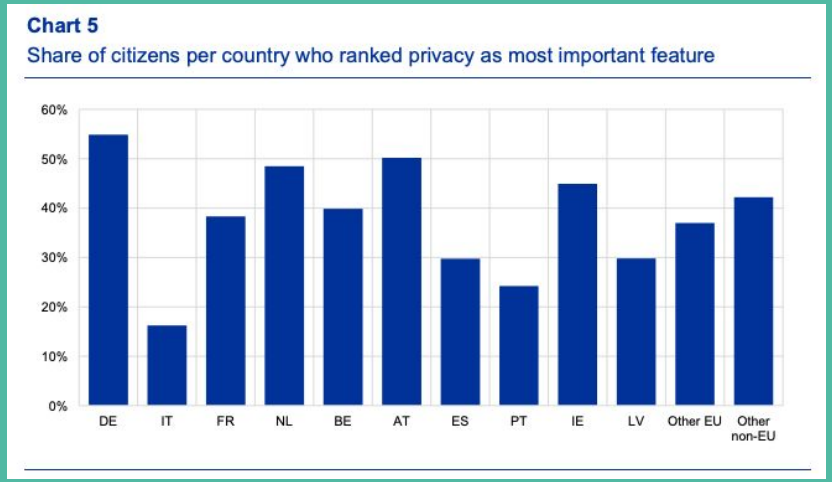
[2] Oliver Wyman, "Blockchain in Capital Markets", 2016.
[3] ECB, "Eurosystem Report on the public consultation on digital euro", 2021

_IV. Potenziale & Rischi

- **Potenziale: un singolo punto di vista condiviso** dal mercato aumenta l'efficienza, riduce costi e tempi, aumenta la resilienza del sistema**[2]**.
- **Rischi: quali dati vengono condivisi?** Chi ha accesso a tali dati?

Tale rischio e' particolarmente percepito per gli utenti retail.**[3]**





[2] Oliver Wyman, "Blockchain in Capital Markets", 2016.
[3] ECB, "Eurosystem Report on the public consultation on digital euro", 2021

_V. “Yes, but Why”?

_V. “Yes, but Why”? 3 domande chiave

- La richiesta di “privacy” e’ un tema comune; eppure, spesso la creazione di chiari requisiti lo e’ molto meno.

_V. “Yes, but Why”? 3 domande chiave

- La richiesta di “privacy” e’ un tema comune; eppure, spesso la creazione di chiari requisiti lo e’ molto meno.

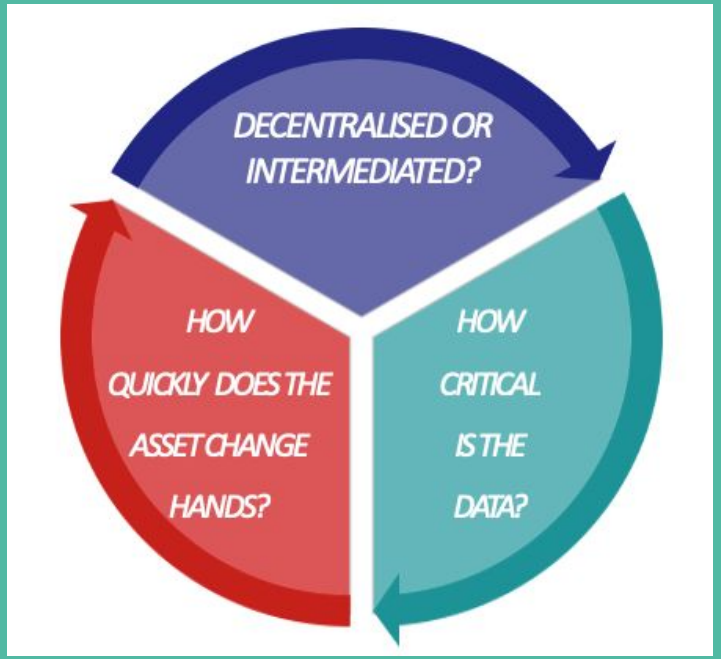
Quali **criteri** possiamo usare per definire questi requisiti quando si parla di Blockchain?

_V. “Yes, but Why”? 3 domande chiave

- La richiesta di “privacy” e’ un tema comune; eppure, spesso la creazione di chiari requisiti lo e’ molto meno.

Quali **criteri** possiamo usare per definire questi requisiti quando si parla di Blockchain?

1. **Centralizzato o Distribuito?** Quanto e’ importante la resilienza del sistema?

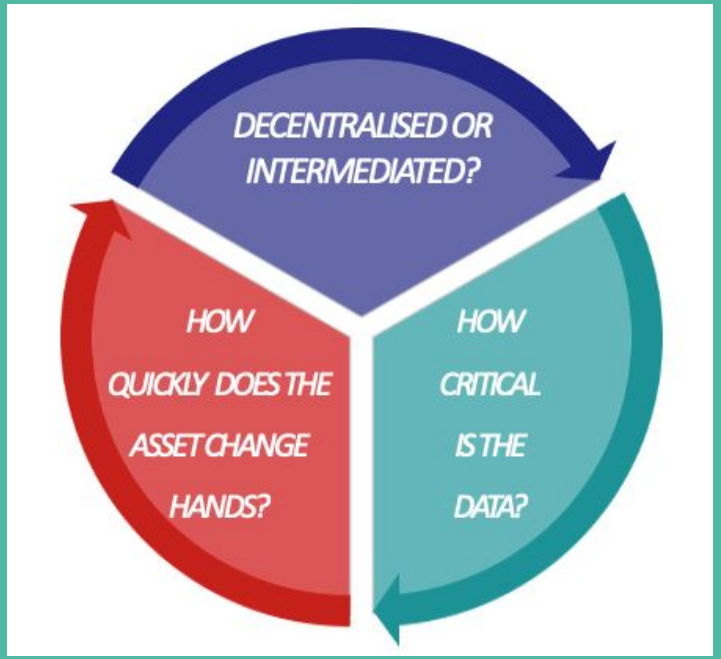


_V. “Yes, but Why”? 3 domande chiave

- La richiesta di “privacy” e’ un tema comune; eppure, spesso la creazione di chiari requisiti lo e’ molto meno.

Quali **criteri** possiamo usare per definire questi requisiti quando si parla di Blockchain?

1. **Centralizzato o Distribuito?** Quanto e’ importante la resilienza del sistema?
2. **Quanto spesso** questi dati vengono modificati?

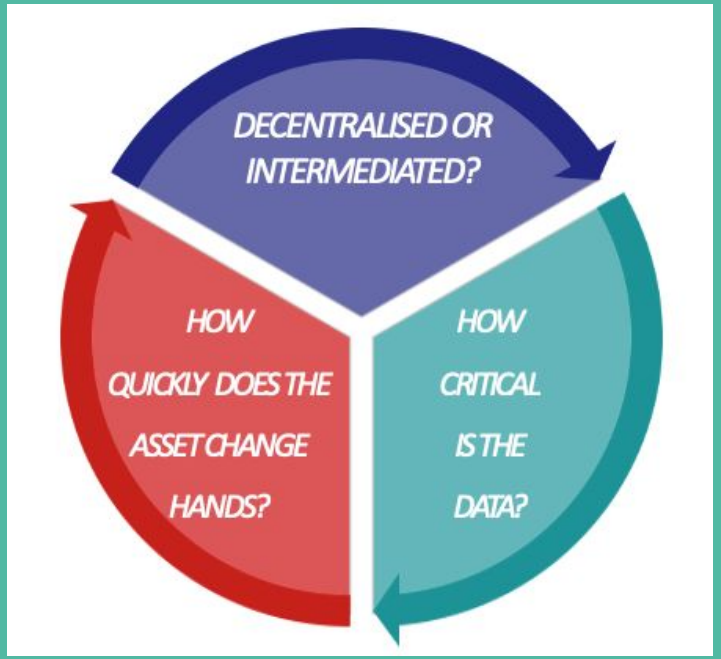


_V. “Yes, but Why”? 3 domande chiave

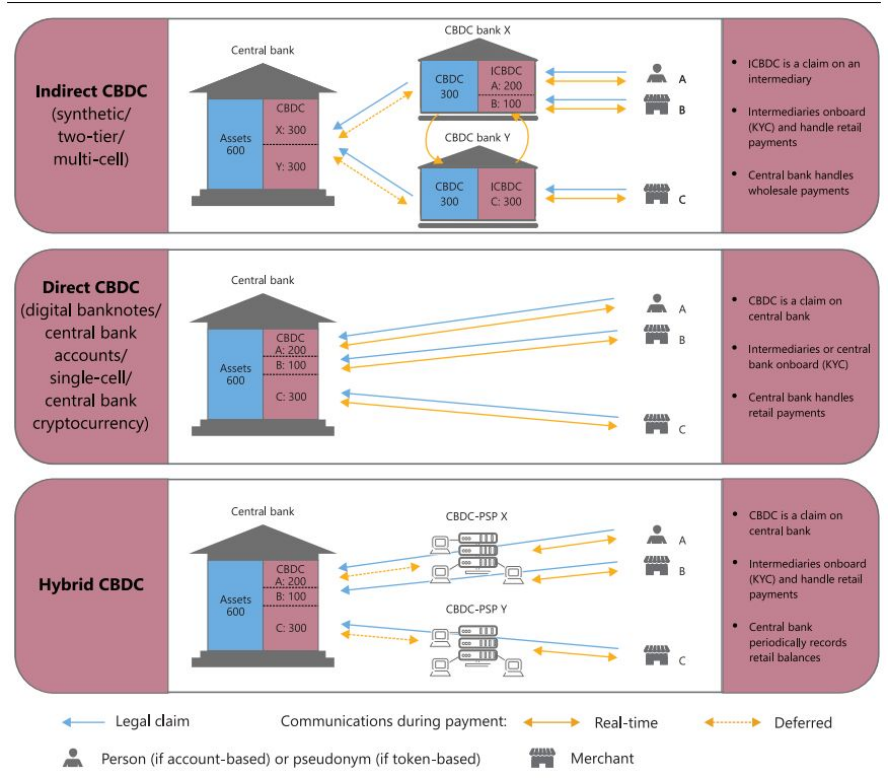
- La richiesta di “privacy” e’ un tema comune; eppure, spesso la creazione di chiari requisiti lo e’ molto meno.

Quali **criteri** possiamo usare per definire questi requisiti quando si parla di Blockchain?

1. **Centralizzato o Distribuito?** Quanto e’ importante la resilienza del sistema?
2. **Quanto spesso** questi dati vengono modificati?
3. **Cosa puo’ essere inferito?** Cosa rappresentano i dati da condividere?

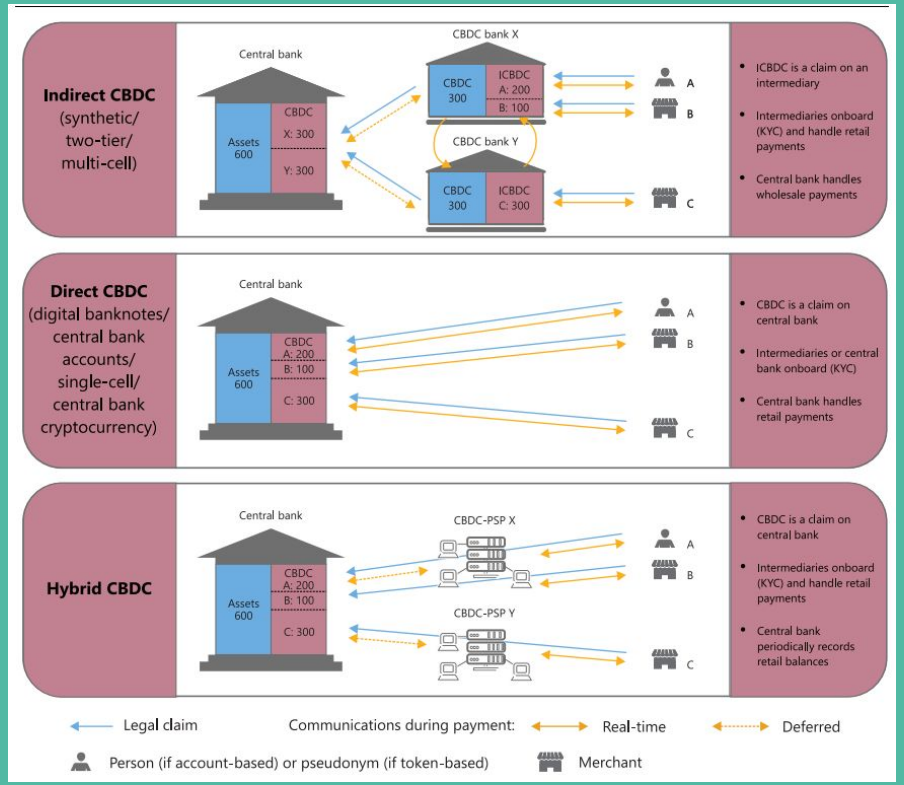


_VI. Applicazioni: retail CBDC



[4] BIS, "The architecture of retail Central Bank digital Currency", 2020

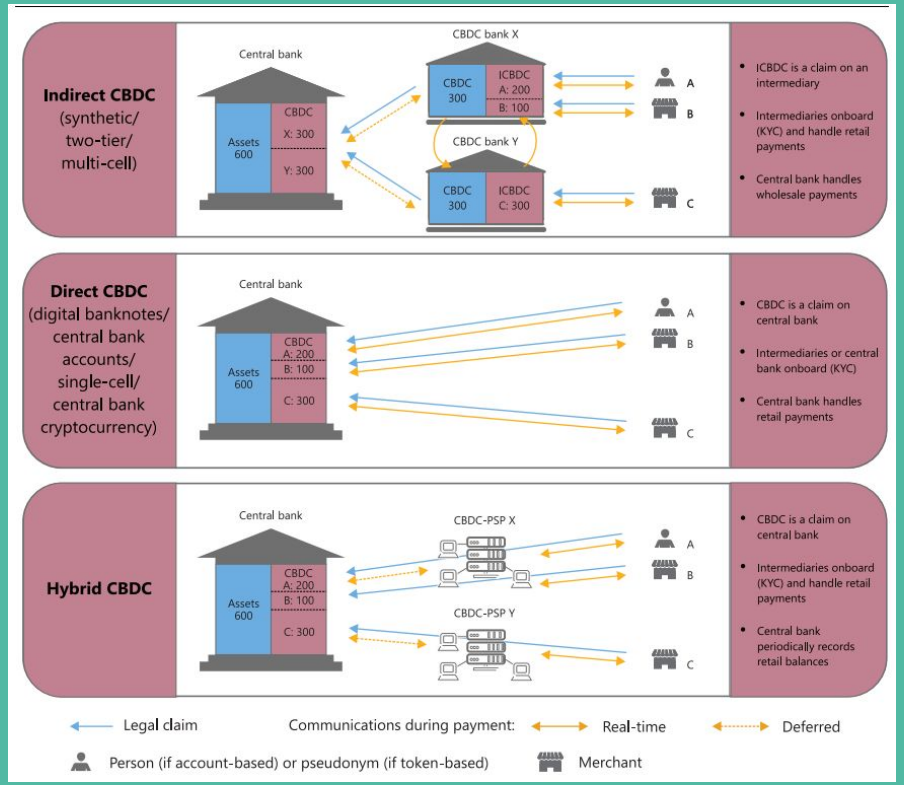
_VI. Applicazioni: retail CBDC



1. Resilienza, de/ centralizzazione:
   a. Importanza sistemica, “programmable money”

[4] BIS, “The architecture of retail Central Bank digital Currency”, 2020

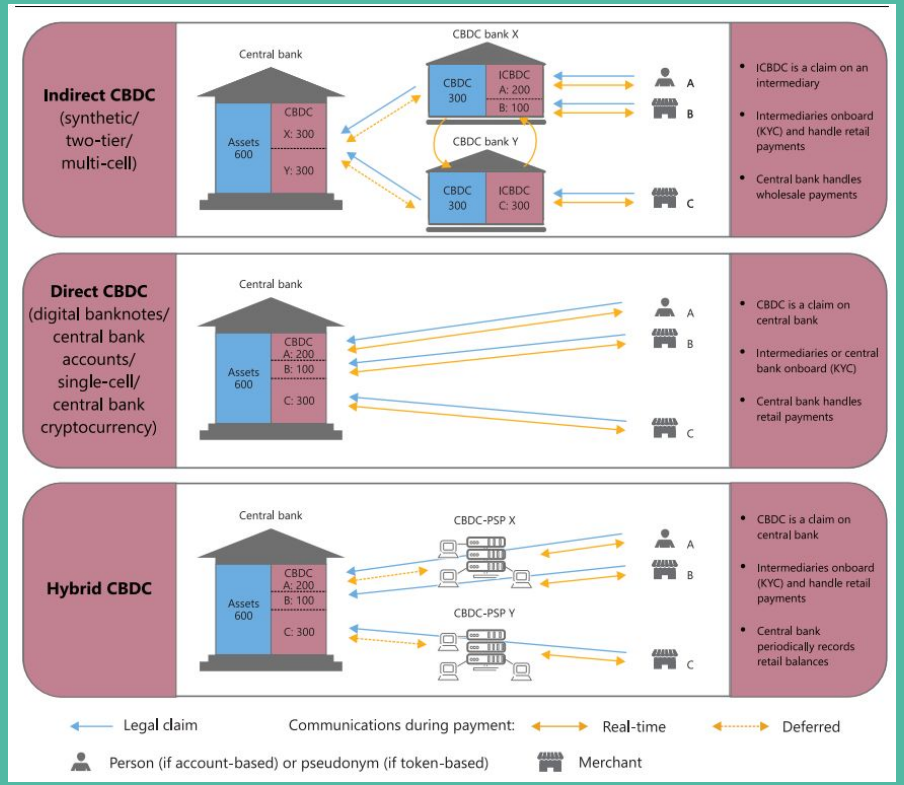
_VI. Applicazioni: retail CBDC



1. Resilienza, de/ centralizzazione:
   a. Importanza sistemica, “programmable money”
2. Quanto spesso sono modificati i dati?
   a. Retail, ~50,000 TPS (e.g. VISA)

[4] BIS, “The architecture of retail Central Bank digital Currency”, 2020

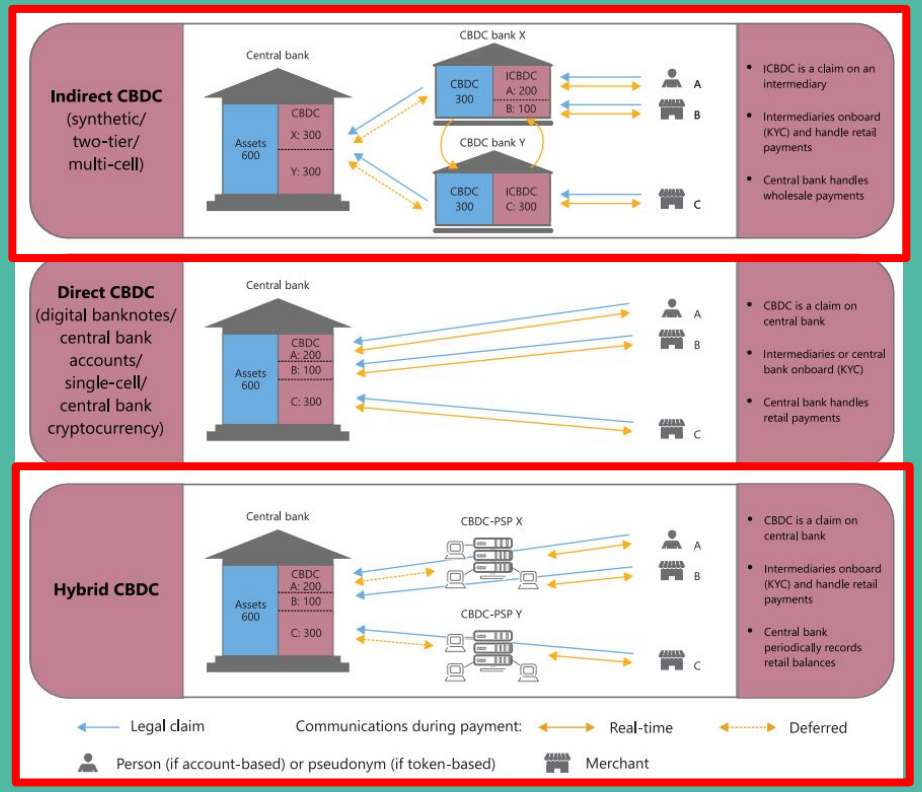
_VI. Applicazioni: retail CBDC



1. Resilienza, de/ centralizzazione:
   a. Importanza sistemica, “programmable money”
2. Quanto spesso sono modificati i dati?
   a. Retail, ~50,000 TPS (e.g. VISA)
3. Cosa puo’ essere inferito da questi dati?
   a. Consumer spending/habits, profiling
   b. Potenzialmente, patrimonio

[4] BIS, “The architecture of retail Central Bank digital Currency”, 2020

_VI. Applicazioni: retail CBDC



1. Resilienza, de/ centralizzazione:
   a. Importanza sistemica, “programmable money”
2. Quanto spesso sono modificati i dati?
   a. Retail, ~50,000 TPS (e.g. VISA)
3. Cosa puo’ essere inferito da questi dati?
   a. Consumer spending/habits, profiling
   b. Potenzialmente, patrimonio

[4] BIS, “The architecture of retail Central Bank digital Currency”, 2020

_VI. Applicazioni: retail CBDC

1. Resilienza, de/ centralizzazione
    a. Importanza sistemica
        i. → ***Blockchain e' adeguata, "Full Consensus" models***

_VI. Applicazioni: retail CBDC

1. Resilienza, de/ centralizzazione
    a. Importanza sistemica
        i. → ***Blockchain e' adeguata, "Full Consensus" models***
2. Quanto spesso sono modificati i dati?
    a. Retail, ~50,000 TPS (e.g. VISA)
        i. → ***Sfida Risolvibile (e.g. sharding, layer 2 solution)***

_VI. Applicazioni: retail CBDC

1. Resilienza, de/ centralizzazione
    a. Importanza sistemica
        i. → ***Blockchain e' adeguata, "Full Consensus" models***
2. Quanto spesso sono modificati i dati?
    a. Retail, ~50,000 TPS (e.g. VISA)
        i. → ***Sfida Risolvibile (e.g. sharding, layer 2 solution)***
3. Cosa puo' essere inferito da questi dati?
    a. Consumer spending/habits, profiling
    b. Potenzialmente, patrimonio
        i. → Serve Privacy, ma a che livello?

_VI. Applicazioni: retail CBDC

1. Resilienza, de/ centralizzazione
    a. Importanza sistemica
        i. → ***Blockchain e' adeguata, "Full Consensus" models***
2. Quanto spesso sono modificati i dati?
    a. Retail, ~50,000 TPS (e.g. VISA)
        i. → ***Sfida Risolvibile (e.g. sharding, layer 2 solution)***
3. Cosa puo' essere inferito da questi dati?
    a. Consumer spending/habits, profiling
    b. Potenzialmente, patrimonio
        i. → Serve Privacy, ma a che livello?

_VII. Applicazioni: cosa proteggere

Supponiamo una soluzione basata su “Ethereum”, dando così precedenza a resilienza e efficienza operativa (single view of the Ledger) la quale e’ sicuramente essenziale per una CBDC sicura da usare per gli utenti.

_VII. Applicazioni: cosa proteggere

Supponiamo una soluzione basata su “Ethereum”, dando così precedenza a resilienza e efficienza operativa (single view of the Ledger) la quale e’ sicuramente essenziale per una CBDC sicura da usare per gli utenti.

Assumendo nessuna protezione all’accesso (ipotesi molto restrittiva), un *attacker* potrebbe ottenere informazioni riguardo a:

_VII. Applicazioni: cosa proteggere

Supponiamo una soluzione basata su “Ethereum”, dando così precedenza a resilienza e efficienza operativa (single view of the Ledger) la quale e’ sicuramente essenziale per una CBDC sicura da usare per gli utenti.

Assumendo nessuna protezione all’accesso (ipotesi molto restrittiva), un *attacker* potrebbe ottenere informazioni riguardo a:

- Payer (address)
- Payee (address)

_VII. Applicazioni: cosa proteggere

Supponiamo una soluzione basata su “Ethereum”, dando cosi precendeza a resilienza e efficienza operativa (single view of the Ledger) la quale e’ sicuramente essenziale per una CBDC sicura da usare per gli utenti.

Assumendo nessuna protezione all’accesso (ipotesi molto restrittiva), un *attacker* potrebbe ottenere informazioni riguardo a:

- Payer (address)
- Payee (address)
- Payer - bilancio complessivo
- Payee - bilancio complessivo

_VII. Applicazioni: cosa proteggere

Supponiamo una soluzione basata su “Ethereum”, dando cosi precendeza a resilienza e efficienza operativa (single view of the Ledger) la quale e’ sicuramente essenziale per una CBDC sicura da usare per gli utenti.

Assumendo nessuna protezione all’accesso (ipotesi molto restrittiva), un *attacker* potrebbe ottenere informazioni riguardo a:

- Payer (address)
- Payee (address)
- Payer - bilancio complessivo
- Payee - bilancio complessivo
- Ammontare del pagamento (ETH oppure Tokens)
- Transaction History (i.e. “Transaction Graph”)

_VII. Applicazioni: cosa proteggere

Supponiamo una soluzione basata su “Ethereum”, dando cosi precendeza a resilienza e efficienza operativa (single view of the Ledger) la quale e’ sicuramente essenziale per una CBDC sicura da usare per gli utenti.

Assumendo nessuna protezione all’accesso (ipotesi molto restrittiva), un *attacker* potrebbe ottenere informazioni riguardo a:

- Payer (address)
- Payee (address)
- Payer - bilancio complessivo
- Payee - bilancio complessivo
- Ammontare del pagamento (ETH oppure Tokens)
- Transaction History (i.e. “Transaction Graph”)

_VII. Applicazioni: cosa proteggere

Supponiamo una soluzione basata su “Ethereum”, dando cosi precendeza a resilienza e efficienza operativa (single view of the Ledger) la quale e’ sicuramente essenziale per una CBDC sicura da usare per gli utenti.

Assumendo nessuna protezione all’accesso (ipotesi molto restrittiva), un *attacker* potrebbe ottenere informazioni riguardo a:

- Payer (address)
- Payee (address)
- Payer - bilancio complessivo
- Payee - bilancio complessivo
- Ammontare del pagamento (ETH oppure Tokens)
- Transaction History (i.e. “Transaction Graph”)

_VII. Applicazioni: cosa proteggere

Supponiamo una soluzione basata su “Ethereum”, dando cosi precendeza a resilienza e efficienza operativa (single view of the Ledger) la quale e’ sicuramente essenziale per una CBDC sicura da usare per gli utenti.

Assumendo nessuna protezione all’accesso (ipotesi molto restrittiva), un *attacker* potrebbe ottenere informazioni riguardo a:

- Payer (address)
- Payee (address)
- Payer - bilancio complessivo
- Payee - bilancio complessivo
- Ammontare del pagamento (ETH oppure Tokens)
- Transaction History (i.e. “Transaction Graph”)

_VIII. I requisiti *minimi*

1. L’ **ammontare** del pagamento (ETH oppure Tokens) & Transaction History (i.e. “Transaction Graph”) deve essere offuscato.

_VIII. I requisiti *minimi*

1. L' **ammontare** del pagamento (ETH oppure Tokens) & Transaction History (i.e. "Transaction Graph") deve essere offuscato.
2. La soluzione deve rispettare de "**Full Consensus**" così da non compromettere la "resilienza" dell'intero sistema .

_VIII. I requisiti *minimi*

1. L' **ammontare** del pagamento (ETH oppure Tokens) & Transaction History (i.e. "Transaction Graph") deve essere offuscato.
2. La soluzione deve rispettare de "**Full Consensus**" così da non compromettere la "resilienza" dell'intero sistema .
3. L'offuscamento non deve compromettere le funzionalità legate alla **programmabilità** della CBDC.

_VIII. I requisiti *minimi*

1. L' **ammontare** del pagamento (ETH oppure Tokens) & Transaction History (i.e. "Transaction Graph") deve essere offuscato.
2. La soluzione deve rispettare de "**Full Consensus**" così da non compromettere la "resilienza" dell'intero sistema .
3. L'offuscamento non deve compromettere le funzionalità legate alla **programmabilità** della CBDC.
4. L'offuscamento deve essere **compatibile** con i principali standard e strumenti (hardware e software) crittografici (e.g. HSMs, interfacce etc.).

_VIII. I requisiti *minimi*

1. L' **ammontare** del pagamento (ETH oppure Tokens) & Transaction History (i.e. "Transaction Graph") deve essere offuscato.
2. La soluzione deve rispettare de "**Full Consensus**" così da non compromettere la "resilienza" dell'intero sistema .
3. L'offuscamento non deve compromettere le funzionalità legate alla **programmabilità** della CBDC.
4. L'offuscamento deve essere **compatibile** con i principali standard e strumenti (hardware e software) crittografici (e.g. HSMs, interfacce etc.).
5. L'offuscamento non deve compromettere la capacità' di processare transazioni del sistema (e.g. **impatto su TPS** deve essere limitato).

_VIII. I requisiti *minimi*

1. L' **ammontare** del pagamento (ETH oppure Tokens) & Transaction History (i.e. "Transaction Graph") deve essere offuscato.
2. La soluzione deve rispettare de "**Full Consensus**" così da non compromettere la "resilienza" dell'intero sistema .
3. L'offuscamento non deve compromettere le funzionalità legate alla **programmabilità** della CBDC.
4. L'offuscamento deve essere **compatibile** con i principali standard e strumenti (hardware e software) crittografici (e.g. HSMs, interfacce etc.).
5. L'offuscamento non deve compromettere la capacità' di processare transazioni del sistema (e.g. **impatto su TPS** deve essere limitato).
6. L'offuscamento non deve compromettere **l'auditabilità** del sistema.

_IX. Un breve panorama

_IX. Un breve panorama

1. “Ephemeral” / “Stealth” addresses & Ring Signatures:
    a. Possono interrompere la tracciabilità dei pagamenti.
    b. Eppure complessi da implementare con strumenti crittografici non standard (point addition & hashes all’interno di HSM e’ richiesto);

_IX. Un breve panorama

1. “Ephemeral” / “Stealth” addresses & Ring Signatures:
   a. Possono interrompere la tracciabilità dei pagamenti.
   b. Eppure complessi da implementare con strumenti crittografici non standard (point addition & hashes all’interno di HSM e’ richiesto);

2. ZK-SNARKs:
   a. Possono offuscare efficacemente l’ammontare e non compromettere full consensus.
   b. Eppure molto dispendiose in termini di risorse computazionali (e conseguentemente di prezzo, soprattutto nelle blockchain pubbliche).
   c. Potenziali attack vectors provenienti da alcuni schemi che richiedono un “trusted setup”.

_X. Conclusione: there is no one to rule them all

In conclusione:

_X. Conclusione: there is no one to rule them all

In conclusione:

- “Full consensus” e’ chiave per ottimizzare e razionalizzare il sistema finanziario (e non solo).

_X. Conclusione: there is no one to rule them all

In conclusione:

- “Full consensus” e’ chiave per ottimizzare e razionalizzare il sistema finanziario (e non solo).
- Questo nuovo modello crea preoccupazioni legate alla privacy dei dati condivisi.

_X. Conclusione: there is no one to rule them all

In conclusione:

- “Full consensus” e’ chiave per ottimizzare e razionalizzare il sistema finanziario (e non solo).
- Questo nuovo modello crea preoccupazioni legate alla privacy dei dati condivisi.
- Ci dobbiamo però chiedere:
  - Cosa stiamo condividendo? Cosa e’ possibile inferire?
  - Quanto e’ importante la resilienza del sistema?
  - Quanto spesso dobbiamo modificare i dati?

_X. Conclusione: there is no one to rule them all

In conclusione:

- “Full consensus” e’ chiave per ottimizzare e razionalizzare il sistema finanziario (e non solo).
- Questo nuovo modello crea preoccupazioni legate alla privacy dei dati condivisi.
- Ci dobbiamo però chiedere:
  - Cosa stiamo condividendo? Cosa e’ possibile inferire?
  - Quanto e’ importante la resilienza del sistema?
  - Quanto spesso dobbiamo modificare i dati?
- Su queste basi, abbiamo esplorato i requisiti minimi di una “killer” app per proteggere la privacy degli utenti in una retail CBDC.

_X. Conclusione: there is no one to rule them all

In conclusione:

- “Full consensus” e’ chiave per ottimizzare e razionalizzare il sistema finanziario (e non solo).
- Questo nuovo modello crea preoccupazioni legate alla privacy dei dati condivisi.
- Ci dobbiamo però chiedere:
  - Cosa stiamo condividendo? Cosa e’ possibile inferire?
  - Quanto e’ importante la resilienza del sistema?
  - Quanto spesso dobbiamo modificare i dati?
- Su queste basi, abbiamo esplorato i requisiti minimi di una “killer” app per proteggere la privacy degli utenti in una retail CBDC.
- Sta ora agli esperti, su queste basi, costruire una soluzione adeguata!

Grazie mille!

Contatti:

Linkedin: linkedin.com/in/simone-cortese/

Email: simone.cortese@fnality.org / cortsim@uwl.ac.uk