ORWELL

IDC – INTELLIGENT DIGITAL CASH

LA SOLUZIONE CRITTOGRAFICA DI MONETA ELETTRONICA REGOLAMENTATA

Abstract

POTENZA DI CALCOLO: utilizzo della crittografia nell'implementazione di meccanismi di pagamento in cui la compensazione e il saldo possono coincidere.

UN EVOLUZIONE DIROMPENTE: cambia il vecchio modello delle infrastrutture di pagamento. Basta con il sistema centralizzato dove compensazione e saldo sono separati e per definizione differiti.

ACCREDITO IMMEDIATO: L'unione temporale tra la compensazione e il saldo consente transazioni in tempo reale e dunque transazioni commerciali con accredito immediato, il motore principale dell'e-commerce.

CASHFLOW: Non solo il privato ma le aziende, dalla piccola alla multi-nazionale necessitano di cicli di cassa sempre più veloci che possano essere supportati da attività in tempo reale.

NETWORK: I metodi di pagamento devono funzionare come un protocollo di comunicazione, implementando il "pagamento come un servizio di rete" (PANS), consentendo di trasferire tutti i tipi di dati legati e complementari alla transazione. Grazie al sistema PANS, è possibile l'utilizzo di tecniche denominate "Rich Data".

IDC: un esatto bilanciamento tra il pagamento, i dati e regolamentazione bancaria. Un protocollo di comunicazione che consenta l'utilizzo della crittografia e quindi un completo e nuovo sistema di pagamento.

Che cos'è iDC®

iDC®

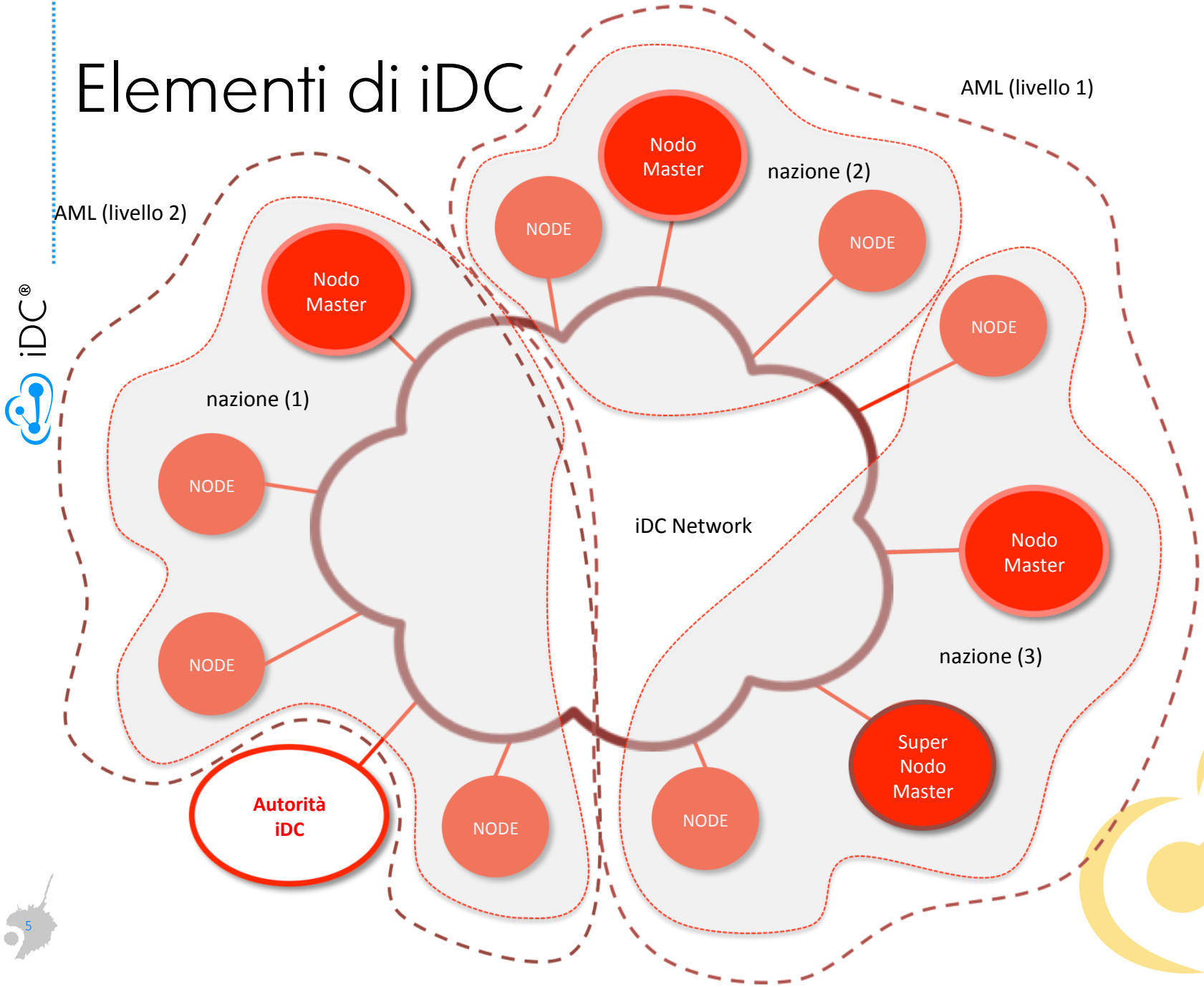
- La moneta elettronica nella sua forma più pura
- Protocollo di Pagamento
- Infrastruttura di pagamento decentralizzata
- Schema di pagamento
- Tecnologia di pagamento in tempo reale Peer-to-peer
- Un sostituto al contante
- Un alternativa infrastrutture centralizzate
- Conforme con EMD, PSD e AMD

- Multi valuta purché il controvalore sia segregato dall'emittente. La moneta elettronica nella sua forma più pura.
- I suoi principi di funzionamento e la sua struttura lo rendono un protocollo di comunicazione utilizzabile per i pagamenti.
- L'intelligenza delle transazioni si trova ai confini della rete, nei Nodi (partecipanti). Non esiste un "Single Point of Failure".
- I partecipanti che aderiscono a iDC possono utilizzarlo in parallelo ai sistemi di pagamento al dettaglio esistenti.
- iDC consente comunicazioni peer to peer, transazioni in tempo reale, in quanto compensazione e saldo coincidono.
- iDC Anonymous Circuit consente il trasferimento di valuta di trasferire conti o portafogli detenuti dai partecipanti a portafogli esterni (smartphone, chiavetta USB, computer hard drive, etc.)
- iDC può essere utilizzato per sostituire infrastrutture di pagamento centralizzate.
- iDC possiede tutte le caratteristiche che consentono il monitoraggio, la tracciabilità e lo screening delle transazioni, richieste dalle normative.

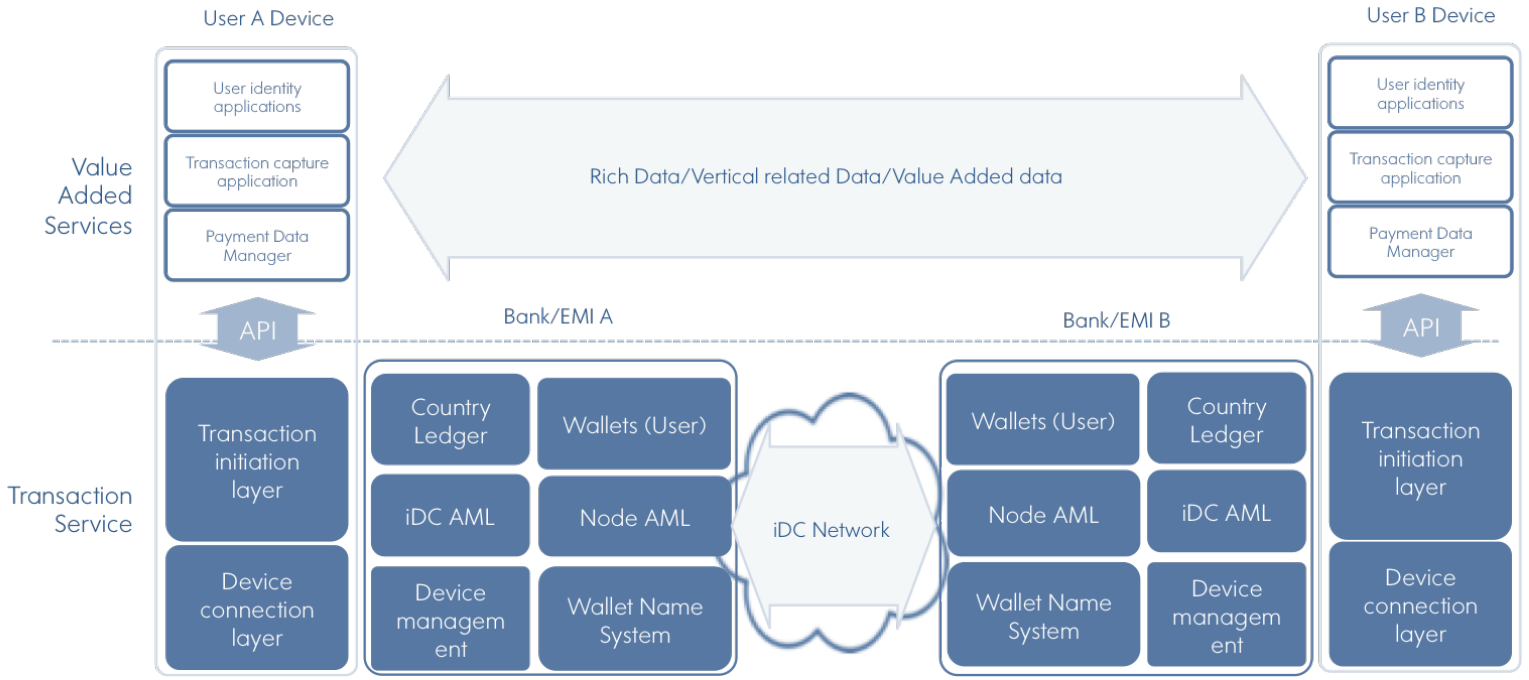
Confronto con le esistenti tecnologie di moneta virtuale

	BITCOIN	RIPPLE	iDC®	Dematerialised Central Bank Money	CASH
Principi	Proof of work Blockchain	Ledger Distribuito Consensus	Blockhain Ledger Distribuito Consensus Close network	Close network	Difficile da falsificare
Emissione	Limitata	Limitata	Senza limiti	Senza limiti	Senza limiti
Valute	Solo BITCOIN	Tutte	Tutte	Tutte	Tutte
Regolato	NO non compatibile con PSD, AMD e EMD	NO non compatibile con PSD, AMD e EMD	SI creato secondo le direttive EMD, PSD e AMD	SI	SI eredita per natura il problema della tracciabilità
Transazioni in tempo reale	NO la validazione avviene da 10 min a 1 ora	Da 2 a 3 secondi	Inferiore al secondo	Da tempo reale a diversi giorni	In tempo reale ma esclusivamente con scambio face-to-face
Emittente autorizzato	NO	NO	SI	SI	SI
Classificabile	NO	NO	SI	SI	N.A.
Sicurezza (debolezze)	Nework Aperto Attaccabile al 50% Dipendente dalla potenza di calcolo	Network Aperto DoS	Sviluppato, eliminando tutti i problemi conosciuti	Central point of failure	Semplice da falsificare Facile da rubare Nessuna tracciabilità
Scalabile	NO	Limitato	SI	SI	N.A
AML	NO	NO	SI	SI	NO

Elementi di iDC



Payment As a Network Service (PANS)



Altri elementi

- iDC Anonymous Circuit:
  - Sostituisce il contante in quanto le unità iDC vengono prelevate e messe in portafogli esterni ai Nodi. I Nodi validano ancora le transazioni, ma gli utenti che pagano non sono conosciuti ai Nodi, quindi non vi è scambio di informazioni.
  - E' possibile limitare gli importi scambiati in linea con le normative antiriciclaggio (in Italia ad esempio il limite del pagamento in contanti è di €999, EMD3 limiterà gli scambi di moneta elettronica anonimi a €250)
  - Ha tuttavia il vantaggio della tracciabilità (le operazioni potrebbero essere tracciate e si possono identificare anche gli indirizzi IP dei dispositivi degli utenti)
  - Gli scambi possono essere soggetti a «hop counting» in modo che dopo un certo numero di transazioni le unità iDC vengono forzatamente trasferite in un portafoglio di un Nodo così che il titolare sia identificabile.
- Sostituzione di un PMI centralizzato esistente
  - Il protocollo iDC potrebbe essere utilizzato per sostituire il PMI centralizzato esistente.
- Trasporto di altri contenuti
  - E' possibile usare l'iDC per il trasporto di altri contenuti e crittografare documenti, come licenze, diritti d'autore, o documenti legati ai diritti commerciali o di diritto di accesso ai contenuti multimediali, ecc..