

Massimo Musumeci

MrBits

Lightning News

Uno sguardo al futuro

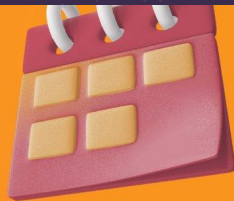


S02E04

23 ottobre 2024



Lugano PlanB e Spazio 21



Speech e Workshop **gratuiti** in Italiano

📍 Asilo Ciani

Venerdì 25 ottobre

10:00 **Presentazione Spazio21**
Speaker: **S&AM**

10:30 **Workshop 1st round**

11:30 **Bitcoin non è crypto**
Speaker: **Francesco Pelle**

12:00 **Workshop 2nd round**

Sabato 26 ottobre

10:00 **Prepararsi all'Apocalisse**
Speaker: **Paolo Ardaino**

10:30 **Workshop 6th round**

Dalla Bitcoin Valley alla Bitcoin Beach
Speakers: **Marco Amadori e Paolo Barrai**

12:00 **Workshop 7th round**

LUNCH BREAK

Interviste Live Webcast Zihuatanejo

14:00	Perché Bitcoin è così difficile? Speaker: Mir	14:00	Bitcoin non fa bollire l'Oceano Speaker: Giorgio Rasetto
14:30	Workshop 3rd round	14:30	Workshop 8th round
15:30	La vera identità di Satoshi Nakamoto Speaker: Giacomo Zucco	15:30	Difendere la sovranità digitale Speaker: Turtlecute
16:00	Workshop 4th round	16:00	Workshop 9th round
17:00	Panel: Worst and best case scenarios Speakers: Riccardo Masutti, Turtlecute, Leonardo Comandini Moderatore: Mattia	16:30	Panel: Bitcoin è di destra o sinistra? Speakers: Giacomo Zucco, Rikki Moderatore: Federico Rivi
17:30	Workshop 5th round	17:00	Workshop 10th round



E se partecipi a 5 workshop, puoi ottenere 10 CHF sul tuo wallet e un biglietto per FC Lugano-BSC Young Boys del 27.10!



Workshop

Venerdì 25 ottobre

Sala Custodia

- 10.30 Custodia con Bitbox: teoria e pratica (Luca - Bitbox) ●
- 12.00 Lunga vita al tuo Bitcoin Wallet (Luca - Bitbox) ●●
- 14.30 Custodia con Jade (A. Saggi - Blockstream) ●
- 16.00 Generazione entropia con dadi (Marij - PlanB Network) ●●
- 17.30 Custodia con Bitbox: teoria e pratica (Luca - Bitbox) ●

Sala Nodi

- 10.30 Perché avere un nodo? (Mattia - Plan B Network) ●
- 12.00 Test e certificato di Plan B Network
- 14.30 Nodo: quale dispositivo usare (Mattia - Plan B Network) ●
- 16.00 Impariamo a usare un nodo (Alekos Filini) ●●
- 17.30 Il potere della decentralizzazione (A. Caccese - BitPoliTo) ●

Sala Mining

- 10.30 Come funziona il Mining (G. Artusio - BitPoliTo) ●
- 12.00 Come funziona il Mining (G. Artusio - BitPoliTo) ●●
- 14.30 Mining Game (M. Amadori - Bitcoin valley) ●
- 16.00 Mining Game (M. Amadori - Bitcoin valley) ●
- 17.30 Miniamo con un S9 / miniminer (G. Artusio - BitPoliTo) ●●

Sabato 26 ottobre

Sala Custodia

- 10.30 Utilizzo di Jade - Avanzato (A. Saggi - Blockstream) ●●●
- 12.00 Do It Yourself Jade (Andrea, M.) ●●
- 14.30 Do It Yourself Jade (Andrea, M.) ●●●
- 16.00 Generazione entropia con dadi (Marij - PlanB Network) ●●
- 17.00 Do It Yourself Jade (Andrea, M.) ●●●

Sala Nodi

- 10.30 Importanza e scelta del nodo (L. Comandini - Blockstream) ●●
- 12.00 Utilizzo del nodo - avanzato (L. Comandini - Blockstream) ●●●
- 14.30 Impariamo a usare Bitcoin Core (D. Brozzoni) ●●
- 16.00 Impariamo a usare Bitcoin Core (D. Brozzoni) ●●●
- 17.00 Partecipare attivamente alla rete (A. Caccese - BitPoliTo) ●●

Sala Mining

- 10.30 Come funziona il Mining (G. Artusio - BitPoliTo) ●●
- 12.00 Gioco POW (M. Farina I.I.S. J. C. Maxwell) ●
- 14.30 Gioco POW (M. Farina I.I.S. J. C. Maxwell) ●
- 16.00 Gioco Mining (M. Amadori - Bitcoin valley) ●
- 17.00 Minare con S9 e miniminers (G. Artusio - BitPoliTo) ●●

Sala Transazioni

- 10.30 Sparrow Base (M. Gandolfi + Laura - Bitcoin Campus) ●
- 12.00 Sparrow Intermedio (M. Gandolfi + Laura - Bitcoin Campus) ●●
- 14.30 Electrum Base (M. Gandolfi + Laura - Bitcoin Campus) ●
- 16.00 Electrum Intermedio (M. Gandolfi + Laura - Bitcoin Campus) ●●
- 17.30 Sparrow Intermedio (M. Gandolfi + Laura - Bitcoin Campus) ●●

Sala Acquisto + LN + Ricompense

- 10.30 Acquisto e Lightning Network (base) (M. Musumeci) ●
- 12.00 Lightning Network e il ruolo negli acquisti (M. Musumeci) ●●
- 14.30 Vexl e acquisto p2p (M. Giorgetti - Vexl Community Manager) ●●
- 16.00 Introduzione acquisto e LN (A. Messina - BitPoliTo) ●●
- 17.30 Introduzione acquisto e LN (D. Vitabile - BitPoliTo) ●

Livello (indicativo):

- Facile ●
- Medio ●●
- Difficile ●●●



Consulta l'agenda e scopri di più

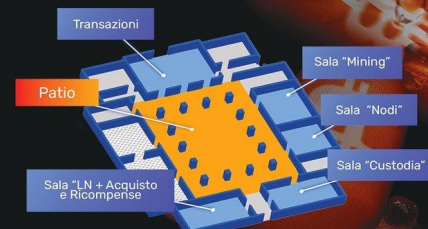


Sala Transazioni

- 10.30 Multisig (multifirma) (M. Gandolfi + Laura Bitcoin Campus) ●●●
- 12.00 Wallet Mobile + Portal (Alekos Filini) ●●
- 14.30 Transazioni - Avanzato (L. Comandini - Blockstream) ●●●
- 16.00 Transazioni - Intermedio (L. Comandini - Blockstream) ●●
- 17.00 Sparrow avanzato e multifirma (Marij - PlanB Network) ●●●

Sala Acquisto + LN + Ricompense

- 10.30 LN e il ruolo negli acquisti (M. Musumeci) ●●
- 12.00 Vexl e acquisto p2p (M. Giorgetti - Vexl Community Manager) ●●
- 14.30 Lightning Network, acquisto, Swap e nodi (M. Musumeci) ●●●
- 16.00 Acquisto e Lightning Network (Davide Vitabile - BitPoliTo) ●●
- 17.00 Acquisto e Lightning Network (A. Messina - BitPoliTo) ●●





Prevediamo il futuro

- Con le elezioni americane è tornata alla ribalta una piattaforma di prediction market, Polymarket
- Piattaforme centralizzate che permettono la compravendita di shares che rappresentano l'avverarsi di un evento (sportivo, politico, demografico, ecc.)
- Dopo alcuni test degli scorsi mesi, è arrivata una piattaforma quasi pronta all'uso beta.predyx.com, e da poco un'altra bitcoinprediction.info
- Da usare con cautela, ma i volumi iniziano ad essere interessanti, anche per l'arbitraggio





Il problema dell'ultimo miglio su LN

- LN è realtà, con investimenti e progetti di ampio respiro, al momento è il progetto scelto da tutta la community per scalare Bitcoin
- Le soluzioni custodial sono pronte e con un'ottima UX, ora la sfida è il non-custodial
- Un problema molto simile a quello dell'ultimo miglio nelle varie reti di trasporto, dove raggiungere gli utenti remoti è la parte più complicata e costosa
- Le soluzioni oggi disponibili richiedono sempre una transazione onchain per l'onboarding, con conseguente costo proibitivo in caso di fee alte



Cosa manca al self custodial

- Due sono i punti principali da migliorare per portare l'UX self custodial di LN al pari di quella del layer 1
 - Interazione del wallet: i wallet devono essere online 24/7 per ricevere pagamenti, e gli sviluppatori si stanno impegnando per mitigare questo problema (Aqua con architettura Liquid, Breez con le notifiche dell'OS)
 - Interazione con la blockchain: onboarding, splicing, swap/loop richiedono sempre una tx onchain.
Da qua nasce la necessità di trovare soluzioni per ridurre o eliminare la necessità di transazioni onchain



Channel Factory

- Proposta del 2018, che richiede qualche tipo di covenant per l'utilizzo su Bitcoin.
- Un provider blocca un quantitativo di BTC che verrà poi usato per aprire canali dei propri utenti, senza necessità di transazioni onchain.
- I covenant garantiscono che i fondi possano tornare agli utenti nel caso di chiusura dei canali stessi, grazie alla spendibilità della transazione di chiusura che garantisce la suddivisione dei fondi tra gli utenti.
- Anche lo splicing e la gestione della liquidità può essere gestita dalla channel factory stessa
- Sono necessarie solo poche transazioni onchain periodiche che contengono tutte le variazioni



Ecash

- Altra proposta per l'ultimo miglio è Ecash, ed in particolare implementazioni già presenti sul mercato come Cashu e Fedimint
- I vantaggi di questo approccio sono: semplicità di utilizzo, nessuna gestione di canali e liquidità, transazioni rapide e gratuite all'interno della federazione
- Gli svantaggi invece sono la fiducia che bisogna riporre verso la federazione, e la complessità di gestione della federazione stessa
- Ottima soluzione per importi molto piccoli, precedenti all'apertura di un canale vero e proprio, magari integrandola con l'utilizzo di sidechain come Liquid



ARK

- Ark è una proposta di maggio 2024, per un nuovo protocollo che si affianca a LN per effettuare transazioni off-chain in modo nuovo e diverso da Lightning Network.
- Viene introdotto il concetto di VTXO (Virtual UTXO), cioè un oggetto che possiede la capacità di creare un UTXO in un secondo momento
- Al momento è possibile utilizzare le funzioni di ARK senza l'attivazione dei covenant (clARK), ma riponendo fiducia negli ASP, ARK service provider
- Questo protocollo si propone come complementare a LN, permettendo scalabilità e flessibilità nella gestione della liquidità nei canali





Covenant e Layer2

Peter Todd has pubblicato qualche settimana un confronto approfondito tra i vari covenant proposti.

<https://petertodd.org/2024/covenant-dependent-layer-2-review>

Le conclusioni sono abbastanza chiare: dopo aver risolto il consensus cleanup (una serie di fix a bug ancora presenti nel codice di Bitcoin), sarà necessario passare ad una implementazione di covenant, che permetta di risolvere il problema della scalabilità (non prima di una lunga fase di test, per molte proposte già in corso).

Tra quelle con i migliori trade-off citiamo CTV e OP_CAT

