TABConf 2022

[K] Keynote [L] Live-Code [P] Panel [R] Party [S] Socratic [T] Talk [W] Workshop

OCTOBER 14 • FRIDAY

9:30am – 10:00am	K	**André Neves Keynote** *Speakers: André Neves*	Main Stage
9:30am – 10:15am	T	**PlebLab Presents: Coach Kyle's Corner** *Speakers: Kyle Murphy* Got questions about starting up a dev lab, running hackathons, or building startups? Come get some insights from PlebLab founder Kyle Murphy.	Village: PlebDev
9:30am – 5:00pm		**Bitcoin Gaming**	Village: Gaming
9:30am – 5:00pm		**NextGen Activities** *Speakers: Elly Pembroke*	Village: NextGen
10:00am – 10:45am	P	**Inheritance planning panel and Q&A** *Speakers: Josh Jalinski, Justine Harper, Jared Pierce, Terrence Yang* Are you a responsible hodler, but you're not sure what will happen to your Bitcoin when you are no longer around to control the keys? Learn about inheritance planning strategies and pitfalls from experienced lawyers and financial planners. They will answer your questions and help you avoid the worst case scenario: not being prepared at all.	Village: NextGen
10:00am – 10:45am	T	**When the Bulls are Away, the Devs Will Play: Finding and Teaching Bitcoin Devs** *Speakers: Adam Jonas* Come for the memes but stay for an analysis of the bitcoin developer shortage and what we can do about it.	Main Stage
10:15am – 11:00am	T	**Nostr Workshop** *Speakers: Brill Saiton* You've heard about Nostr, come learn about building on it from Super Testnet, Lightning Escrow's world class CTO.	Village: PlebDev
10:45am – 11:45am	S	**Welcome & Socratic Panel: The "G" Word** *Speakers: Jeremy Rubin, Matt Corallo, Buck* Bitcoin is rife with complexity. Generally speaking, this complexity is most widely understood to manifest as an extension of the feature-set available to the network and the interactions among users who exercise these functions in their unique contexts. But complexity also exists within the processes which govern modifications to Bitcoin's consensus critical code pathways. Understanding, improving upon and ensuring robustness in these processes is vital to Bitcoin's long term survival. In this panel we will investigate different perspectives on these processes and how we as a community can constructively work together in an increasingly adversarial world.	Village: BitDevs Socratic
11:00am – 11:45am	P	**Onchain Panel** *Moderators: Daniel Ameli* *Speakers: Andrew Chow, Gloria Zhao, Murch, Pieter Wuille*	Main Stage
11:00am – 12:20pm	L	**Live Code-athon: niftynei (Blockstream / CLN / Base58)** *Speakers: niftynei* Come do some 'coder' bingo, eat some popcorn, and watch leet hackers work on a something live!	Village: PlebDev
11:30am – 12:30pm		**Lunch**	Hallway

12:00pm – 12:45pm	P	**Offchain Panel** *Moderators: Paul Itoi* *Speakers: Olaoluwa Osuntokun, Valentine Wallace, Bastien Teinturier, Gregory Sanders, Tadge Dryja* Come find out what's coming in the next chapter of the Lightning network. We'll discuss the tradeoffs between privacy and reliability and you'll learn about trampoline payments, eltoo, asynch payments, and more.	Main Stage
12:00pm – 4:00pm		**Chess Tournament** *Speakers: Mike Jarmuz*	Village: Gaming
12:15pm – 1:15pm	S	**Socratic Panel: Transaction Introspection** *Moderators: Ras @coinward* *Speakers: Burak, Keagan, Sanket Kanjalkar* Covenants offer the promise to extend Bitcoin into something more useful than its already proven to be, but require serious consideration. This panel will dive into the ascendant topics most critical to the covenant discussion. We'll attempt to elucidate a clearer picture of the various implementations which add more transaction introspection to the bitcoin protocol. Following the noteworthy approaches to implementing covenants that introduce new opcodes can be a rollercoaster. We've got a great group that can not only help get everyone up to speed, but peek into the future that may already be possible with bitcoin script as it exists today.	Village: BitDevs Socratic
12:30pm – 2:00pm	L	**Live Code-athon: Rachel Rybarczyk (Stratum v2)** *Speakers: Rachel Rybarczyk* Come grab a "coder" bingo card, get some popcorn, and watch some leet coders work on code live. Some in-person, some remote.	Village: PlebDev
1:00pm – 1:45pm	P	**Legal Panel** *Moderators: Justine Harper* *Speakers: Hussein Badakhchani, Zack Shapiro, Stan Sater*	Main Stage
1:45pm – 3:00pm	S	**Socratic Session: Bitcoin Development** *Speakers: Ben Carman, Murch* A focused Socratic Seminar on Bitcoin protocol development. Topics will be selected from mailing lists, prominent github repos, network graphs, research papers, vulnerability reports and other sources.	Village: BitDevs Socratic
2:00pm – 2:45pm		**Intro to tinkercad for 3d printing** *Speakers: Aria Pembroke*	Village: NextGen
2:00pm – 2:45pm	P	**Stablecoins on lightning** *Moderators: Graham Krizek* *Speakers: Olaoluwa Osuntokun, Ryan Gentry*	Main Stage
2:00pm – 3:30pm	L	**Live Code-athon: Evan Kaloudis (Zeus)** *Speakers: Evan Kaloudis* Come grab a "coder" bingo card, get some popcorn, and watch some leet coders work on code live. Some in-person, some remote.	Village: PlebDev
3:00pm – 3:45pm	T	**ROAST: Robust Asynchronous Schnorr Threshold Signatures** *Speakers: Tim Ruffing*	Main Stage
3:00pm – 3:45pm	W	**Intro to digital logic** *Speakers: Silas Pembroke* We will use a digital logic simulator to show how fundamental logic gates can be combined to create adders, multipliers, and binary counters. This interactive course has specifically been designed for TabConf by Silas.	Village: NextGen

3:15pm – 3:45pm	T	**CoinPools** *Speakers: Antoine Riard* We'll recall the privacy notions for second-layers (counterparties confidentiality, protocol usage, contract content confidentiality, third party leaks, the types of privacy leaks and attacks), how CoinPool enables to uplift many L2s in a single wrapper, and the specific "new" attacks vectors against multi-party constructions and potential mitigations.	Village: BitDevs Socratic
3:30pm – 5:00pm	L	**Live Code-athon: Rusty Russell (Blockstream / CLN)** *Speakers: Rusty Russell* Come grab a "coder" bingo card, get some popcorn, and watch some leet coders work on code live. Some in-person, some remote.	Village: PlebDev
4:00pm – 4:30pm	T	**Provably Bug-free BIPs & Implementations** *Speakers: Jonas Nick* Writing good specifications is hard. Misinterpretations of seemingly minor aspects can result in catastrophic vulnerabilities in implementations. Therefore, in the BIP draft "Half-Aggregation of BIP 340 Schnorr signatures" recently published by Blockstream Research, we use a different approach than previous cryptography BIPs. Most importantly, our draft includes a _formal_ specification (a mathematically precise description of the scheme) written in the hacspec language, a subset of rust. This type of specification allows using software tools to prove security properties and the absence of certain kinds of bugs. Moreover, developers are able to write implementations whose behavior is provably identical to that of the specification.	Village: BitDevs Socratic
4:00pm – 4:45pm	T	**Lightning is Broken AF (But We Can Fix It)** *Speakers: Matt Corallo*	Main Stage
4:00pm – 4:45pm	W	**Interplanetary Bitcoin** *Speakers: Asher* Let a former NASA scientist virtually take you on a journey through space. We will point out Blockstream satellites, discuss timechain synching with extraterrestrial nodes, and take audience suggestions for planets, stars and galaxies to visit.	Village: NextGen
4:00pm – 6:00pm		**Chess Finals** *Speakers: Mike Jarmuz*	Village: Gaming
4:35pm – 7:30pm	W	**Codex32** *Speakers: Andrew Poelstra* Codex32 is an error-correcting code designed to be computable without the use of electronic computers. Users can compute and verify checksums by hand; we have provided lookup tables, volvelles and worksheets to assist with this process. The codex32 checksum, like all linear codes, is compatible with Shamir's Secret Sharing Scheme, a mechanism to split a secret into many "shares", such that the original secret can be reconstructed from some number of them. In SSSS, users choose a threshold value k, typically 2 or 3; they then generate k-many random shares, and then compute a number of derived shares (up to 31 in total). A random secret can then be computed from any k shares. If the initial random shares have a valid codex32 checksum, then so will all the derived shares and the final secret.	Village: BitDevs Socratic

5:00pm – 6:00pm W **Keysigning Party!** Village: PlebDev

Speakers: niftynei, Murch

Got a GPG Key? Key signing parties are an opportunity to expand your keyring of people you've verified (in-person).

If you want to attend, please sign-up and submit your exported public key by email to murch@murch.one in advance.

Bring a drivers license/passport or other identity document, if you want others to attest to you identity.

What?

• Exchange GPG keys with other attendees

Who?

• Developers who want to use their keys to sign releases
• Others who want to help each other to attest their keys' authenticity

How?

• 5:00: Meet, chat, and handout list of fingerprints
• 5:10–5:30: Present each attendee's fingerprint
  • Each fingerprint is presented separately on a slide
  • Key owner confirms fingerprint and UID, reads last 16 characters of fingerprint
  • Other attendees mark entry on their personal list as desired
• 5:30–5:45: Check other attendees' identification where requested
• 5:45–end: Hang out

Before?

• Submit your public key, fingerprint and UID by email to Murch by 2022-10-14, 12pm

After?

• Certify the keys of other attendees
• Send public key with added signature to key owner. Encrypt it to the owner's key, and send it to the owner's email address corresponding to the UID you signed.

7:00pm – 10:00pm R **Afterparty** STATS Brewpub (300 Marietta Street NW, Atlanta, GA)