TABConf 2022

W Workshop

OCTOBER 13 • THURSDAY

9:00am – 10:00am W **Intro to Zero Knowledge Proof** Village: PlebDev

Speakers: Nadav Kohen

9:00am – 10:00am W **Simplicity Playground** Main Stage

Speakers: Burak

Title: Simplicity Playground

Duration:
30-60 Mins

What will I learn?
You will get to know Simplicity basics and how to write Simplicity programs with no prior background in bitcoin programming.

What will I get out of this workshop?
– Types, Terms, and Arguments in Simplicity
– Typing rules and strict script-wiz typing format
– Defining bits, bit-strings and byte-strings
– Writing and executing Simplicity programs

What knowledge do I need beforehand?
No programming skills are required.

Do I need to setup an environment or download any software?
Nope. Just bring your web browser.

Do I need access to a BTC or LN node?
No.

Anything else I should know?
No.

9:00am – 10:00am W **Watching for forks in the Bitcoin network** Village: BitDevs Socratic

Speakers: Thomas Sharp

Watching for forks in the Bitcoin network

Goals:
1. Understand what a fork is, and the need for a fork monitor.
2. Explain forkscanner, a rust implementation of fork monitoring, and how it uses the bitcoin network.
3. Demonstrate usage of the forkscanner.

Overall:
We'll talk about watching forks, stale blocks, potential double spend attempts.
We'll show our implementation of a fork scanner, and show how to bring it up and configure it.

Prerequisites:
Some basic BTC knowledge, though we can go over some of that for background info.
If they would like to follow along, I'd recommend installing docker, and nodejs.
Access to nodes will be needed, we can look at providing access to ours.

10:00am – 11:30am W **Build a fedimint module** Village: BitDevs Socratic

Speakers: Justin Moon

Most people are familiar with Fedimint as a federated chaumian mint, but you could build practically any application in a federated manner using Fedimint. In this workshop we'll build a Fedimint module which allows people to bet on the bitcoin price. Along the way you'll setup a Fedimint development environment, get a high-level tour of the codebase, and learn how existing functionality like ecash is implemented in Fedimint.

To get ready for the workshop, try to setup a fedimint developer environment yourself

If you get stuck, ask for help in discord

10:00am – 11:30am W **Building Lightning-based Authentication with LSATs** Main Stage

Speakers: Buck

Slides: https://docs.google.com/presentation/d/1lGONa4CpQz3nEXpO1oLBFiGa7st2YKUZyKWhhDLNb3s/edit?usp=sharing

Duration:

1.5 hours?

Can go longer or shorter depending on what's the most useful and valuable to participants given the rest of conference.

Goals:

- Learn about Lightning Service Authentication Tokens (LSATs), the 402 Response Error Code why macaroons are better than cookies, and how they can be used to build a better authentication ecosystem
- Practice parsing and validating LSATs with the LSAT Playground (https://lsat-playground.vercel.app/)
- Build your own custom paywall using LSATs by deploying a proxy server that is capable returning 402 responses and validating paid requests to access a restricted endpoint
- Extra credit: support for delegation- clients can sell restricted use of an LSAT they paid for to another user.

Pre-requisites:

(I'll probably need to update this as I actually try and build out the workshop exercise)

- Setup Polar (https://lightningpolar.com/) or similar for a local bitcoin and lightning network dev environment
- recommended knowledge: read up on LSATs from lightning labs' docs (https://lsat.tech/) and macaroons vs cookies (https://hackingdistributed.com/2014/05/16/macaroons-are-better-than-cookies/)
- play around with the LSAT Playground (https://lsat-playground.vercel.app/)

10:00am – 11:30am W **Intro to Multisig & Sovereign Recovery** Village: PlebDev

Speakers: Trey Sellers, Tyler Campbell, Justine Harper

What will I get out of this workshop?

A deeper understanding of multisig technology, as well as, how to build your own multisig wallet/address (and rebuild it) across multiple wallet software platforms.

What will I learn?

Multisig overview, single-sig vs multi-sig, building a multi-sig wallet, deep dive into recovering your multi-sig wallet, and intro to collaborative multi-sig custody.

Description

Join the Unchained team for a workshop all about multi-sig! Multisig is a bitcoin native protocol that allows you to build wallets created with multiple keys, while also establishing your own quorum of signatures needed to redeem (or spend) that bitcoin. In this workshop, we will be digging into the nuts and bolts of multisig and walking you through how to build your own. Good for beginners, or those who are just trying to continue to build their knowledge.

What knowledge do I need beforehand?

All are welcome – We will start with the basics!

Do I need to set up an environment or download any software?

Nope!

Do I need access to a BTC or LN node?

Nope!

Anything else I should know?

We will be raffling off a Coldcard Mk4 as well as some other swag at the end of the workshop for those who actively participate.

11:30am – 12:30pm W **Attacking lightning** Village: BitDevs Socratic

Speakers: Tony

Attacking Lightning Workshop

Time Duration:

60 Minutes

Goals:

- What will attendees get out of this workshop?
- Hands on experience exploiting known vulnerabilites on Lightning
- What will attendees learn?
- They will learn what some of the vulnerabilities are on Lightning and how to exploit them and defend from them.

Description:

- Describe the overall workshop and spirit of what will happen.
- This will be very "Red Team" / "Hack The Box" style where attendees will have a simulated Lightning Network on their computer (via custom polar docker nodes) and their job is to "Capture The Flags" via attacking the other simulated nodes. Such attacks include things like channel jamming to stop payments, finding unannounced channels, inserting themselves into routes to find payments between two nodes, etc.
- The spirit is to have fun but also learn how some of the attacks can be a concern.
- I will help walk people through it and ideally present so people can follow along, but they are also encouraged to experiment on their own.

Prerequisites:

- Any recommended knowledge needed?
- How to use Polar and understand basic Lightning networking / opening channels / making payments.
- Any setup of an environment / software downloaded?
- Polar with custom docker images. Instructions will be given on how to do this.
- Is access to BTC or LN node needed?
- Only locally via Polar.
- Anything else?
- Requires own computer with Docker & Polar installed.

11:30am – 12:30pm W **Demystifying Elliptic Curves** Village: PlebDev

Speakers: Asher

Demystifying Elliptic Curves

runtime: approx 1h

We provide a gentle introduction to elliptic curve cryptography, including continuous and finite point spaces, point addition, and point multiplication, with application to ecdsa signatures, secret sharing and encrypted messaging. The material is presented in a visual manner supported with interactive dashboards. This allows for an intuitive grasp of the basic components behind bitcoin scripting with no prior knowledge of programming languages required. All materials are available on github, and attendees are encouraged to contribute
https://github.com/asher-pembroke/elliptic

11:30am – 12:30pm W **Intro to Rapid Gossip Sync with LDK** Main Stage

Speakers: Arik Sosman, Conor Okus

Goals: Attendees will get an overview of the Rapid Gossip Sync protocol, how to use it and how it improves the UX in certain environments such as mobile.

Description:

- What is Rapid Gossip Sync?
- RGS vs P2P
- A walkthrough of using RGS to fetch channel graph data
- Visualise the network graph in a browser using d3.js

Prerequisites:

- General lightning network knowledge is beneficial
- Access to a laptop with node.js installed
- The workshop GitHub repo can be found here - https://github.com/arik-so/rgs-workshop

Join our Discord - https://discord.gg/5AcknnMfBw

1:30pm – 3:00pm W **Starter kit for building your own bitcoin hardware project with MicroPython** Village: PlebDev

Speakers: Keith Mukai

Workshop title:

Starter kit for building your own Bitcoin hardware project w/MicroPython

Workshop description:

What if you could devise your own Bitcoin hardware device from a cheap, off-the-shelf microprocessor board? What new, innovative solutions would you create?

Keith will walk you through the building blocks you'll need to get started. We'll build a Bitcoin-enabled custom MicroPython firmware for a variety of inexpensive microprocessor boards (e.g. ESP32, Raspi RP2040, STM32). We'll compile in Bitcoin Core's secp256k1 library for fast elliptic curve calculations. We'll also include Stepan Snigirev's "embit" library (used by Specter Desktop, Specter-DIY, SeedSigner) to provide higher-level Bitcoin functions; I don't know how to sign a psbt or what to do with secp256k1 but Stepan's library does!

We'll then briefly discuss incorporating displays, UI/graphics libraries (LVGL), cameras, buttons, etc.

From this starting point you'll be able to build ANY Bitcoin hardware project you can imagine, coding it in easy, mostly-familiar MicroPython (essentially the same as Python 3 but with some limitations).

Prerequisites for attendees:

* Basic Linux and Python proficiency.
* Laptop w/Docker installed. Downloading dependencies (compilers, etc) ahead of time will speed things up.
* ZERO experience with MicroPython or microprocessor boards required.

Supplies needed:

Attendees will receive a FREE esp32-S2 kit, courtesy of Bitcoin Magazine! All you need to bring is a laptop and a micro USB cable.

1:30pm – 3:30pm W **Packaging Your Favorite Open Source Project for Start9 EmbassyOS** Village: BitDevs Socratic

Speakers: Matt Hill, Dread

Workshop Title:
Packaging Your Favorite Open Source Project for Start9 EmbassyOS

Time Duration:
- How much time is needed to complete the workshop?
Ideally, 2 hours.

Goals:
- What will attendees get out of this workshop?
If they follow along on with their own Embassy One, they will get their own custom app running on their EmbassyOS

What will attendees learn:
Service Packaging Best Practices for the Start9 EmbassyOS

Description:
- Describe the overall workshop and spirit of what will happen.
Are you tired of waiting for your favorite Bitcoin applications to show up on your Start9 Embassy? Have you ever wanted to use your own custom web-based application hosted on your own server?
This workshop will show you step-by-step how to package, install, and run your choice of software on Embassy. Minimum development experience is needed, as this workshop will be just the beginning of your hero's journey into service packaging for Embassy. Get ready to join the community of package developers building out the future of sovereign computing!

Prerequisites:
- Any recommended knowledge needed?
Recommended: basic programming background

Any setup of an environment / software downloaded:
Environment Setup is optional but recommended. Setup instructions here: https://start9.com/latest/developer-docs/getting-started/environment-setup

Is access to BTC or LN node needed:
No.

Anything else:
Optional in order to follow along, bring your own Embassy,
or your own DIY Equipment (Raspberry Pi, 1TB SSD Drive, 32GB SD Card)

1:30pm – 3:30pm W **Working with the Taro Protocol** Main Stage

Speakers: Hannah Rosenberg

Title:

Working with the Taro Protocol

Duration:

90 mins

Workshop Goals:

After the workshop attendees should...

- Have a solid understanding of what Taro is and what it can and can't do
- Understand some basic Taro use cases
- Be able to differentiate between Taro universe types
- Understand the basics of how fungible assets are transferred on the Lightning Network
- Have experience installing and configuring Taro, and created their own (regtest/testnet) asset

Description:

This workshop is designed for tech savvy Bitcoiners who want to dive into the Taro protocol! After 90mins attendees will leave with a solid understanding of what Taro is, how it can be used, and will gain some hands-on experience with the Taro client.

Prerequisites:

- A solid understanding of the Bitcoin protocol, familiarity with the Lightning Network, and a basic understanding of Taproot.
- Access to a computer with GoLang installed and a regtest/testnet Bitcoin node setup.
- Some familiarity with Linux/Unix as all examples and demos will be shown on a Ubuntu server.

Recommended reading/viewing prior to the workshop:

- https://youtu.be/-yiTtO_p3Cw
- https://docs.lightning.engineering/the-lightning-network/taro

3:00pm – 3:30pm W **Magma Channel Shop, Earn Income with your liquidity** Village: PlebDev

Speakers: Jesse

Workshop Title:
Magma Channel Shop

Time Duration:
15-30 mins

What will attendees get out of this workshop:
Experience purchasing a channel and posting a channel offer on Magma

What will attendees learn:
How to use Magma Channel Marketplace, Valuing Liquidity on Lightning, How to post an offer, How to buy a lightning channel.

Description:
Attendees will learn fundamentals of lightning liquidity and what makes it valuable. Magma channel marketplace will be explained, enabling attendees to post an offer of bitcoin liquidity and to buy an offer if they would like.

Prerequisites:
Available for LND nodes and is a standard offering for Umbrel, Raspiblitz, and Voltage.

Is access to BTC or LN node needed?
Yes, bitcoin and a lightning node are required.

Anything else?
A willingness to learn! Voltage can set you up with a node, but participation requires that your node already has a channel and is visible in the lightning network graph. This sometimes takes several hours after opening a channel.

3:30pm – 4:30pm W **Getting started with lnc-web** Main Stage

Speakers: Evan Kaloudis

Workshop Title:
Getting started with lnc-web

Time Duration:
45-60 min

Goals:
Attendees will get an overview of how Lightning Node Connect works and be able to get started with building our own lightning web apps with lnc-web

Description:
- Overview of LNC
- Overview of lnc-web
- Overview of Lightning Terminal and getting an LNC connection string
- Walkthrough of setting up LNC connection
- Walkthrough of available calls
- Demo app

Prerequisites:
- General knowledge of LN recommended
- LND node with LITD on mainnet or testnet required
- Node.js required
- Experience with ReactJS frontend recommended

3:30pm – 5:00pm W **Remote signing for lightning node** Village: PlebDev

Speakers: Paul Itoi

Hosted by Evan & Jules

Workshop Title:

Remote Signing for Lightning Node

Time Duration:

1-1.5 hours

Goals:

- What will attendees get out of this workshop?

Hands on experience running learning real life use cases for separating the private keys from hosted lightning nodes.

They get to take home a prototype board that works with Core lightning (possibly greenlight as well).

What will attendees learn:

How to flash, pair and use a remote signing device running the Validated Lightning Signer with Core Lightning (artist formerly known as c-lightning)

https://vls.tech (they will launch their site soon)

Recommended knowledge needed:

Ability to use CLI for tailing logs.

Prerequisites:

https://github.com/stakwork/sphinx-key/blob/hardware-readme/sphinx-key/README.md

- Is access to BTC or LN node needed?

No, we will host or Voltage will assist in booting up Core lightning nodes.

Anything else?

They will need to run Sphinx on their mobile device to configure the signer hardware.

3:30pm – 6:30pm W **98% Real bitcoin smart contracts - Learn by playing a fun game.** Village: BitDevs Socratic

Speakers: Jeremy Rubin

98% Real Bitcoin Smart Contracts™
Learn by playing a fun game.

Time Duration:
- How much time is needed to complete the workshop? 3 - 3.5 Hours

Goals:
- What will attendees get out of this workshop?
- Good Vibes
- Play a fun game

What will attendees learn:
- Understanding how to architect Federated Smart contracts with Judica's Software
- Basics of Sapio
- Basic Bitcoin DeFI Concepts
- Rollups
- Alternative Market Makers
- NFT-ized Positions (Bundling into a new asset)
- Bonded Attestation Chain (Off chain protocol for ensuring honest event sequencing)
- https://rubin.io/bitcoin/2021/12/17/advent-20/
- How to define rules for automated Bitcoin contract execution
- Types of smart contracts that can be built in Bitcoin
- What it takes to deploy to the real world

Description:
- Describe the overall workshop and spirit of what will happen.

Judica is building a complete toolchain that unlocks a new paradigm for Bitcoin Smart Contract Development. Does that sound Big, Complicated, and Scary? It doesn't have to be – to make it easy and fun to learn, we've created a low-latency multiplayer bitcoin mining empire-building game that is backed by 98% Real Bitcoin Smart Contracts™ that you can join us to play.

After a few solid play sessions, we'll dive into how it all works under the hood and relates to non-game applications, followed by an open discussion on the frontier of what you can build.

Prerequisites:
- Any recommended knowledge needed?
- To Play:
- Setting up / Configuring software (git, installing dependencies, building)
- comfortable with basic command line usage
- To Learn:
- Knowledge of how Bitcoin Transactions work
- Knowledge of the capabilities of Bitcoin Script
- Any setup of an environment / software downloaded?
- Game software (to be distributed at workshop / Builder Day)
- Support for Unix (Mac / Linux) OS, Limited Windows Support
- Is access to BTC or LN node needed?
- Come with a Local Bitcoin Core Node on laptop or otherwise reachable (mainnet Pruned OK, we may connect to custom Signets day-of)

Anything else?
- Open mind, good attitude
- Optional: Come with a group of up to 5 people (we'll pair up people who come without)

4:30pm – 6:30pm W **Integration of Lightning into webApps** Main Stage

Speakers: Nate

What will I get out of this workshop?

You will gain a basic familiarity of the integration of both backend and frontend webapp development with lightning functionality.

What will I learn?

You will learn the basic functions and processes to connect a lightning node to webapps.

Description

Follow along with the devs of Voltage as they walk through the process of connecting a lightning node to a pre-built webapp project. Only a laptop is required to participate. All knowledge levels are welcome to join in. This will be a beginner friendly workshop. We are hoping to inspire and grow confidence in the developer community to integrate lightning into more applications.

What knowledge do I need beforehand?

- Basic python or JS.
- Familiarity with LND encouraged but not required.

Do I need to setup an environment or download any software?

No. We will be utilizing a pre-built environment to keep it simple, but you may clone it if you wish during the workshop setup.

Do I need access to a BTC or LN node?

No. It will be provided as part of the workshop, including liquidity so we can skip as much set-up as possible and get right into the fun.

5:00pm – 6:30pm W **Setting up Vortex on your lightning node** Village: PlebDev

Speakers: Ben Carman

Workshop Title:

Setting up Vortex on your lightning node

Time Duration:

1 - 1.5 hours

Goals:

- What will attendees get out of this workshop?

- A setup testnet(or signet) node with a coinjoined channel
- an understanding of what vortex is and how it works
- knowledge of how to set vortex up on their own node

Description:

- Describe the overall workshop and spirit of what will happen.

Plan:

- intro on what vortex is
- over view of the software
- tutorial on setting it up
- get everyone in the room to do a coinjoin ✌️

Prerequisites:

- Any recommended knowledge needed?
- Any general knowledege about running a BTC/LN node is helpful
- Any setup of an environment / software downloaded?
- git
- java
- sbt
- Is access to BTC or LN node needed?
- yes, both

- Anything else?

- testnet or signet funds