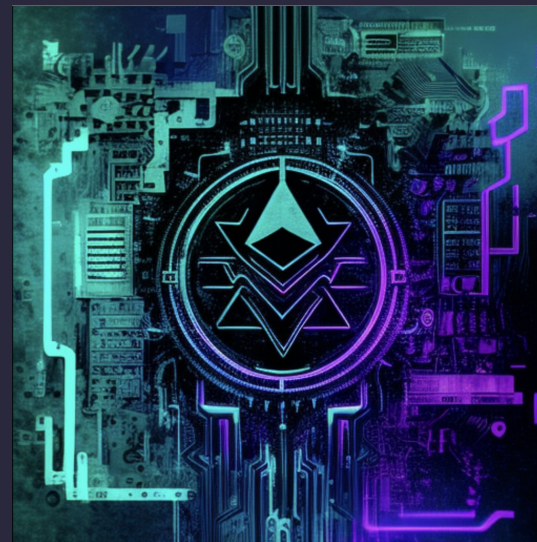




Personal notes on things happening on Devconnect 2023

Martinet Lee



Devconnect

- A decentralized conferences

ETHSTAKER'S STAKING GATHERING 10:00 - 18:00 EVERY DAY ETHSTAKER 👤 300-350 ALL ARE WELCOME! TALKS & PRESENTATIONS DISCUSSIONS LEARN MORE -- TICKETS AVAILABLE NOW!	AUTONOMOUS WORLDS ASSEMBLY 09:00 - 18:00 EVERY DAY OXPARC 👤 500 WORKSHOP TALKS & PRESENTATIONS DISCUSSIONS LEARN MORE -- APPLICATION OPEN NOW!	ETHGLOBAL ISTANBUL HACKATHON 13:00 - 23:59 DAY 1 00:00 - 23:59 DAY 2 ETHGLOBAL 👤 1,500 ALL ARE WELCOME! HACKATHON WORKSHOP EVENING EVENT TALKS & PRESENTATIONS DISCUSSIONS LEARN MORE --			
TRUSTX ALL DAY SECUREJUM 👤 256+ INTERMEDIATE TALKS & PRESENTATIONS LEARN MORE -- SOLD OUT	ETHCONOMICS 1:00 -- 6:00 PM ROBUST INCENTIVES GROUP 👤 100 INTERMEDIATE VIDEO TALKS & PRESENTATIONS DISCUSSIONS LEARN MORE -- APPLICATION OPEN NOW!	PROGRAMMABLE CRYPTOGRAPHY CONFERENCE (PROGCRYPTO) 09:00 - 18:00 EVERY DAY OXPARC, PRIVACY & SCALING EXPLORATIONS 👤 1000 ALL ARE WELCOME! TALKS & PRESENTATIONS WORKSHOP DISCUSSIONS LEARN MORE -- TICKETS AVAILABLE NOW!	CENSORSHIP.WTF 10:00 - 18:00 T&T 👤 300-500 INTERMEDIATE TALKS & PRESENTATIONS LEARN MORE -- APPLICATION OPEN NOW!		
ETHGÜNÜ (ETH DAY) 9:30 - 18:00 TÜRKİYE ETHEREUM COMMUNITY 👤 2000 ALL ARE WELCOME! VIDEO TALKS & PRESENTATIONS LEARN MORE -- TICKETS AVAILABLE NOW!	L2DAYS ISTANBUL 10:00 - 18:00 EVERY DAY L2BEAT, SCROLL 👤 2000 ALL ARE WELCOME! TALKS & PRESENTATIONS LEARN MORE -- TICKETS AVAILABLE NOW!	D1CONF - DECENTRALISED INSURANCE CONFERENCE 08:30 - 18:00 ETHERISC / CHAINPROOF / QUANTSTAMP 👤 120 ALL ARE WELCOME! TALKS & PRESENTATIONS DISCUSSIONS LEARN MORE -- TICKETS AVAILABLE NOW!	THE DAOIST'S GLOBAL GOVERNANCE GATHERING 10:00 - 19:00 EVERY DAY THE DAOIST 👤 400 ALL ARE WELCOME! WORKSHOP TALKS & PRESENTATIONS DISCUSSIONS SOCIAL EVENT LEARN MORE --		
FORMAL VERIFICATION HANGOUT 2 9:30 -- 18:00 FV TEAM + FRIENDS 👤 100 INTERMEDIATE DISCUSSIONS	NOTDEVCON BY ITU BLOCKCHAIN 09:00 - 19:00 ITU BLOCKCHAIN 👤 1500 ALL ARE WELCOME! WORKSHOP TALKS & PRESENTATIONS DISCUSSIONS SOCIAL EVENT	GOOD INTENT-IONS: THE FIRST INTENT-CENTRIC CONFERENCE 9:00AM - 6:00PM GOOD INTENT-IONS 👤 200 ALL ARE WELCOME! TALKS & PRESENTATIONS DISCUSSIONS SOCIAL EVENT WORKSHOP	SCHELLING POINT SESSIONS 10:00-18:00 GITCOIN 👤 120 ALL ARE WELCOME! TALKS & PRESENTATIONS DISCUSSIONS	WALLET UNCONFERENCE 09:00 - 19:00 WALLETUNCON TEAM 👤 150 ADVANCED DISCUSSIONS	LIGHT CLIENT SUMMIT 10:00 - 16:00 LIGHT CLIENT WORKING GROUP 👤 50 INTERMEDIATE VIDEO TALKS & PRESENTATIONS

Notable larger events

- ProgCrypto
- L2Days
- TrustX - Security
- D1Conf
- ETHGlobal Pragma
- EVM Summit
- Solidity Summit

Main themes

- L2s
- ZK
- AA/Intent
- Security
- Autonomous World

Main themes

- L2s
 - Secure Development on L2s
 - Data Availability
 - State growth
 - Security models of L2s
 - Rollup on Bitcoin
 - MEV
- ZK
 - Techniques for lowering costs
 - Acceleration
 - Security

Main themes

- AA/Intent
 - Wallet / UX
 - MEV
- Security
 - Tooling
- Autonomous World - on-chain gaming
 - ??????

L2s - Gotcha Development on L2s

- EVM Opcode behaviour inconsistencies
 - Origin, Caller (How is it defined?)
 - Number, Timestamp (L1 or L2?)
 - Blockhash (L1 or L2?)
 - Push0
- TL;DR: Everyone is doing things differently

L2s - Data Availability

- DA Solution - Cost is an issue
 - Celo is going to use EigenDA
 - Data Availability Sampling
 - ZK rollups talking about compression
- State explodes

Bandwidth

	Proto-Danksharding	Danksharding	EigenDA
Target Bandwidth	32KB/s	1.3 MB/s	3-10MB/s
Network Topology	P2P	P2P	Direct connections
Publishing Duration	14 days*	14 days*	14 days

*"Blob Archive" nodes may store longer



DAS is the only secure & scalable DA solution

	Solution	Security	Scalability
✗	Full node		
✗	No DA		
✗	DAC		
✗	Cryptoeconomic DAC		
✓	DAS no reconstruction		
✓	DAS with reconstruction		
✓	Anonymous DAS		

L2s - Security Models

- Censorship Resistant
 - Forced Inclusion
 - Forced Exit
 - Upgrades

Summary - production L2 censorship resistance mechanisms

Project	Practical* forced exits	Fraud or validity proofs	"Safe" upgrades
Arbitrum	✓	✓	✗
Optimism	✗	✗	✗
zkSync	✗	✓	✗
Starknet	✗	✓	✗
Scroll	✗	✓	✗
Polygon zkEVM	✗	✓	✗
dYdX	✓	✓	✗
Fuel v1	✓	✓	✓

*practical in this case means I personally think you could use them if you tried hard enough, while only using publicly available documentation, tools, and no special support from the team. Prove me wrong!

L2s - Blockchain Monitoring

- Phylax talk - Blockchain Monitoring is MEV
- Zircuit Launch - Security at the Sequencer Level

Defense in Depth

- While developing Dapp, all of these improves your security stance.
- If one layer fails, then other layers can mitigate the issues.



Security - Tools Development

- Certik - LLM for auditing
 - 30% accuracy on function based
- EVM Radar
 - Database of function bytecode on every contract
 - Idea: scan vulnerabilities with Database
- Slither now supports vyper
- ToB - RoundMe: checking division and rounding issues

Security - Auditing

- Methodology
 - ZK bugs / how to audit circuits
 - Web2 stack in the Web3 space
- Assessments
 - Severity of bugs
 - Audit Quality assessments between firms
 - Centralization - value controlled by a group of users

ZK

- Security
 - zkEVM exploits
 - ZK Security Research
- RLN
- Tools for Devs
 - Open source Library
 - Framework for building zkVM
- Applications
 - DID (Taiwan!)
 - Voting
 - ZuPass

AA - Cryptography on top of AA

- MPC
 - Pros
 - Off-chain recovery
 - Truly Cross-chain (can support Bitcoin)
 - No gas overhead
 - No modification needed from Dapps
 - Cons
 - No mature library (cutting edge research)
 - Immutable authentication rules, no timelocks, limited to Multisig
 - Currently incompatible with Trezor/Ledger

AA - Cryptography on top of AA

- MPC
 - Forget password functionality - reshare operation
 - Anomalous behaviour blocking / censorship (not signing)
 - Cannot: reimburse gas, complex logic on fund logic, ..
- AA
 - Key management costs on-chain txs.
- MPC + AA
 - Off-chain key recovery / change
 - On-chain fund logic management

AA - Cryptography on top of AA

- Schnorr
- Unclear: what happens if a key is lost?

	Schnorr + AA	MPC + AA	MPC	AA
multi-sigs	✓	✓	✓	✓
Gas abstraction	✓	✓		✓
No fancy math/setup	✓			✓
Can rotate keys	✓	✓		✓
Truly cross-chain (eg BTC)			✓	
Cheap (gas)	✓ *	✓ *	✓ ✓ (zero overhead)	
Private	✓	✓	✓	
Txn batching	✓	✓		✓

Schnorrkel.js: Schnorr signatures for Ethereum

- <https://github.com/borislav-itskov/schnorrkel.js/>
- TypeScript library to produce MuSig2 Schnorr multi-signatures
- Arbitrarily aggregatable public keys; you can pre-calculate the "address" of any combination of signers
- Cheap verification: 3k gas! Thanks to ecrecover() magic
- Integrated with Ambire contracts, Safe contracts WIP
- Rust port is WIP



Problems with MPC wallets, solved by Schnorr

- ✓ No bleeding edge cryptography required, Schnorr signatures are very established
- ✓ More key rotation options, but generally not required cause it's combined with AA
- ✗ Cannot be used currently with Trezor/Ledger until they implement it

Intent

- CowSwap - Defi Trading App
- Brink - Intent Infrastructure protocol
- Essential - Intent Infrastructure
- Squid Router - Defi Trading App, crosschain, on Axelar
- Enso - Unified Defi API, crosschain defi
- Uniswap - Defi Trading App
- Blocto - Wallet
- Propeller Heads - MEV minimizing infrastructure
- Tokka Labs - Market Maker
- Anoma - Generic Intent protocol

Intent

Follow-up research:

(1) Compare the “intent infrastructure protocol” Brink, Essential, and Anoma.

(2) Compare Cross-chain Defi focused

MEV

- MEV-burn
 - Validators being over compensated by MEV atm
 - How to distribute MEV to base protocol Ethereum?

UTXO based smart contract systems

- PLASSSSMMMAAA IS BACK BABY
- Fuel
- Aleo / Mina iirc



Taiwanese@Devconnect!

Zircuit Launch

- Research: Security at the Sequencer Level
- Current status of monitoring / incident response
- The two bets & the one new design area
 - Technology
 - Social norm

<https://twitter.com/ZircuitL2>

Defense in Depth

- While developing Dapp, all of these improves your security stance.
- If one layer fails, then other layers can mitigate the issues.



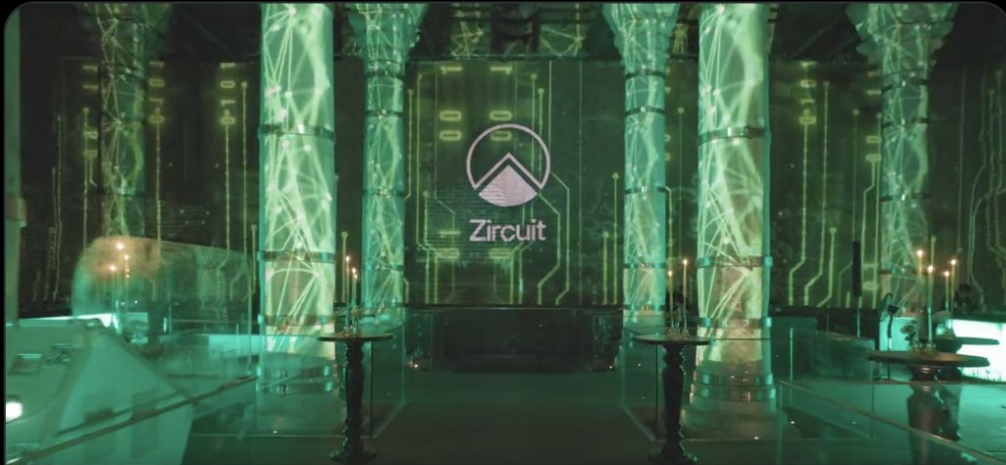
Zircuit Launch



Zircuit 🟡 @ZircuitL2 · Nov 16

Celebrating our testnet launch at the Cistern of Theodosius from the depths of Istanbul 🌐 ✨

Just the start of our journey into the uncharted...more to come 🔑 🐱





/THAT'S A WRAP!  (mic drop)



CREDITS: This presentation template was created by **Slidesgo**, and includes icons by **Flaticon**, and infographics & images by **Freepik**

