# An Intro to Alephium

**Cheng Wang**

@ EPFL Meetup

# About Me

- **Research @ *EPFL***
  Proposed the first linear-time asynchronous Byzantine agreement algorithm in 2015.

  State-of-the-art time complexity. Message complexity improved by others.

- **Engineering**
  Passionate about building practical systems to solve real-world problems.

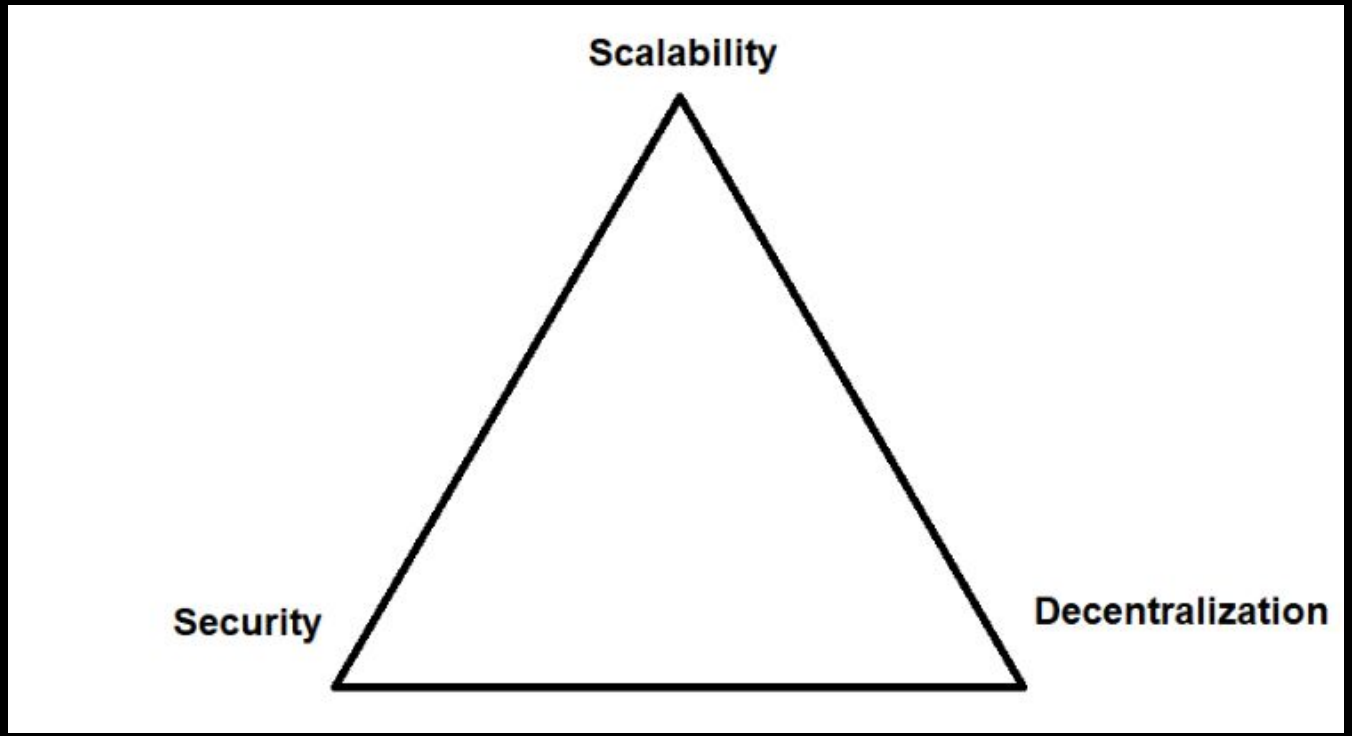
- **Alephium (2018 - now)**
  A platform to apply cutting-edge R&D.

# Why Alephium?

# Why Blockchain?

- Decentralization: no centralized entity for transaction
- Security: consensus algo + cryptography
- Openness, Transparency, Efficiency, Ownership, Privacy etc.

# Blockchain is hard



# Current Status

Bitcoin is rock solid

# Ethereum + Layer 2

**Gwart**
@GwartyGwart

Base is incredible. Most centralized l2. Least details about their plans to decentralize. Keeps OP cabal quiet by pretending to care about quadratic voting and giving 10% tithe. Pays Ethereum mainnet virtually nothing. Runs yuppie granola ad campaigns “come get some nitro cold brew in Williamsburg for $1 if you pay with usdc” and “mint a beautiful NFT of this coke bottle for onchain summer” doesn’t make sense, still have the most TVL. Pissed off miladies, didn’t matter. Pissed off racer, didn’t matter. Main guy comes announces they’ll do a giga gas or peta gas or whatever, doesn’t matter it’s on a single server. Now pushing USDC for gas payments. Honestly really savvy all around game see game Base, never decentralize, it clearly doesnt need that

11:15 pm · 16 Oct 2024 · **156.8K** Views

Andre Cronje
@AndreCronjeTech

Why L2s as appchains are not logical for builders:

- Barely any infra when deploying (stable coins, oracles, institutional custody, etc)
- No foundation/labs to help support
- Centralised and open to attack
- Fragmenting liquidity and forcing it onto bridges
- No community of users or builders
- Time spent on dealing with the above instead of application and users
- Kills network effects
- Still a long TTF (some providers wont work with you)
- Building alone (no frens)

Appchains also grossly underestimate the cost of infra and compliance (explorers, custody, exchanges, oracles, bridges, toolkits, IDEs, on/off ramps, native issuance&integration, regulatory, compliance). 2024 alone this has already cost us $14m, and a large part are recurring costs.

# Solana, Sui, etc...

## Hardware Recommendations

The hardware recommendations below are provided as a guide. Operators are encouraged to do their own performance testing.

- CPU
  - 12 cores / 24 threads, or more
  - 2.8GHz base clock speed, or faster
  - SHA extensions instruction support
    - AMD Gen 3 or newer
    - Intel Ice Lake or newer
  - AVX2 instruction support (to use official release binaries, self-compile otherwise)
  - Support for AVX512f is helpful
- RAM
  - 256GB or more
  - Error Correction Code (ECC) memory is suggested
  - Motherboard with 512GB capacity suggested

**vitalik.eth**
@VitalikButerin

If an "L1 founder" blurts out a "north star" that contains words like "chain go fast" without containing any words like "robust", "censorship-resistant", "decentralized", they're kinda revealing their own priorities right then and there?

1:54 AM · Oct 15, 2024 · **240.4K** Views

# PoS is trending, but

- PoW is way more simpler and battle-tested
- PoW scales better as there is no need to manage validators
- PoW’s token distribution is more permissionless
- PoW supports multiple concurrent proposers by default

# Summary

- Bitcoin is the most robust crypto network (IMO)
- Ethereum’s scaling solution values decentralization, but has issues
- Many chains focus on speed over decentralization/security

# What is Alephium?

- Scale blockchain following Bitcoin’s philosophy
- Leverage Bitcoin’s tech stack: PoW + UTxO
- Bring programmability to Bitcoin’s tech

# Scalability

# BlockFlow Sharding

- **Based on Bitcoin's core tech stack: PoW + UTXO**
- **An elegant and complete sharding algorithm**
  - **No master chain needed** to coordinate all shards
  - **Single-step** cross-shard transactions
  - **DAG-based** fork-choice rule for consensus
- **Implementation: practical and deliverable**

https://github.com/alephium/research/blob/master/alephium.pdf

# Programmability

# Year of DeFi (2019)

- **Increased Popularity**
  MakerDao, Uniswap, Compound
- **New DeFi projects**
  Lending, borrowing, DEX, NFT
- **Growth**
  Significant rise in Total Value Locked (TVL)

# Challenges of DeFi

## Security risks

Smart contract vulnerabilities

Hacks and exploits

## Scalability

High TX fees

Transaction execution

State bloating

## User experience

Complexity

Usability

# Stateful UTxO Model

- **Hybrid approach: Combine UTXO model with Account model**

  Assets managed in UTXO model for better security
  Contract states managed like Account model for programmability

  Tokens are first class citizens

- **Transactions: Follow the input/output model of UTXO**

  No reentrancy attacks or flash loans

- **No concurrency issue due to mutable contract states**

# Alphred VM

A brand new VM built for stateful UTXO model

- Efficient and secure transaction execution
  Less computation, less IO, less gas
- Compact bytecode format
  Bridge example: ~1KB vs. ~10KB (EVM), ~1MB (Solana)
- Asset permission system (APS)
- Storage renting mechanism
- Sub-contract system
- ...

# Ralph Programming Language (1)

- DSL: Domain specific language for building dApps on Alephium
- Simplicity: easy to learn, use, and audit
- Security: built-in checks for common pitfalls
  - Explicit annotations for mutability, asset usage, and external calls

    *@using(updateFields = true, preapprovedAssets = true, checkExternalCaller = false)*
  - Overflow checks enabled by default

# Ralph Programming Language (2)

Works seamlessly with Alphred VM

- Built-in functions for VM interaction: *transferToken!(...)*
- Brace syntax for APS: *foo{caller → tokenId: 100}(...)*
- Built-in support for secure contract creation and migration
  - *copyCreateContract!(...)*, *migrateWithFields!(...)*
- Efficient event system with minimal onchain footprint
  - *emit TokenSwapped(...)*

# DEX code

```
@using(preapprovedAssets = true, assetsInContract = true, checkExternalCaller = false)
pub fn swap(sender: Address, to: Address, amount0In: U256, amount1In: U256, amount0Out: U256, amount1Out: U256) -> () {
  assert!(amount0Out > 0 || amount1Out > 0, ErrorCodes.InsufficientOutputAmount)
  assert!(amount0Out < reserve0 && amount1Out < reserve1, ErrorCodes.InsufficientLiquidity)

  // fee: 0.003 * amountIn
  let newReserve0 = reserve0 + amount0In - amount0Out
  let newReserve1 = reserve1 + amount1In - amount1Out
  let newReserve0Adjusted = (newReserve0 * 1000) - (amount0In * 3)
  let newReserve1Adjusted = (newReserve1 * 1000) - (amount1In * 3)
  let kAdjusted = reserve0 * reserve1 * 1000_000
  assert!(newReserve0Adjusted * newReserve1Adjusted >= kAdjusted, ErrorCodes.InvalidK)

  transferTokenToSelf!(sender, token0Id, amount0In)
  transferTokenToSelf!(sender, token1Id, amount1In)
  transferTokenFromSelf!(to, token0Id, amount0Out)
  transferTokenFromSelf!(to, token1Id, amount1Out)

  update(newReserve0, newReserve1)
  emit Swap(sender, amount0In, amount1In, amount0Out, amount1Out, to)
}
```

# Start Building

We prioritize UX and DevX

- Tutorials
- dApp Templates
- Docs: docs.alephium.org
- Join the dev discord

# More than dApps

# Proof of Less Work (PoLW)

- Energy Efficiency: Reduce PoW's high energy consumption
- Retains PoW's advantages in the blockchain trilemma
- Shift part of the external electricity cost to internal network cost

https://github.com/alephium/research/blob/master/polw.pdf

# Progress

# Mainnet Launch (2021-11-8)

- Mature BlockFlow technology with 64 seconds block time
- Initial version of Alphred VM and Ralph language
- Simple Typescript SDK
- Desktop wallet release
- Reference pool implementation
- Successful bootstrapping of mining community
- ...

# Leman Upgrade (2023-03-27)

- Built bridge, DEX, NFT marketplace
- Subcontract system, Efficient contract storage, Dynamic array indexing
- Improved difficulty adjustment algorithm (DAA)
- External call check
- Generated TypeScript code for Ralph contracts
- Token standards, wallet abstractions
- Mobile wallet & Extension wallet
- ...

# Rhone upgrade (2024-06-12)

- Block time reduction to 16 seconds
- Map data structure in Ralph
- Multiple inheritance and dynamic method dispatching
- Sequential transactions
- Gasless transactions
- Better support for PoLW
- Typescript SDK 1.0.0
- Optimized full node
- ...

# Current Status

- **2nd TVL amongst PoW chains, after BTC**
  - Live bridge to Ethereum, more chains to come
  - DEX, NFT marketplace, Game & more
- **100+ builders in the 1st hackathon**
- **150K+ addresses** (+200% YTD)
- **50K+ native wallet downloads**
- **15+ CEX, ~25 pairs**
- **Hashrate surpassed 10PH/s** (+10000% YTD)

# Ecosystem

Dashboard: https://www.alph.land

- DeFi: Bridge, DEXes, NFT marketplaces
- Hardware wallets: Ledger, OneKey, and more
- Infra: Explorer, Oracle, ANS, etc.
- A few cool games
- More to come: DEX, Stablecoin, lending
- Highlight: Liquidity mining
- A strong community of supporters and devs

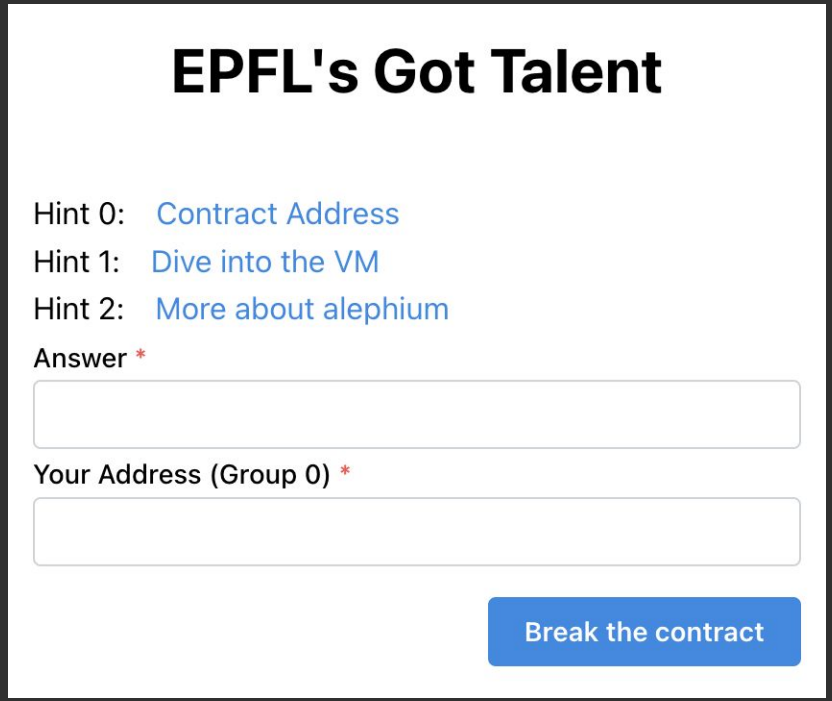
# A Small Puzzle

# Find the number

Puzzle: https://epfl-meetup.alephium.org

Wallet: https://alephium.org/#wallets

Reward: 100 $ALPH



Buidl Deliver