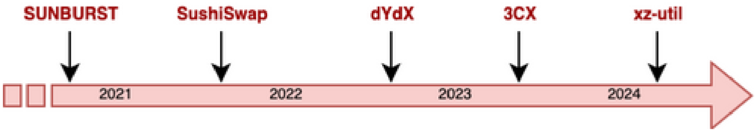
Strengthening the Go Ethereum Supply Chain by Build Integrity

Vivi Andersson <vivia@kth.se> Supervision: Javier Ron, Martin Monperrus

> Software supply chain attacks are a reality

- “2023 saw **twice as many** software supply chain attacks as 2019-2022 combined” [1]
- The xz-util attack showcases the sophistication of supply chain threats
  - Social engineering, obfuscation, manipulating sources, packages...

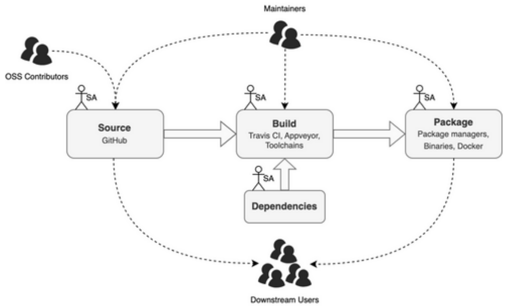
...and supply chains grow with code reuse, becoming increasingly complex to understand and manage



Software supply chain attacks over the years

> Go Ethereum is a high-value target

- Majority execution client for Ethereum
- Exploits can affect software operators and Ethereum Mainnet [2]
- Supply chain security of blockchain software remains relatively unexplored [3]



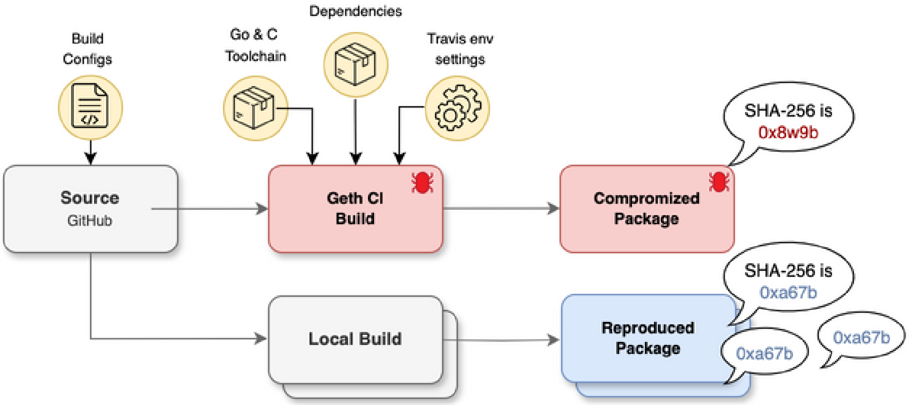
The Go Ethereum Supply Chain

> Build-based threats

- A lack build **transparency** produces opaque binaries which are challenging to validate
- Thus, compromised builds can be difficult to detect -- **how to ensure integrity in build processes?**

> Strengthening the Supply Chain: Reproducible Builds [4]

- Increased trust can be put in binary artifacts if there is a guarantee that the same source code always compiles to the same binary
- Independent builders compare cryptographic hashes of the output artifact
- Mitigates compromises that change the intended semantics of the sources



Reproducible builds increase trust in compiled artefacts by distributed consensus on valid checksums

> Contributions

- Go Ethereum software supply chain **audit**
- Increased **integrity** of software through reproducibility
- ...

[1] Sonatype. 9th Annual State of the Software Supply Chain. Tech. rep. Oct. 2023. [2] go-ethereum. Vulnerability disclosure. Aug. 2023.
[3] Soto-Valero, César, Monperrus, Martin, and Baudry, Benoit. “The Multibillion Dollar Software Supply Chain of Ethereum” IEEE C. (2022)
[4] Lamb, Chris and Zacchiroli, Stefano. “Reproducible Builds: Increasing the Integrity of Software Supply Chains”