Rust v Blockchaine

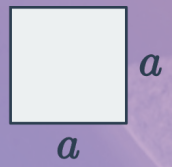
Programovanie v jazyku Rust

Dušan Morháč

Obsah prezentácie

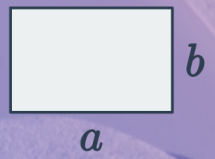
- Quiz 1 – Rust
- Čo je to Blockchain? (SPOILER – DMBLOCK)
- Rust v Blockchain developmente
- Quiz 2 – Rust a Blockchain
- Čo sú to Smart kontrakty? (SPOILER2 - DMBLOCK)
- Rust a Smart kontrakty
- Quiz 3 – Rust a Smart kontrakty
- Budúcnosť Rustu v Blockchaine a adopcia
- Q&A

štvorec



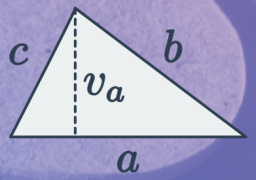
$S = a^2$

obdĺžnik



$S = a \cdot b$

trojuholník



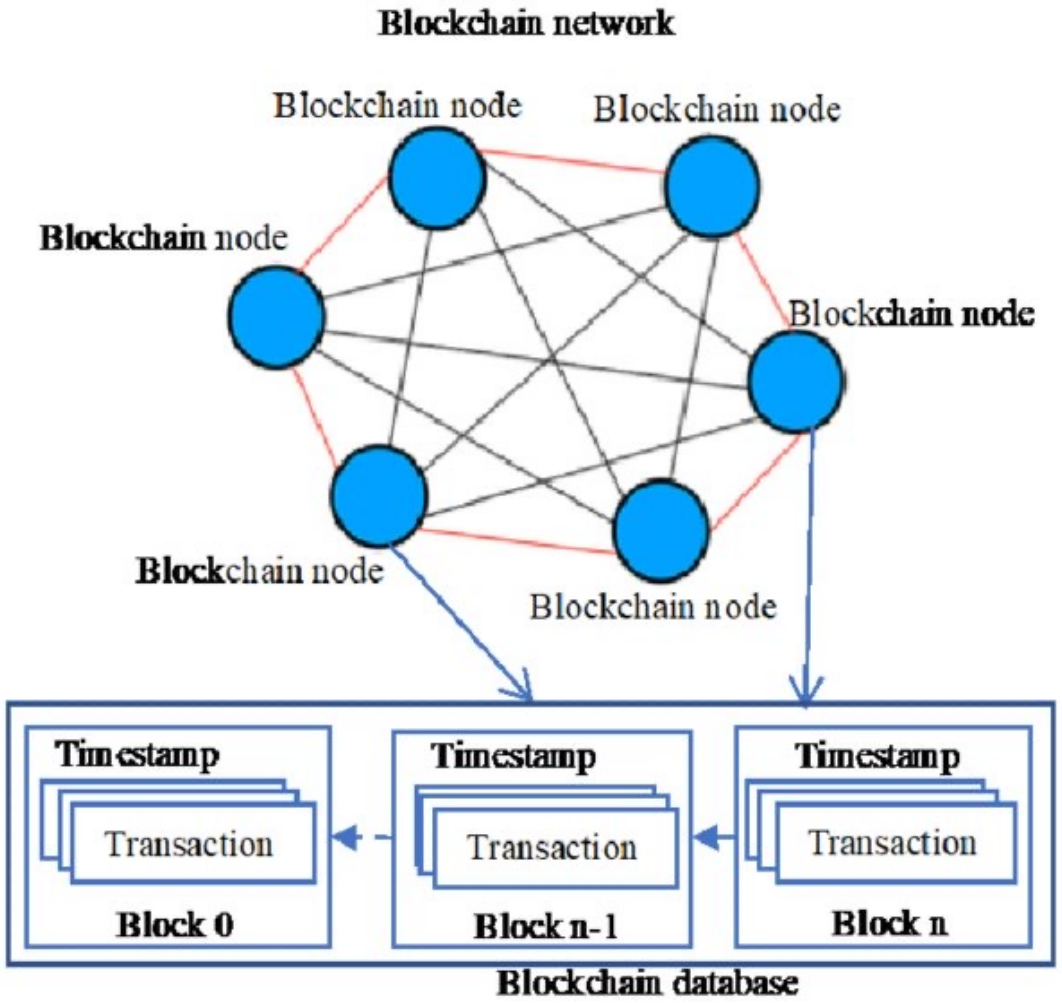
$S = \frac{1}{2}a \cdot v_a$

kruh

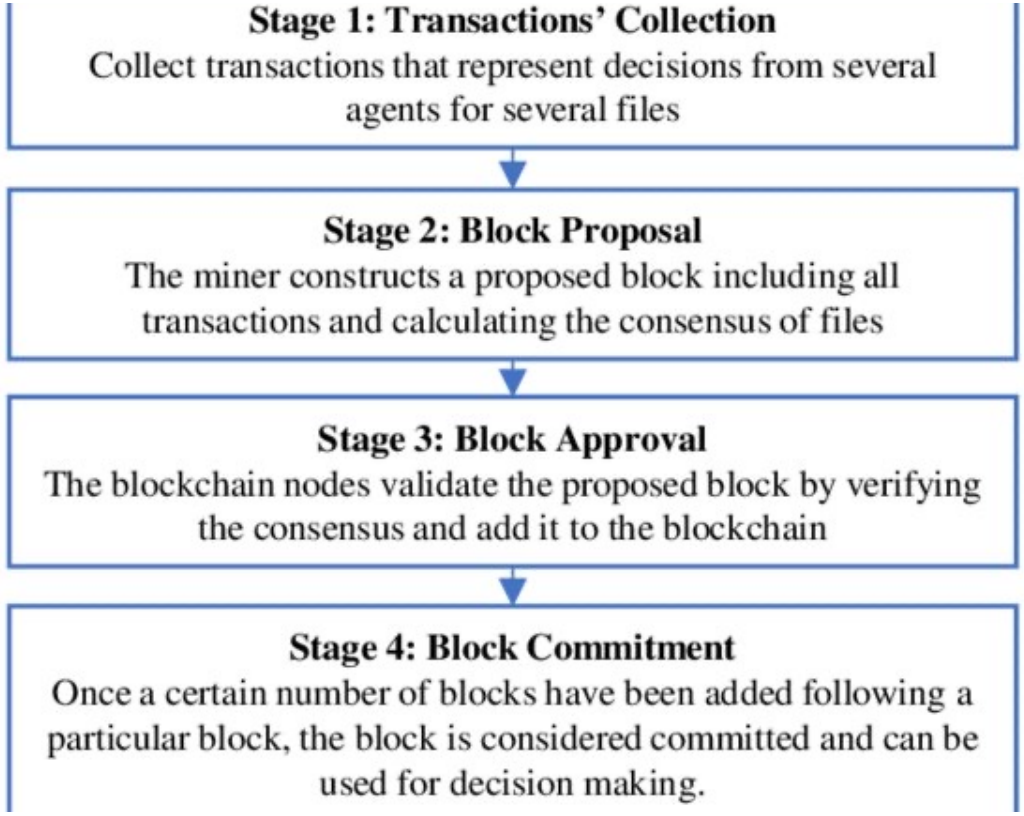
$S = \pi r^2$

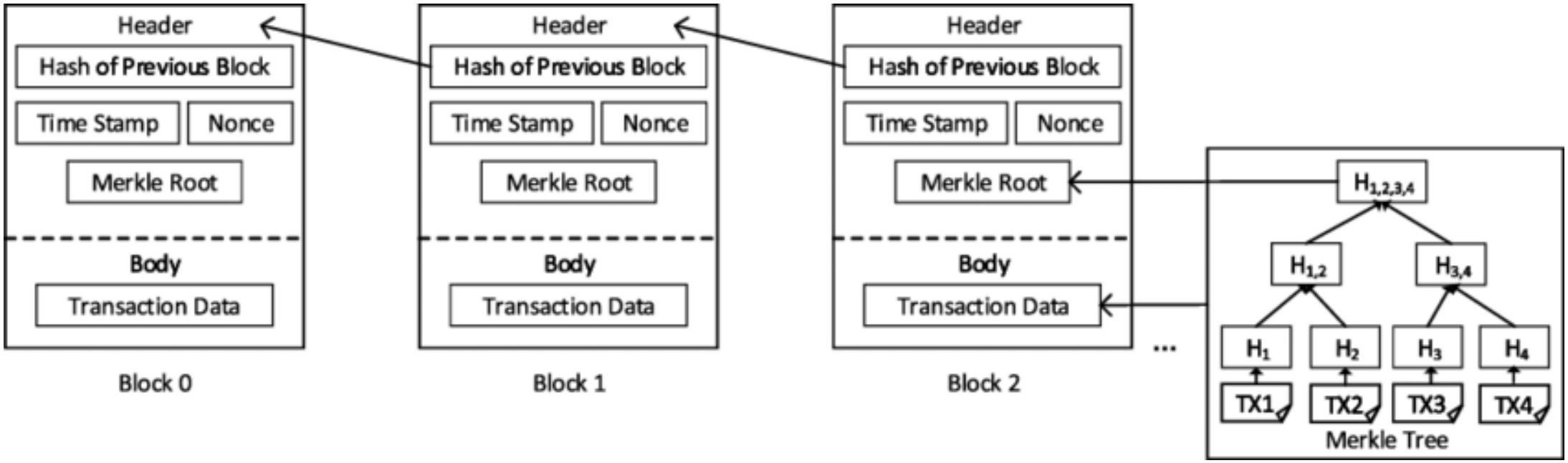

Quiz 1 - Rust

Čo je to Blockchain v skratke?



Čo sú to tie “Bloky?“

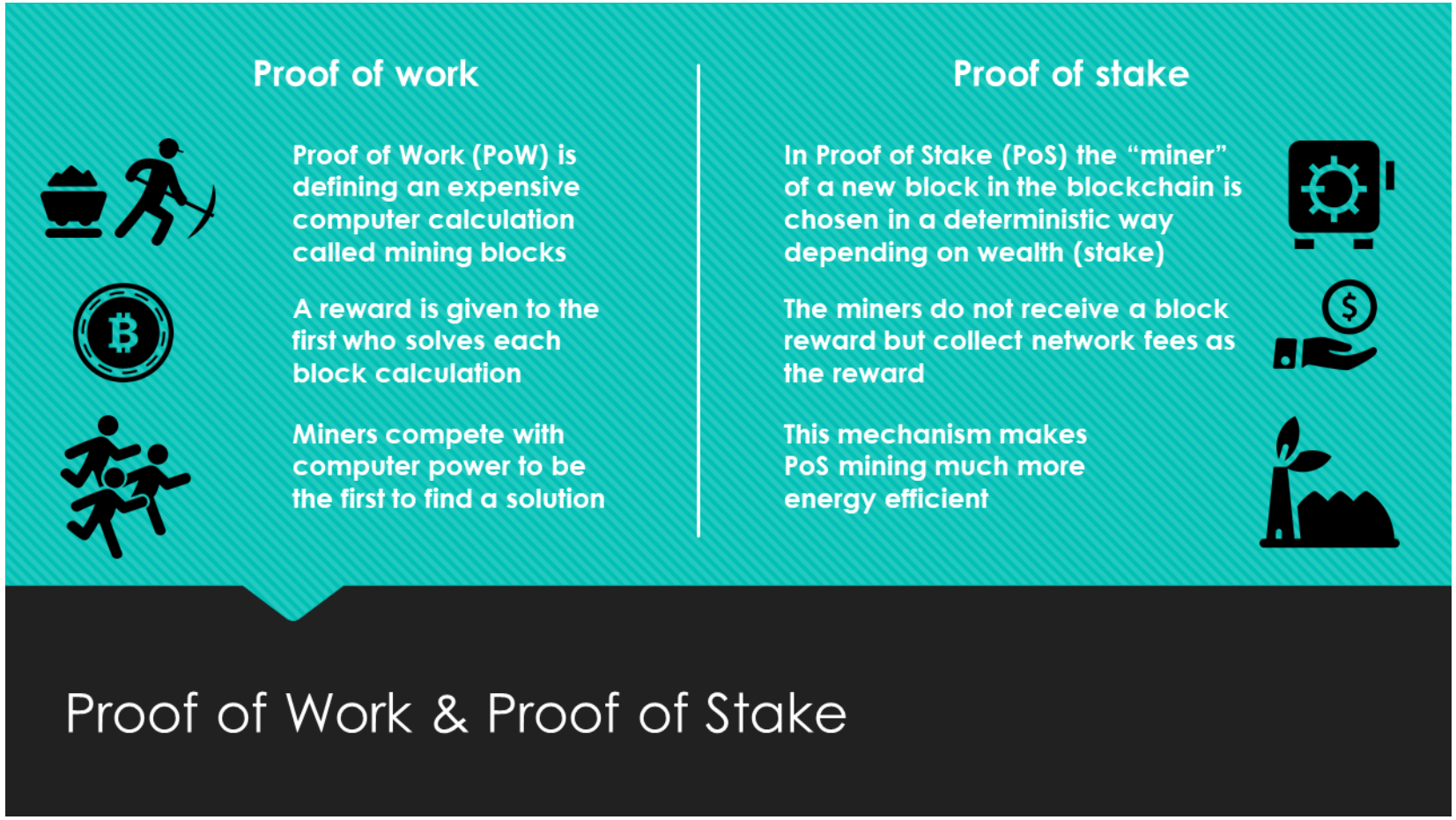




Ako sa blok pridá do siete?

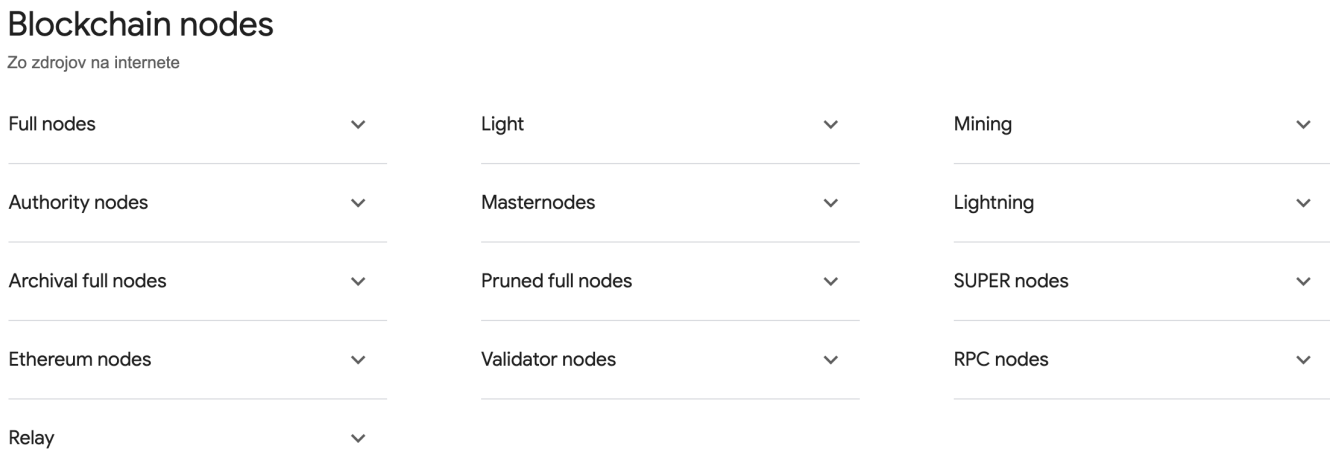
- POW
- POS
- NPOS

POW, POS, NPOS?


Proof of work
Proof of Work (PoW) is defining an expensive computer calculation called mining blocks
A reward is given to the first who solves each block calculation
Miners compete with computer power to be the first to find a solution
Proof of stake
In Proof of Stake (PoS) the "miner" of a new block in the blockchain is chosen in a deterministic way depending on wealth (stake)
The miners do not receive a block reward but collect network fees as the reward
This mechanism makes PoS mining much more energy efficient
Proof of Work & Proof of Stake

Čo sú „Nody?“

- Full nodes
- Light nodes
- Mining nodes
- Validator nodes
- RPC nodes



Rust v Blockchain developmente

WHY RUST ?

- Performant
- Safe (no undefined behaviour)
- Correct (well designed API)
- Extensible (dependencies, macros)

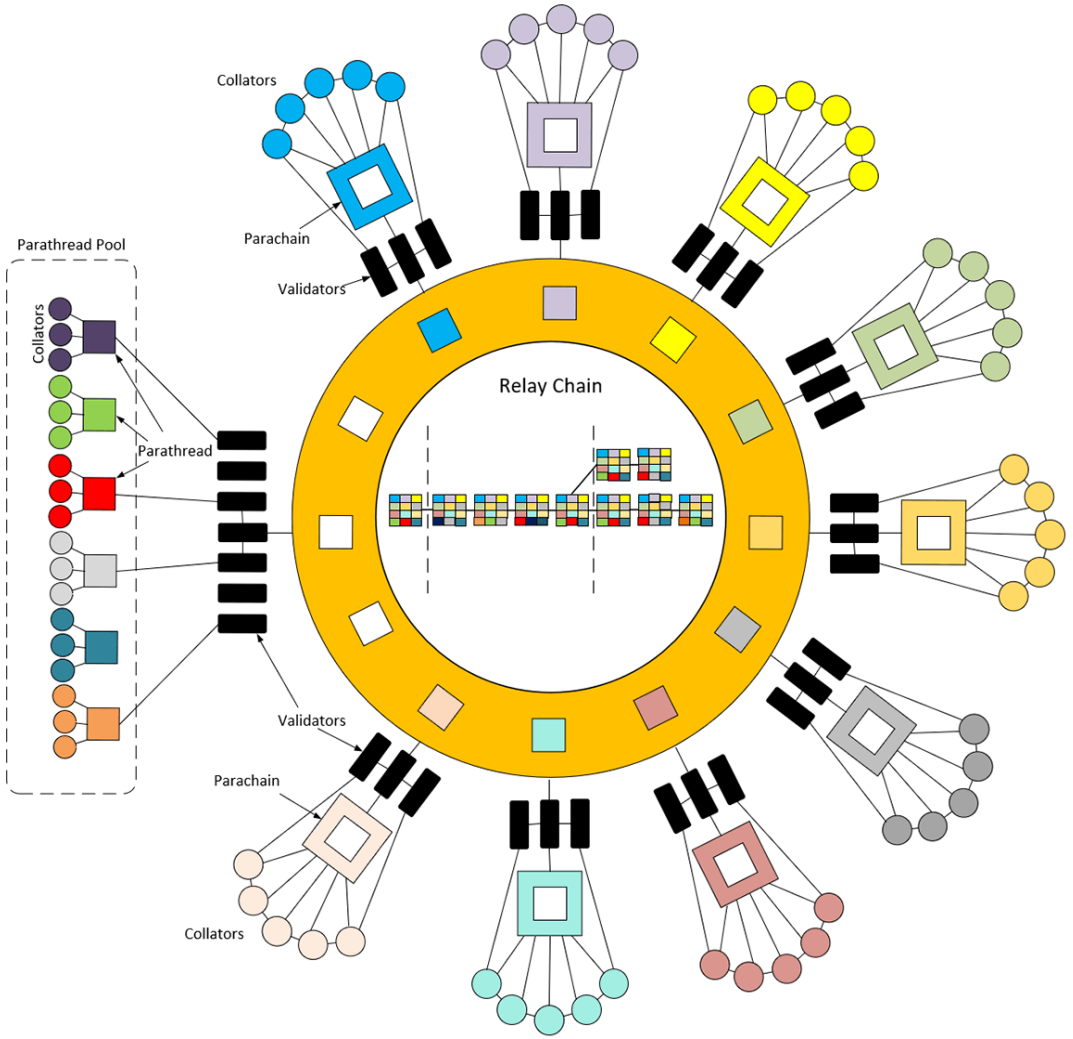
Blockchainy využívajúce Rust

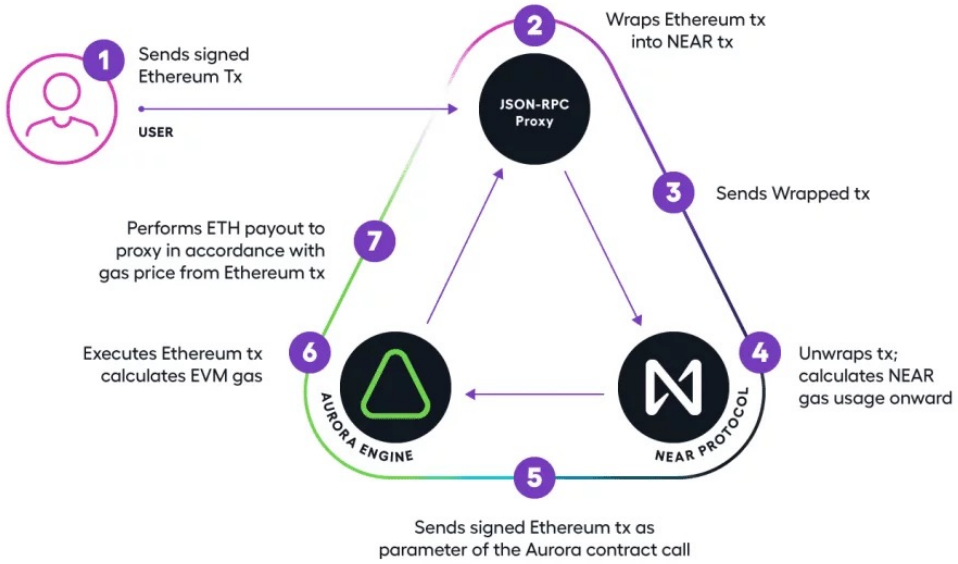
- Solana: Vysoko výkonná blockchain platforma s focusom na škálovatelnosť
- Polkadot: Decentralizovaný “Blockchain blockchainov“
- Elrond: Decentralizovaná oracle sieť.
- Near Protocol: Decentralizovaná platforma pre aplikácie

SOLANA

substrate_

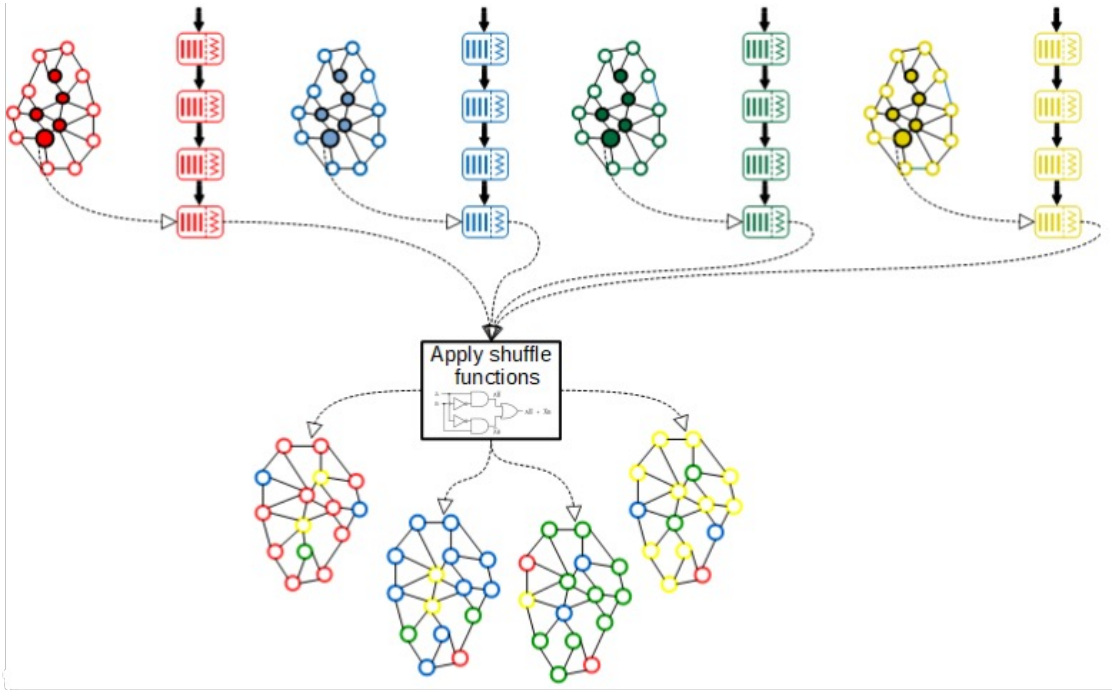
Polkadot




1
Sends signed
Ethereum Tx
USER
2
Wraps Ethereum tx
into NEAR tx
JSON-RPC
Proxy
3
Sends Wrapped tx
4
Unwraps tx;
calculates NEAR
gas usage onward
NEAR PROTOCOL
5
Sends signed Ethereum tx as
parameter of the Aurora contract call
AURORA ENGINE
6
Executes Ethereum tx
calculates EVM gas
7
Performs ETH payout to
proxy in accordance with
gas price from Ethereum tx

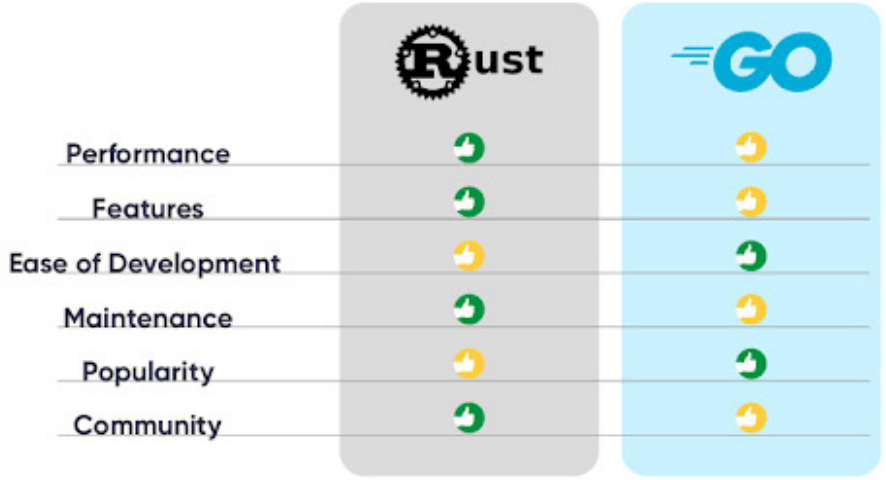
NEAR

elrond



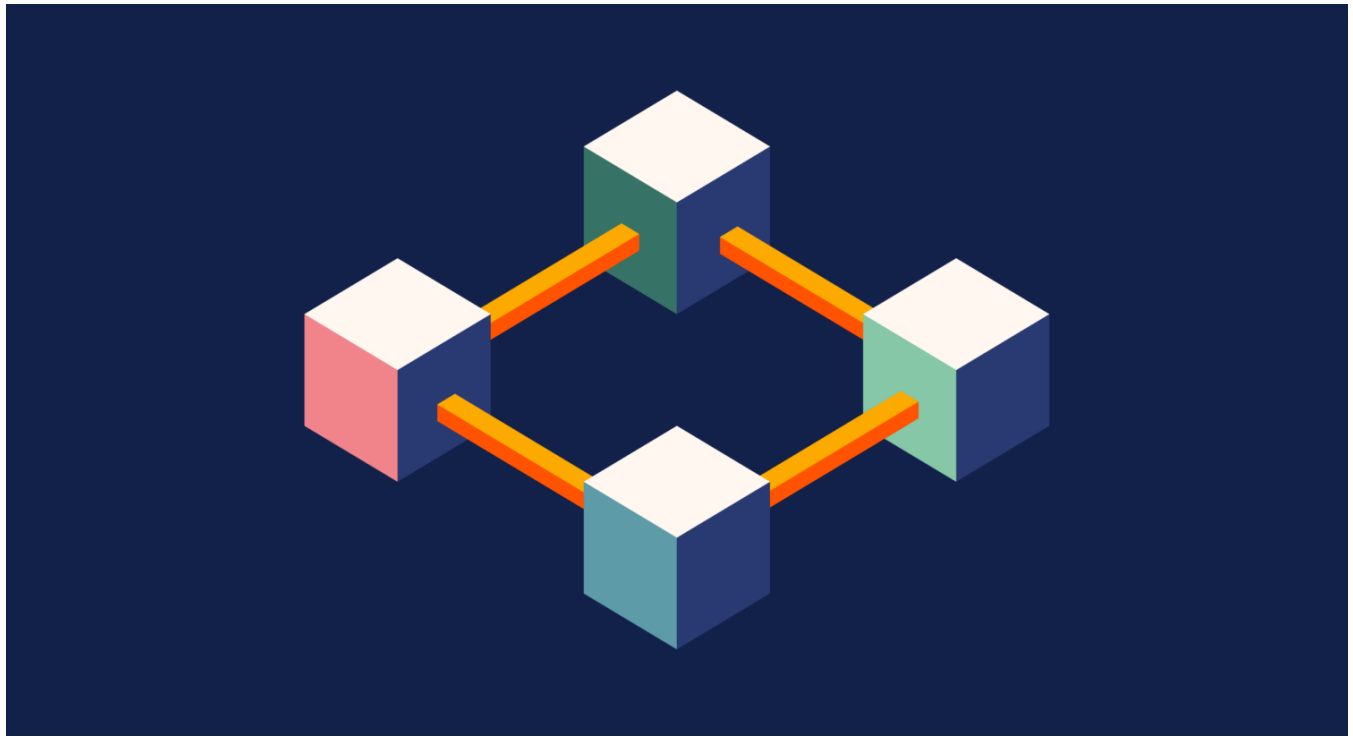
Rust vs GO v Blockchaine

- **Bezpečnosť**
- **Výkon**
- **Nástroje a ekosystém**
- **Komunita a podpora**
- **Zložitosť**



Tradičné vs Rust blockchainy

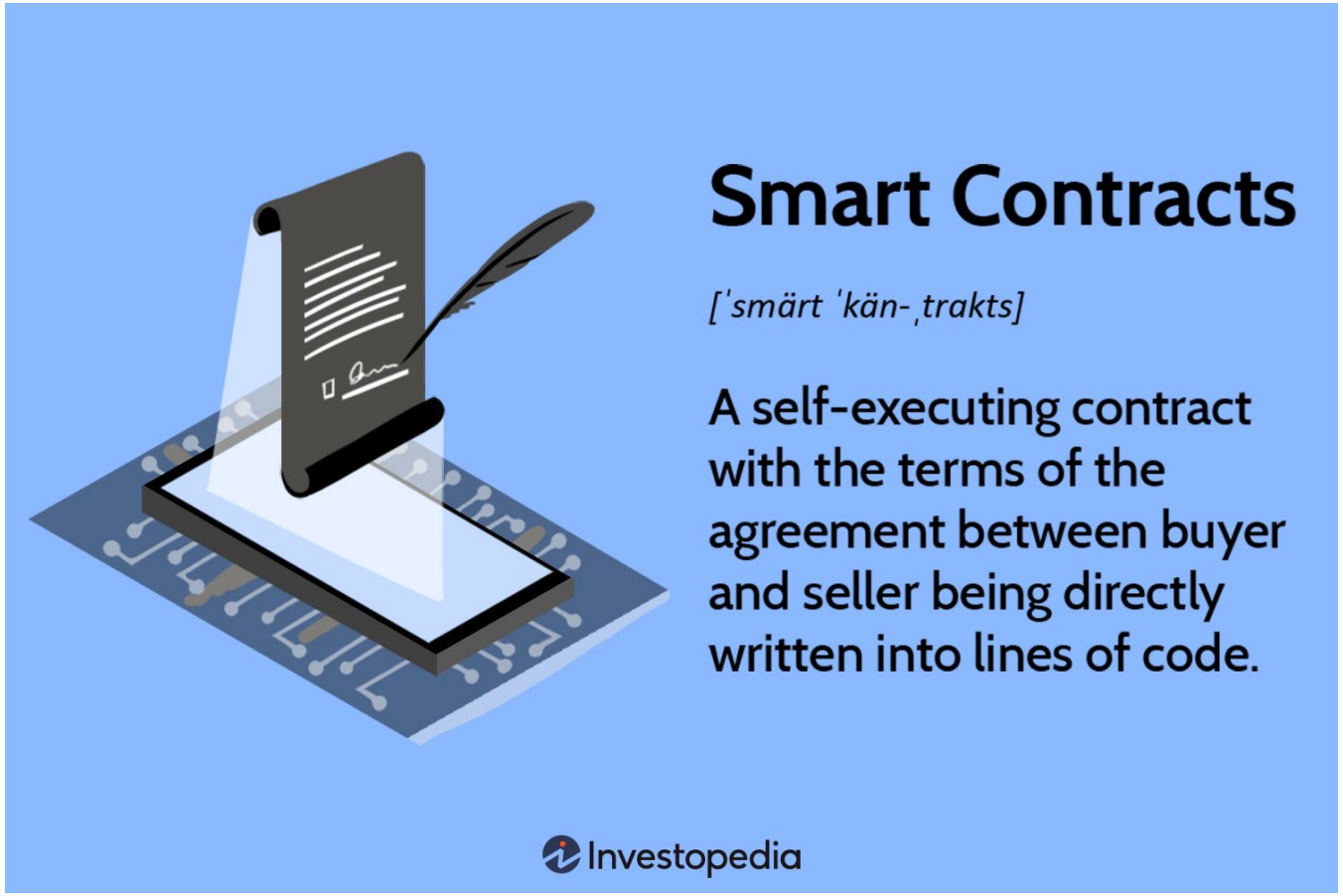
1. **Jazyk implementácie**
2. **Bezpečnosť a zraniteľnosti**
3. **Výkon**
4. **Flexibilita**
5. **Ekosystém a podpora**



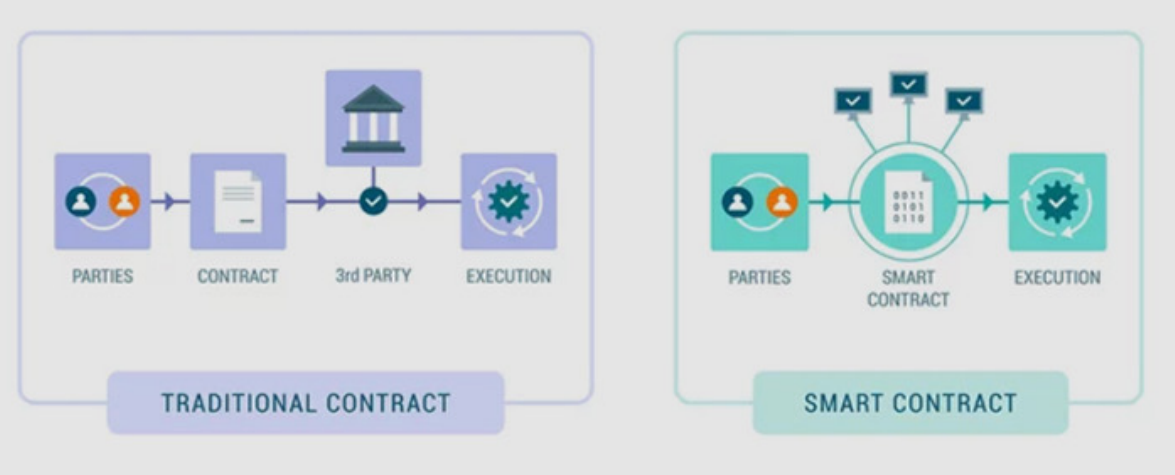
Quiz 2 – Rust a Blockchain

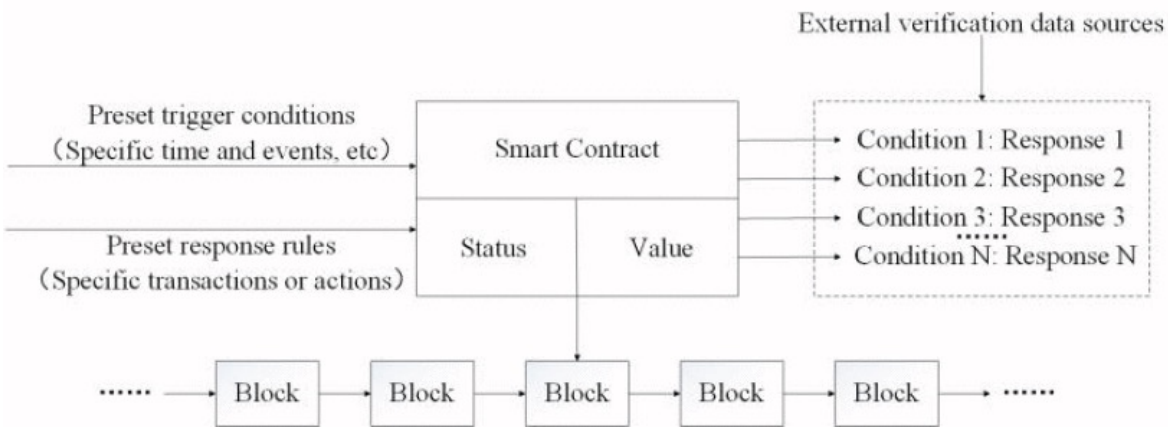
Čo sú to Smart kontrakty v skratke?

- Automatizované self executing programy
- Transparentné
- Programovateľné podmienky
- Bezpečné proti alteringu



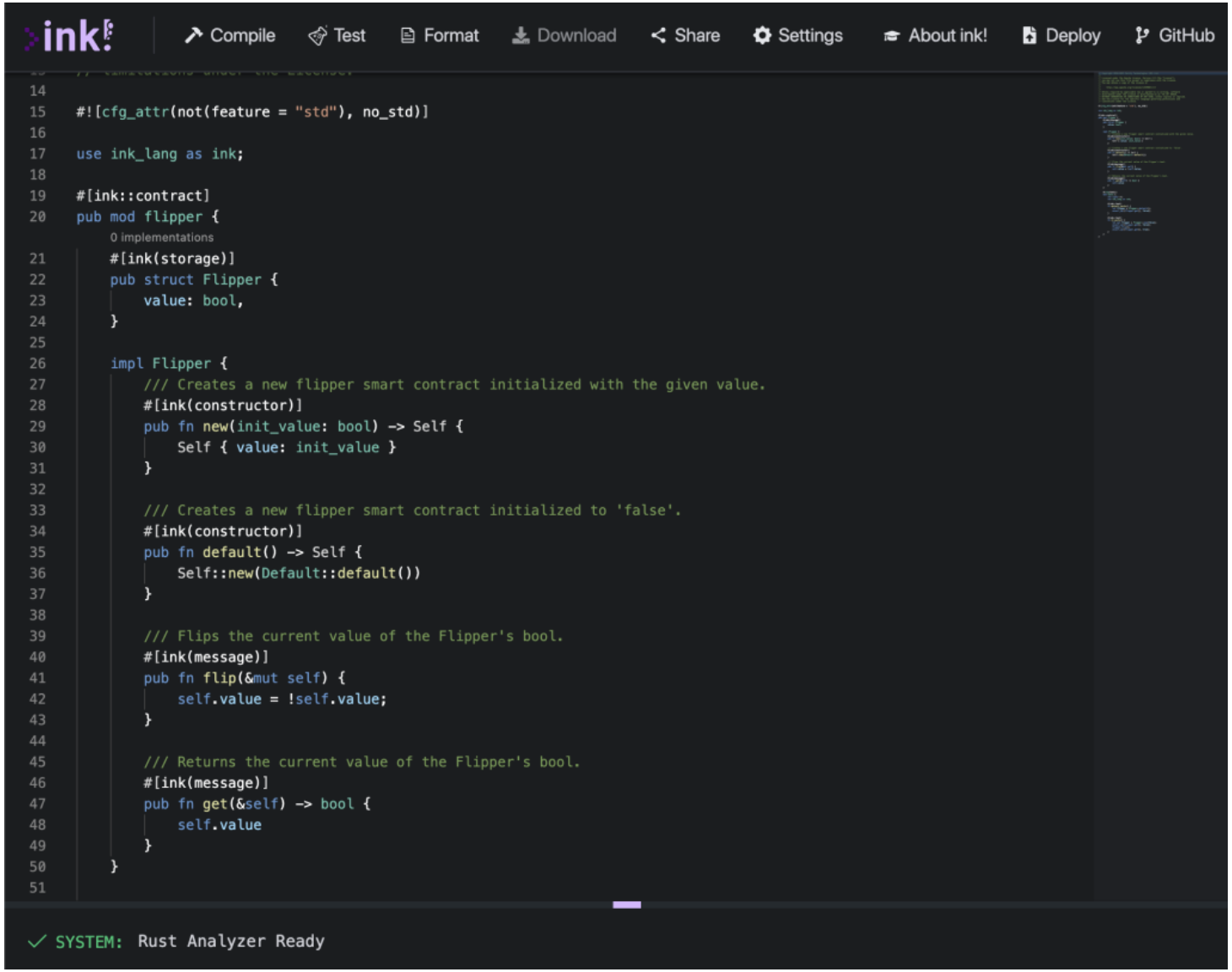
Ako smart kontrakty fungujú?





Smart kontrakty v Ruste

- Ink!
- Casper smart contracts



Rust smart kontrakty vs smart kontrakty v Solidity

Rust

PROS	CONS
Memory Safety: Uses a unique ownership model to manage memory automatically, preventing common security issues.	**Learning Curve**: The complexity of its features like ownership and borrowing can be challenging for beginners.
Performance: Known for its speed and efficiency, making it suitable for high-performance applications.	**Less Tailored for Blockchain**: While growing in blockchain, it's not as specialized for smart contracts as Solidity.
Reliability: Its emphasis on safety and performance makes it a strong choice for critical system-level applications.	**Compile Times**: For large projects, the compilation can be time-consuming due to its detailed and thorough process.

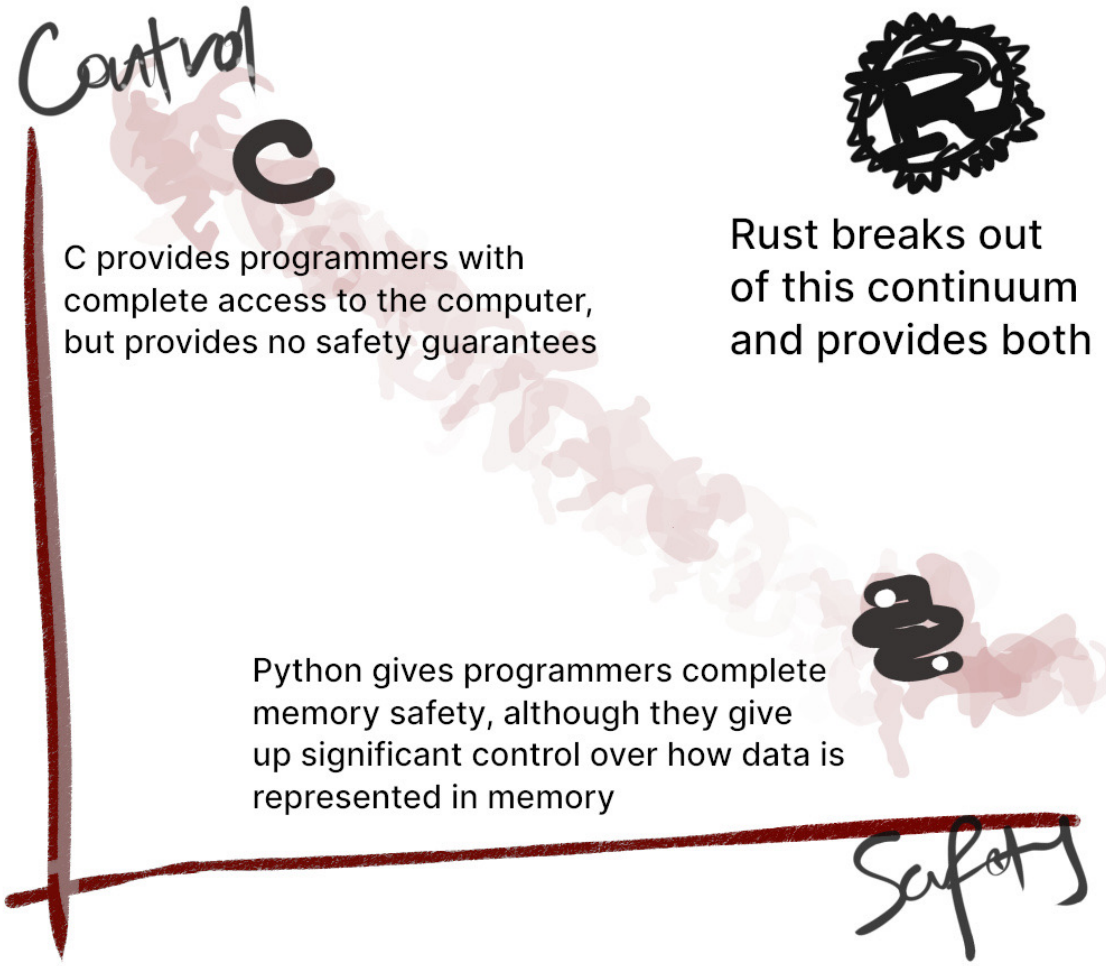
Solidity

PROS	CONS
Ease of Use: Familiar syntax for those with JavaScript experience, making it accessible to a wide range of developers.	**Security Concerns**: Historically, Solidity has had vulnerabilities, especially in earlier versions, which have led to notable smart contract breaches.
Large Community: Robust ecosystem with extensive learning resources, tools, and frameworks for Ethereum development.	**Limited to EVM**: Primarily focused on Ethereum, which may limit its application scope compared to more versatile languages.
Specialized for Smart Contracts: Optimized features and functionalities for developing and deploying smart contracts.	**Young Language**: Being a relatively newer language, it's still evolving, which sometimes leads to changes and inconsistency in use.

Quiz 3 Rust a smart kontrakty

Bezpečnosť blockchainov implementovaných v Ruste

- Bezpečný jazyk
- Ochrana proti zraniteľnostiam
- Paralelizmus
- Bezpečné kontrakty
- Auditovateľnosť



Developer experience v Blockchainoch implementovaných v Ruste

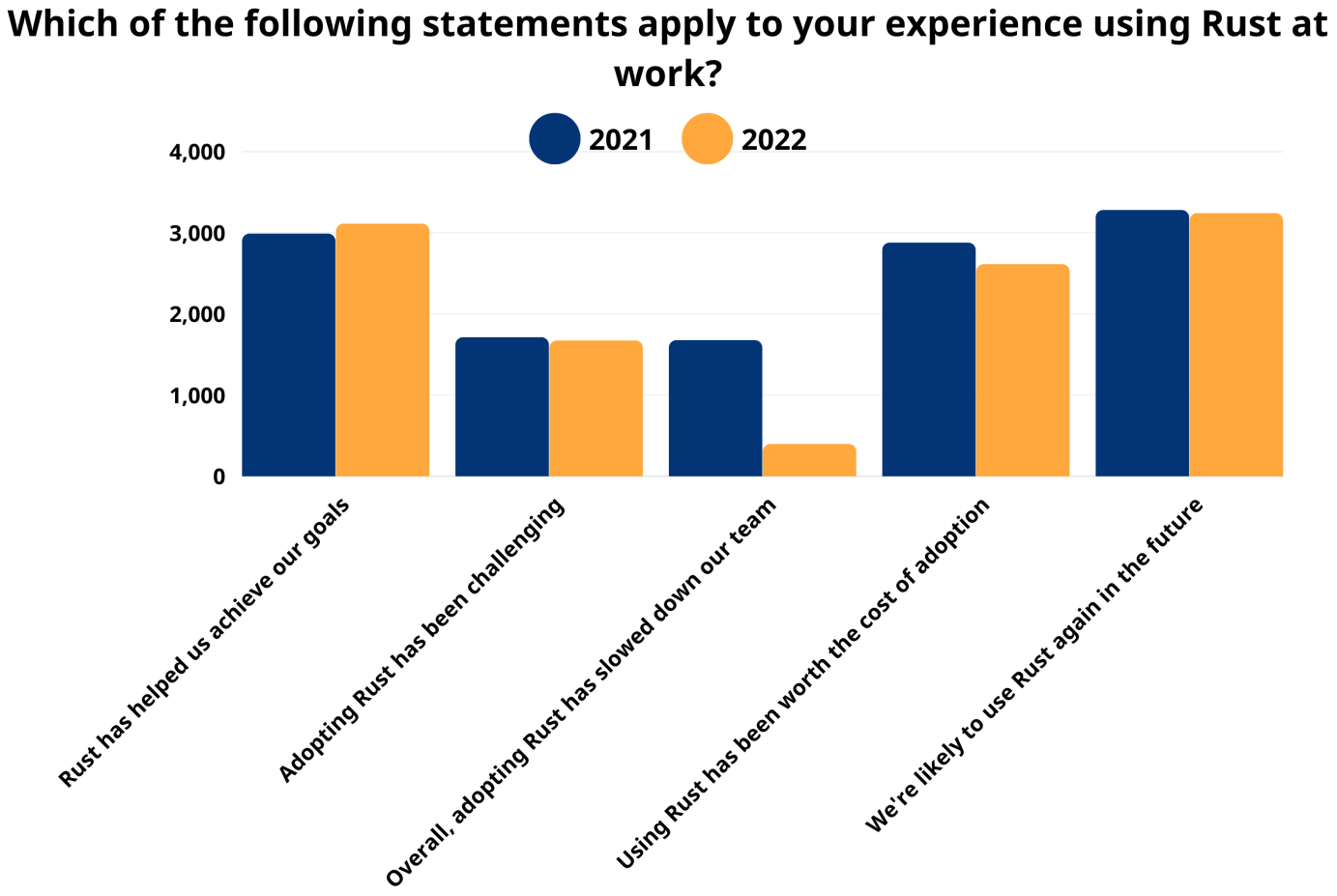
- **Silná dokumentácia**
- **Nástroje a knižnice**
- **Integrácia s IDE**
- **Vývojové prostredie a testovanie**
- **Podpora komunity**

Výzvy vo vývoji blockchainu založenom na Ruste

- **Špecializovaná znalosť**
- **Integrácia s existujúcimi blockchain platformami**
- **Optimalizácia výkonu**
- **Bezpečnosť**
- **Podpora a ekosystém**

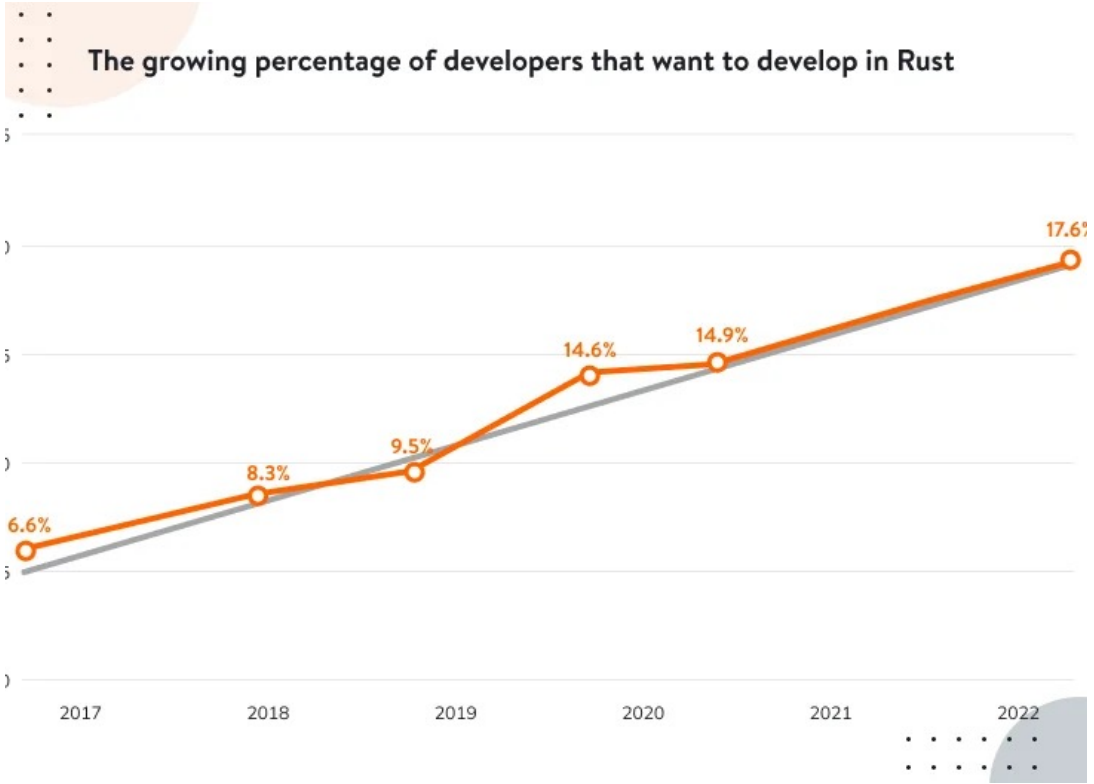
Budúcnosť Rust jazyka v Blockchaine

- **Zvyšujúca sa popularita**
- **Bezpečnosť**
- **Podpora od komunity**
- **Efektívny výkon**
- **Rozmanitosť použitia**



Trend adopcie Rustu v Blockchaine

- **Zvýšený záujem a prieskumy**
- **Začínajúce projekty**
- **Prispôsobenie existujúcich projektov**
- **Rastúca podpora a ekosystém**
- **Spolupráca a inovácie**



Summary

1. Rust je veľmi vhodný programovací jazyk na Blockchain
2. Ak chcete vedieť viac o Blockchaine a Smart kontraktoch – DMBLOCK (Spamujte Kika pre viac info)
3.

Zdroje

- https://medium.com/@AlexanderObregon/the-rise-of-rust-in-blockchain-development-eddbad0d9424
- https://www.sciencedirect.com/science/article/pii/S1877050920323565
- https://ieeexplore.ieee.org/abstract/document/8424966?casa_token=9VDrrTEF3I4AAAAA:svdQGpsXBYz7OOv1oDQ8WFEBCu7FHv81TVgBDOC1rryunKzZ8n6zkMhlxnl61WN8ZGpsy2htIen_Ow
- https://ieeexplore.ieee.org/abstract/document/10053178?casa_token=jk5Yo9cu0S4AAAAA:OqljGzq9UArfJZuio_Hv1lxrvs6DmTzWj2EQ-jpAASvDOjw2HPt3xQhzRj0wBxBNgxC4UtlVOXEbzA
- https://github.com/rust-in-blockchain/awesome-blockchain-rust
- https://casper.network/en-us/web3/web3-development/building-a-blockchain-in-rust/
- https://www.itmagination.com/blog/rust-development-blockchain-web3
- https://101blockchains.com/top-blockchains-using-rust-programming-language/
- https://blockchainmagazine.net/top-5-blockchains-using-rust-as-their-programming-language/
- https://www.cryptopolitan.com/top-10-blockchain-projects-that-use-rust-for-its-performance-safety-and-reliability/
- https://litslink.com/blog/rust-vs-go-for-blockchain
- https://www.linkedin.com/pulse/rust-blockchain-technology-perfect-match-hireotter/
- https://www.researchgate.net/publication/333486562_Probabilistic_Blockchains_A_Blockchain_Paradigm_for_Collaborative_Decision-Making/figures?lo=1
- https://www.semanticscholar.org/paper/An-Overview-of-Smart-Contract%3A-Architecture%2C-and-Wang-Yuan/357a8010971cb55ec5795f6c27f162af0fba3575

Q&A