

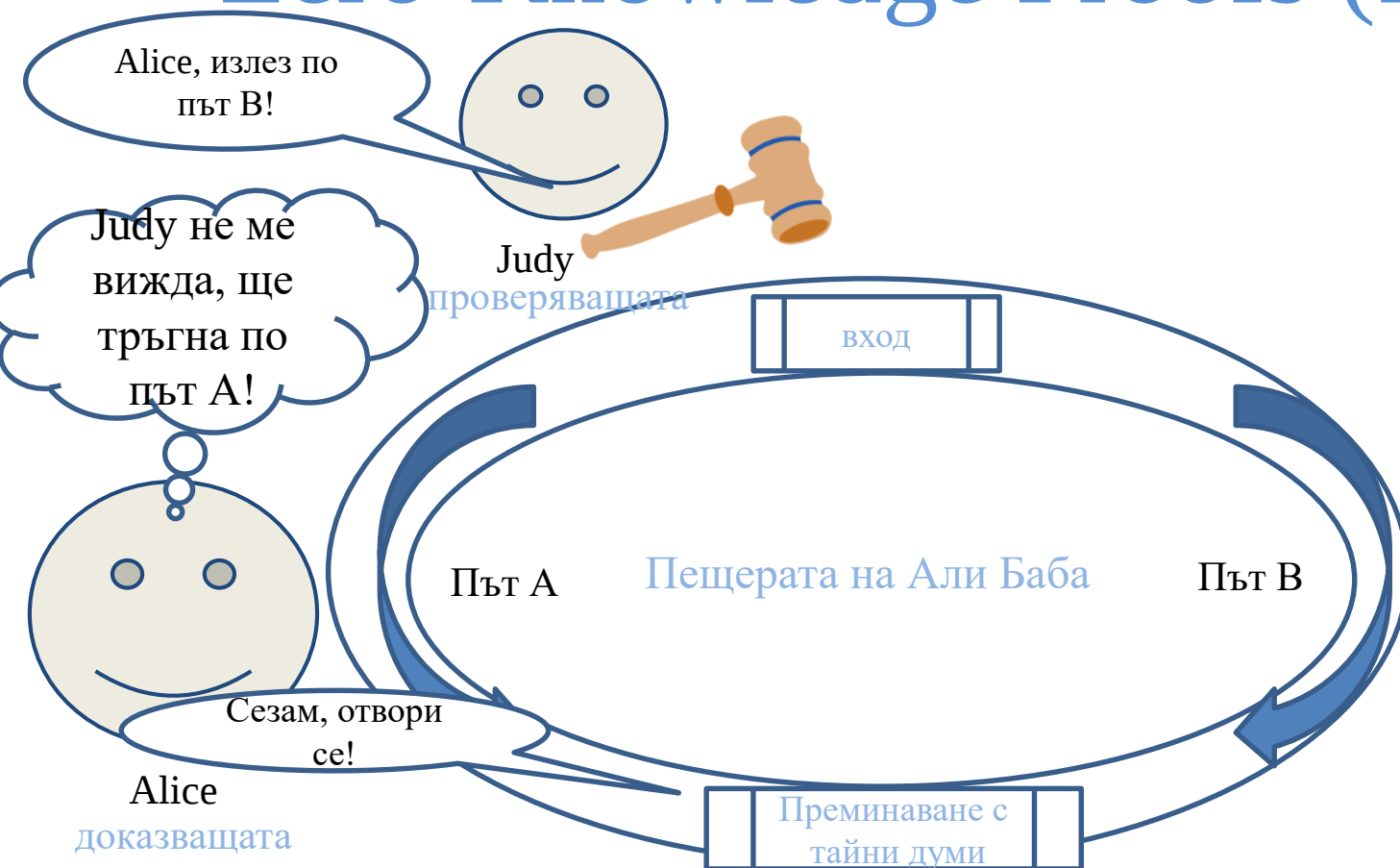
Zero-knowledge proof

проф. д-р инж. Венета Алексиева

ОСНОВНИ МОМЕНТИ

- Сигурност и поверителност на участниците в мрежата
- Zero-knowledge proof
- Zero-Knowledge Succinct Non-Interactive Arguments of Knowledge
- Zero-Knowledge Scalable Transparent Arguments of Knowledge
- Архитектура на ZKP

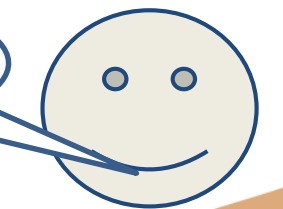
Zero-Knowledge Proofs (ZKP)



Решение: Judy остава отвън и не вижда Alice по кой път тръгва.

Zero-Knowledge Proofs (ZKP)

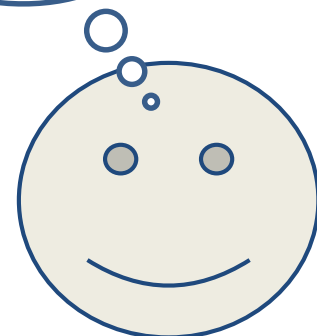
Alice, излез по път В!



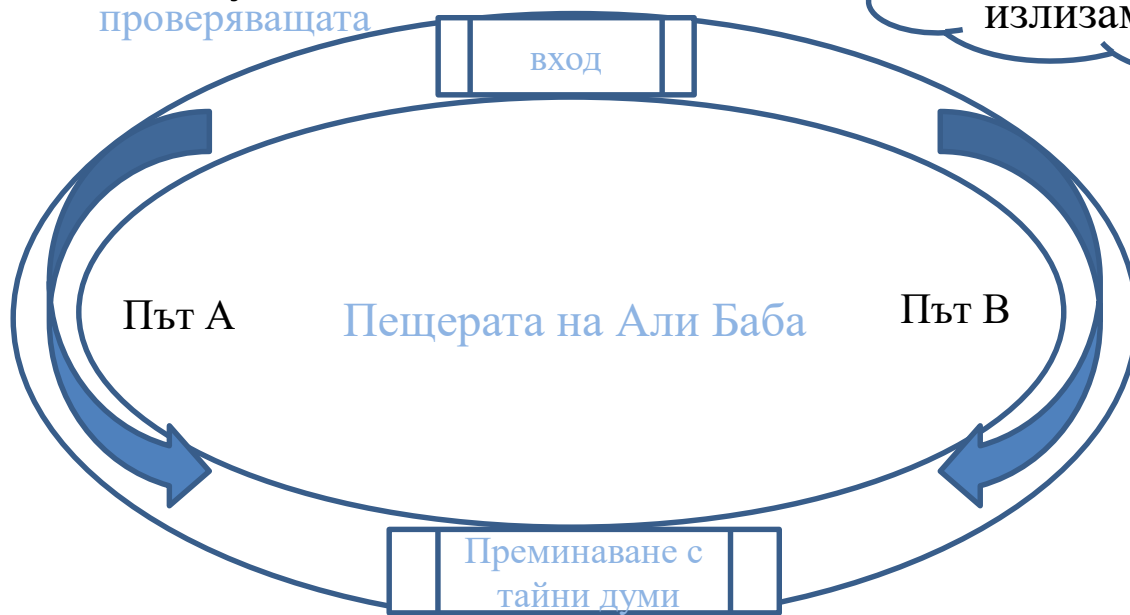
Judy
проверяващата



Преминах с
вълшебните думи и
излизам по път В!



Alice
доказващата



Ако Alice знае вълшебните думи няма значение по кой път тръгва, ще се върне по поискания от Judy.

Ако Alice не знае вълшебните думи, няма да отвори вратата. Ако трябва да се върне по път В, а се върне по път А – значи не ги знае.

За 1 опит е 50% е шансът Alice да уцели какво ще поиска Judy. След 5 повторения шансът пада на 3,1%, след 20 повторения е 0.0001%

Zero-Knowledge Proofs (ZKP)

- ZKP е криптографска техника, която позволява валидиране на данни без разкриване на поверителна информация извън необходимото за процеса на проверка.
- Този подход подобрява поверителността и сигурността, като смекчава потенциалните рискове от разкриване на данни, които не са необходими.
- ZKP позволява на една страна (доказващ) да докаже на друга страна (проверяващ), че **дадено твърдение е вярно, без да разкрива никаква друга информация, освен самия факт, че твърдението е вярно.**

Предназначение на ZKP

Традиционните блокчейни (като Bitcoin и Ethereum) са напълно публични — всеки може да види баланса и историята на транзакциите. ZKP решава:

- **Абсолютна поверителност (Privacy):**
 - Позволява изпращането на транзакции, при които сумата, подателят и получателят остават скрити за баланса на мрежата, но математически се доказва, че транзакцията е легитимна и парите съществуват (напр. при криптовалути като **Zcash**).
- **Масшабируемост (Scalability) чрез ZK-Rollups:**
 - Вместо блокчейнът да обработва 1000 транзакции една по една, технология от второ ниво (Layer 2) ги събира, обработва ги извън основната мрежа и генерира едно малко математическо "доказателство" (proof). То се изпраща към главната мрежа на Ethereum, която го проверява мигновено. Това прави транзакциите **стотици пъти по-евтини и по-бързи**.

Пример за употреба на ZKP

- За мащабиране на Ethereum (ZK-Rollups):
 - zkSync, Starknet, Polygon (zkEVM), Linea, Scroll - Мрежи от второ ниво, които правят транзакциите в Ethereum до 100 пъти по-евтини.
- За поверителност и сигурност:
 - Aleo, Mina Protocol (Блокчейн с фиксиран размер от едва 22 KB, т. К. цялата история на веригата е компресирана в едно ZK доказателство).

Ноо...

- ZKP) се използват активно на три нива:
 - в блокчейн мрежите,
 - в киберсигурността
 - при защитата на личните данни в дигиталния свят.

Приложения на ZKP

1. Блокчейн и мащабиране на Ethereum (Layer 2)

- Това е най-масовото практическо приложение в момента. Използва се за обединяване на хиляди транзакции в едно общо доказателство, за да се намалят таксите:
 - **zkSync, Starknet, Scroll и Linea**: Мрежи от второ ниво, които правят транзакциите в Ethereum до 100 пъти по-евтини.
 - **Mina Protocol**: Блокчейн с фиксиран размер от едва 22 KB (колкото една текстова снимка), тъй като цялата история на веригата е компресирана в едно ZK доказателство.

Приложения на ZKP

2. Поверителни транзакции (Privacy Coins)

- **Zcash (ZEC) и Iron Fish:** Криптовалути, които позволяват на потребителите да изпращат пари напълно анонимно. Смарт договорот доказва, че койните са истински и не са похарчени два пъти, без никой да вижда баланса на портфейла или сумата на превода.

Приложения на ZKP

3. Дигитална идентичност (Decentralized Identity)

- **Електронни паспорти и лични карти:** Позволява на гражданите да докажат пред институция или уебсайт, че имат право на достъп (например, че са пълнолетни или граждани на ЕС), без да споделят имената си, ЕГН или рождена дата.
- **Worldcoin (World ID):** Използва ZK доказателства, за да потвърди, че даден потребител е реален човек (чрез сканиране на ириса), без да свързва неговата биометрична информация с крипто портфейла му.

Приложения на ZKP

4. Финансов сектор и банково дело (DeFi & TradFi)

- **Проверка на кредитоспособност:** Потребител може да докаже на банка или DeFi платформа, че доходите му са над \$50,000 на година, за да получи заем, без да показва точния размер на заплатата си или банковите си извлечения.
- **Институционална търговия:** Големи инвестиционни фондове извършват сделки на блокчейна, като доказват, че разполагат с необходимия капитал, без да разкриват търговските си стратегии пред конкурентите.

Приложения на ZKP

5. Сигурни системи за гласуване (E-Voting)

- **Анонимен електронен вот:** ZKP се прилага при електронни избори, където системата може да провери и потвърди, че гласът е на легитимен избирател и е преброен правилно, но никой (дори администраторът на системата) не може да разбере за кой кандидат е гласувано.

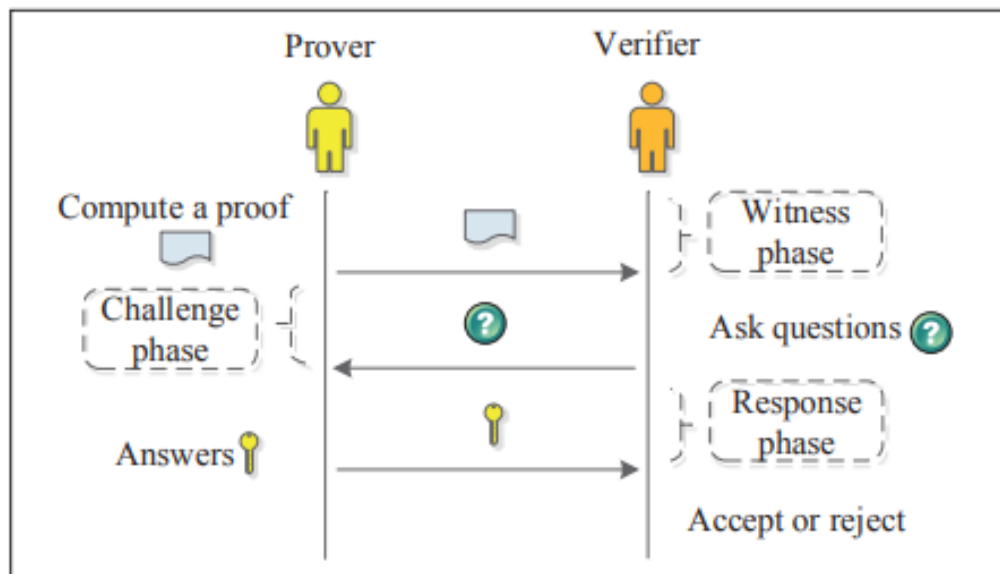
Zero-Knowledge Succinct Non-Interactive Arguments of Knowledge (Zk-SNARKs)

- Този модел използва опростен процес на доказване, използващ кратки низове от символи, което повишава неговата практичност, като същевременно запазва производителността на блокчейна.
- Той е лек, като включва само доказващия, проверяващия и настройката (която генерира ключовете за доказване и верификация).

Zero-Knowledge Scalable Transparent Arguments of Knowledge (Zk-STARKs)

- За разлика от zk-SNARK, zk-STARK не изискват надеждна настройка, което ги прави по-сигурни.
- Те използват усъвършенствани математически техники, като например бърз Reed-Solomon IOP of proximity и Merkle дървета, за да постигнат тази сигурност.

Архитектура на ZKP



- Фаза на свидетелство
 - Доказващият генерира доказателство и представя свързаното с него твърдение на проверяващия.
- Фаза на оспорване
 - Верифициращият задава конкретни въпроси, за да оцени валидността на доказателството.
- Фаза на отговор
 - Доказващият предоставя отговори, които верифициращият използва, за да приеме или отхвърли доказателството.

Подходи

- Използване на езици за описание на хардуер (HDL)
 - Пример: Circom
- Използване на библиотеки в езиците за програмиране на високо ниво
 - Примери – Gadgetlib (C++), Arkworks, Bellman (Rust)
- Използване на специфични за ZKP езици за програмиране
 - Примери – ZoKrates, Noir, Leo, Zinc и др.

Предимства на ZKR

1. Подобрява сигурността на данните за участниците в мрежата.
2. Подобрява прозрачността в управлението на веригата за доставки.
3. Поддържа мащабируемостта на блокчейн чрез оптимизиране на обработката на транзакции.

Zk-Rollups

- Този подход комбинира ZKP и Rollups, за да подобри ефективността на блокчейна.
- Rollups служат като решение за мащабиране на Layer-2, обработвайки множество транзакции в едно доказателство, като по този начин намаляват разходите и подобряват мащабируемостта.
- Компонентът ZKP гарантира сигурност и поверителност, позволявайки транзакциите да бъдат „масово проверявани“, без да се компрометира поверителността на данните.

Изкуствен интелект и блокчейн

- Агентите с изкуствен интелект (AI), наричани още автономни агенти, са управлявани от AI програми, способни независимо да определят целите на задачите, да задават приоритети и да изпълняват задачи въз основа на зададените им приоритети.
- Тези агенти работят в итеративен цикъл, като непрекъснато прецизират и изпълняват задачи.
- След като целта е определена, агентите автономно поемат процеса.
- Примери: AutoGPT, BabyAGI и Microsoft Jarvis (HuggingGPT).

Decentralised Autonomous Agents (DAA)

- Интеграцията на блокчейн технологията с агентите с изкуствен интелект доведе до появата на децентрализирани автономни агенти (DAA).
- DAA работят независимо в блокчейна, използвайки интелигентни договори и децентрализирани протоколи за изпълнение на задачи, без да разчитат на централен орган.
- Агентите с изкуствен интелект притежават способността да учат, да овладяват задачи от реалния свят и да предоставят точни резултати.

Характеристики на DAA

- Самоуправляващи се организации
 - DAA функционират автономно, вземайки решения без външен контрол.
- Автоматизирано изпълнение на задачи
 - Тяхното функциониране е подобно на автоматите за продажба, които раздават продукти въз основа на потребителски вход без човешка намеса.
- Децентрализация
 - Те изпълняват действия без зависимост от централизиран орган.
- Оперативна съвместимост
 - DAA могат да взаимодействат между множество платформи, включително публични и частни блокчейни и решения извън веригата.

Приложения на DAA

- Децентрализирани финанси (DeFi)
 - Автоматизирано управление на портфолио, управление на активи и алгоритмична търговия.
- Интелигентно изпълнение на договори
 - Автоматизиране на договорни споразумения без необходимост от посредници.
- Управление на данни
 - Сигурно и автоматизирано обработване на данни в децентрализирани мрежи.

Въпроси ?

Благодаря за вниманието !