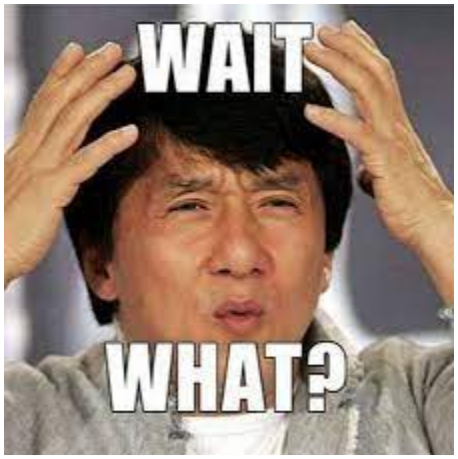
What is a zero knowledge proof?

Zero knowledge proof е метод при който една страна така наречения proover може да докаже на друга страна така наречения verifier, че някакво твърдение е вярно без да издава никаква друга информация освен, че твърдението е вярно.
Wait what?



Това може да изглежда много нереално първоначлно, когато човек го чуе
В интернет има множество примери за zero knowledge proofs. (graph coloring, tunnel door, where is waldo) някой от вас може да са ги чували, ако са гледали за zkp в youtube или google. Нито един от тези примери няма някакво директно практическо приложение и те кара да се чувстваш още по зашеметен как забога работят ZKP????

Всъщност много по-добър и реално практичен пример, с който предполагам сте запознати е public / private key криптографията. Там може да докажеш на някой че знаеш частния ключ за някой публичен ключ без да издаваш какъв е частния ключ. Това се случва с така наречения подпис. Той ти дава съобщение, което ти подписваш с твоя частен ключ и той може да верифицира, че това съобщение е подписано от частния ключ зад този публичен ключ. TODO: Insert picture here

Това се случва благодарение на някакви математически трикове. Които са извън темата на сегашната лекция.

Но ако приемем тези математически трикове за черна кутия, може да си представим че би било възможно да се измислят такива трикове при които някой да може да ти докаже че притежава поне един от няколко частни ключа.
Ок then

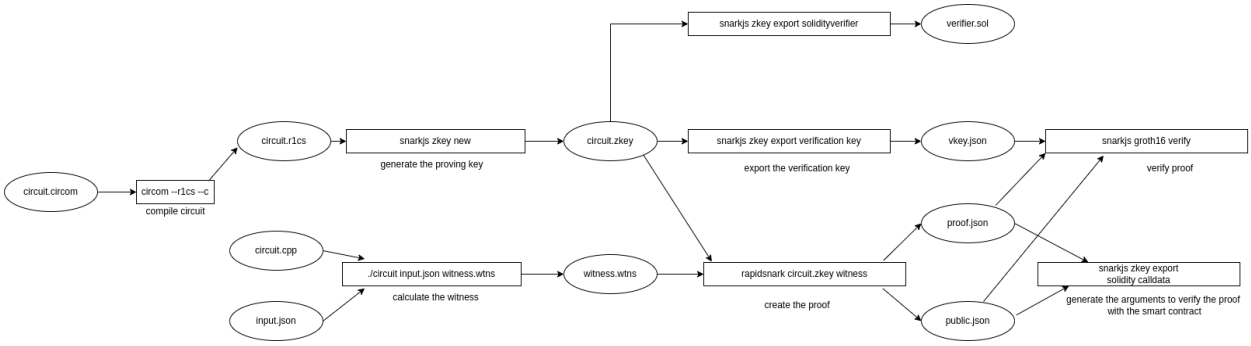
Всъщност причината zkp да станат толкова популярни е измислянето на системи, където можеш да опишеш определени входни променливи и определени зависимости между тях (компютърна програма) и да ти се генерират математическите трикове с които да създаваш доказателство от входните променливи. И да можеш да верифицираш това доказателство.

Най-популярните протоколи за създаване на zero knowledge proofs са
zk-SNARK
Succinct Non-Interactive Argument of Knowledge
Succint означава че доказателството е кратко в случая на SNARK с константен размер, тоест верифицирането на доказателството отнема константно време независимо от размера на проблема който доказваме. Това дава още едно интересно приложение на zkp а именно че може да се ползват за доказване че наистина сме изпълнили някакво изчисление коректно.

zk-STARK

Enough is enough.
Най-лесно е да разбереш нещо, като го видиш на практика

Значи буквално хората са създали различни DSLs за писане на zero knowledge circuits. Това е програмата от която се генерират prover-а (програмата която генерира доказателствата) и verifier-а (програмата която верифицира доказателтвата)



Very basic circom демо:
(Multiply3)
(Hash something and prove I know it)??

Voting system demo
(ZKHACK)