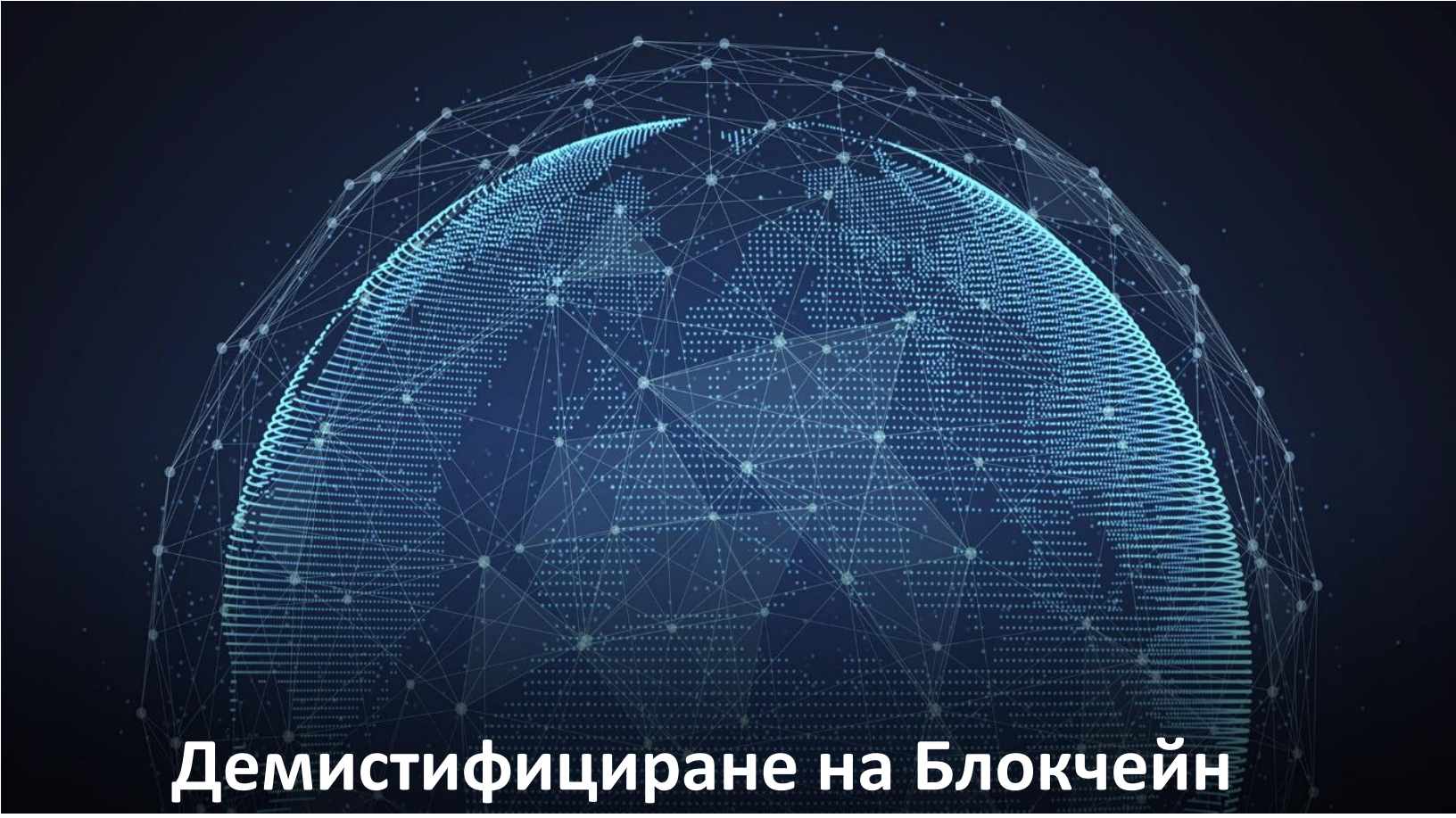


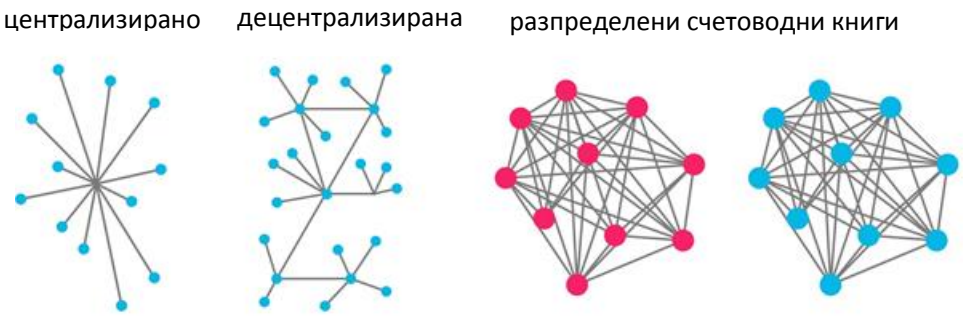
Демистифициране на Блокчейн

Какво е блокчейн?

Въпреки буквалния превод и значение на думата блокчейн - верига от блокчета, това е по-скоро набор от технологии, които могат да бъдат програмирани да записват и проследяват нещо ценно. Към момента обаче вече имаме процеси за проследяване на данни. **Какво е толкова специалното на блокчейн?**

1. **Метод за проследяване и съхранение на данни:**

Blockchain съхранява информация в пакети, наречени блокове, които се подреждат по хронологичен ред, за да образуват последователност или запис на събития - Блокчейн. В този смисъл е подобно на счетоводна книга, ако някой желае да пренапише данните в един отделен ред в миналото, няма да може. Промяната трябва да бъде регистрирана в нов блок, който ще детайлизира промяната от X-Y и ще отбележи точното време и дата, на които е направена промяната (регистрация на времето). За разлика от текущите писмени форми на дневници или файлове с база данни в една система, Blockchain е проектиран да бъде децентрализиран и разпределен в мрежа от компютри, създавайки



ключово предимство пред стандартните решения за съхранение на данни.

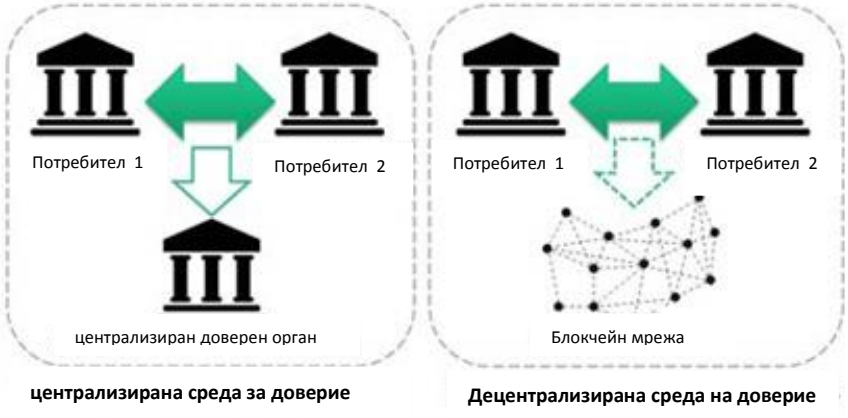
Има очевидни предимства, а именно намаляване на бюрокрацията и осигуряване на бърз и лесен достъп до данните. Още по-важно е, че децентрализацията на информацията значително намалява риска от подправяне на данни и подобрява устойчивостта на системите срещу кибер-атаки.

Увеличава доверието в данните - Създаване на блокчейн:

В първия етап от добавянето на данни към Blockchain трябва да бъде решен криптографският пъзел, като по този начин се създаде блок. Компютърът, който решава пъзела, споделя решението с всички останали компютри в мрежата. Този процес е известен като "Доказателство за свършена работа". Мрежата след това колективно проверява това доказателство за работа и ако е вярно, блокът се добавя към веригата. Тази комбинация от комплексни математически пъзели и проверка от цялата мрежа от компютри означава, че потребителите могат да се доверят на данните във всеки блок във веригата. С други думи, мрежата изгражда доверието за нас.

За да се изгради още повече доверие в данните, мрежите за проверка по веригата допълнително използват нещо, наречено "хаш функция", което отнема големите бази от данни, съставящи блоковете, и създава уникална стойност на данните с фиксирана дължина, иначе известна като хаш. Всяка промяна в оригиналните данни и функция ще доведе до напълно различна хаш стойност, поради което хашове са известни като "цифрови пръстови отпечатъци". Тъй като хаш функцията не може да бъде върната обратно, тя служи като метод за проверка на автентичността на данните, като същевременно запазва частното съдържание защитено. Всеки произведен блок съдържа хаш от предишния блок, като по този начин образува верига: блок-веригата.

Какво означава това доверие в мрежа в сравнение с доверието, което познаваме? Премахва необходимостта от посредници. Понастоящем, когато правим бизнес един с друг, ние не споделяме нашите частни финансови или бизнес регистри, а по-скоро разчитаме на доверени посредници като адвокат или банка, за да потвърдим самоличността и документацията. Например, ако искам да продам моят автомобил на някого в друга държава, ще трябва да използвам сайт на трета страна (посредник), като например ebay или mobile.de, който може да потвърди самоличността ми и факта, че наистина притежавам колата. Въпреки това, дори и при сайта на трета страна, все още има малък риск, че бих могъл да фалшифицирам самоличността или

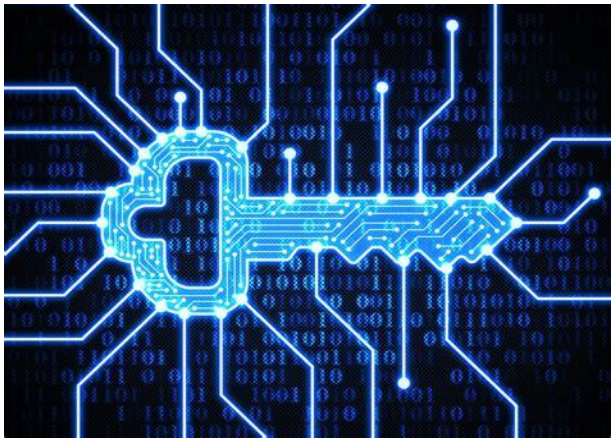


централизирана среда за доверие **Децентрализирана среда на доверие**

собствеността си върху автомобила, поради което сайтове като eBay предлагат пълна

компенсация на купувачите в случай на измама. Въпреки това, с Blockchain, мрежата изгражда доверието за нас. Използвайки процес, наречен криптография, купувачът може да потвърди самоличността на продавача и че той наистина притежава колата.

Какво представлява криптографията?



За да обясня криптографията в Blockchain, ще използвам аналогията на физическа кутия. Вероятно вече сте запознати с нормалната криптография, известна като "симетрична" криптография.

Пример: Иван има кутия с ключалка и разбира се ключ, който може да отключи и отвори кутията. Ако иска да пази вещите си безопасно, той ги заключва в кутията, и само той или някой, който притежава копие на ключа, може да отвори кутията.

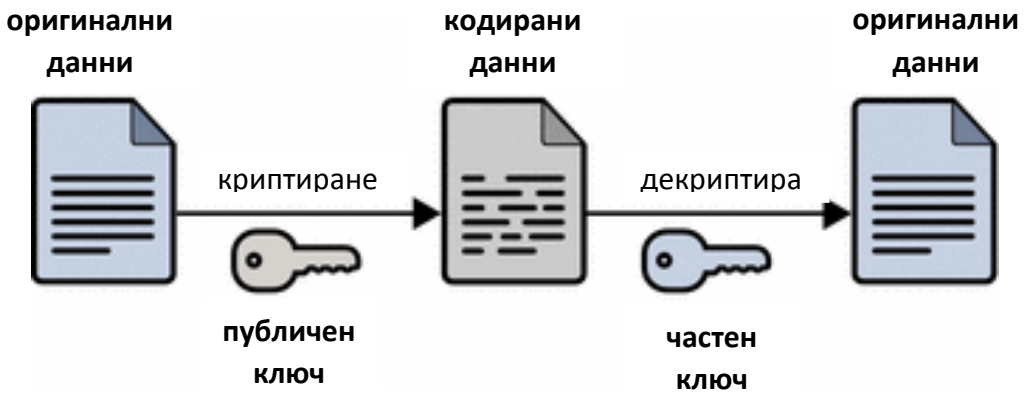
Това е симетрична криптография: имате един ключ и го използвате, за да шифровате "заключване" и да дешифрирате "отключите" вашите данни. В асиметрична или "публична ключова" криптография нещата са малко по-различни. Кутията на Иван вече има много специална ключалка с 3 възможни опции, опция А (заключена), опция Б (отключена) и опция В (заключена). Иван вече има два ключа, един частен ключ, който работи по посока на часовниковата стрелка, отключва от А до Б и заключва отново от Б до В. Другият е публичен ключ, който притежава, но също така дава на всеки, когото среща. Този клавиш работи в обратна посока, отключвайки кутията от В до Б и отново заключвайки от Б до А.

Какъв е смисълът, бихте попитали?

Представете си, че искате да изпратите на Иван важни документи; можете да поставите документа в кутията и да използвате копие на публичния ключ, за да го заключите. Тъй като публичният ключ се обръща само обратно на часовниковата стрелка, вие го превъртате в позиция А. Сега единственият ключ, който може да отключи кутията (позиция АБ) е частният ключ на Иван, затова сте уверени, че Иван е единственият който може да получи документите, които му изпратихте. Ето защо технологията се нарича криптиране с публичен ключ: всеки, който притежава копие от публичния ключ на Иван, може да постави документите в кутията, и да бъде сигурен, че само Иван може да я отключи.

Освен това "шифроването на публични ключове" има друга употреба, а именно, че ако Иван иска да изпрати някой документ, получателят може да бъде сигурен, че документът е автентичен, тъй като, ако могат да използват публичния ключ на Иван, те знаят, че само Иван би могъл да постави документа там. Единствено неговият частен ключ може да заключи кутията по посока на часовниковата стрелка, от Б до В, следователно, ако има данни за някой, който държи публичния ключ, те могат да са сигурни, че самият Иван е поставил данните там. Това се нарича цифров подпис.

В случая на блокчейн е дори по-лесно от примера. Можете да съхранявате частния си ключ, номер, във файл или USB, в зависимост от това, което ви се струва като най-сигурната опция за вас; Междувременно вашият публичен ключ, също и дълъг номер, може да бъде показан в подписа ви за електронна поща, LinkedIn, визитни картички, уебсайтове и т.н. И вместо кутии можете просто да заключвате и да отключвате данни автоматично чрез приложение с кода си.



Николас Даниелс,
Университета в Кент