# Top 8 Privacy Coins

Steven White12-15 minutes 16.04.2018 г.

Често срещано погрешно схващане е, че [биткойните и другите криптовалути](https://www.investinblockchain.com/top-cryptocurrencies/" \o "Биткойн и други криптовалути" \t "_blank) са напълно анонимни и непроследими. Всъщност много блокчейни само прикриват самоличността на потребителите, като същевременно оставят след себе си публичен запис на всички транзакции, извършени в блокчейна. Данните в книгата често включват колко токена потребителят е получил или изпратил в исторически транзакции, както и баланса на всяка криптовалута, която има в портфейла си.

Съществува опасение, че дори със скритата им самоличност, потребителите все още могат да бъдат идентифицирани въз основа на тяхната дейност в блокчейн. Ето защо някои хора се обръщат към монети за поверителност – криптовалути, които предоставят на потребителите по-високо ниво на анонимност.

Въпреки че са противоречиви (някои власти разглеждат монетите, ориентирани към поверителността, като незаконен инструмент, който може да бъде използван от престъпници за извършване на незаконни дейности, като например пране на пари), монетите за поверителност са най-безопасният начин за потребителите да извършват [блокчейн транзакции,](https://www.investinblockchain.com/best-practices-cryptocurrency-transactions/" \o "блокчейн транзакции" \t "_blank) без техните финансови данни да бъдат разкрити на обществеността. Тези платформи обикновено имат няколко функции, ориентирани към поверителността, като скрити адреси или частни транзакции, които могат да се използват за скриване на потребителска информация в блокчейни.

Ако се интересувате да научите повече за монетите за поверителност, ето нашите топ 8 любими, които в момента се предлагат на пазара.

## **Monero**



**[Monero](https://www.investinblockchain.com/what-is-monero/" \o "Monero" \t "_blank)** стартира през 2014 г. и оттогава се разрасна, за да се превърне в една от най-стабилните и сигурни монети за поверителност, пуснати до момента. Тяхната платформа за криптовалута е продукт на Bitcoin fork, но за разлика от Bitcoin, Monero е създаден с няколко функции за анонимност. Monero ефективно позволява на своите потребители да имат твърд контрол върху поверителността на своите данни, като запазват информацията за транзакциите напълно анонимна в блокчейна.

Monero има няколко уникални характеристики, които му помогнаха да се разрасне, за да стане най-големият претендент на пазара на монети за поверителност.

#### **Подписи на пръстени**

Пръстеновият подпис е цифров подпис, който се създава чрез обединяване на група от подписващи. Monero използва този цифров подпис, за да въведе множество подписващи (обикновено 5) във всяка транзакция. Само изпращачът може да генерира и изпрати ключа за изразходване и само действителният получател ще може да открие ключа и да изразходва средствата, свързани с него. С поставен подпис на пръстена е невъзможно да се свърже която и да е транзакция обратно към който и да е потребител, предлагайки висока степен на поверителност.

#### **Ring Confidential Transactions (RingCT)**

Тази функция скрива сумата на всяка транзакция в мрежата на Monero. RingCT работи, като създава криптографско доказателство, което може да покаже, че входните и изходните суми са равни, без да разкрива нито едно от действителните числа.

#### **Стелт адреси**

Monero също използва мрежа от стелт адреси, за да позволи на потребителите да се изключат от блокчейна. Скритият адрес е адрес за еднократна употреба, който се създава за всяка транзакция. Потребителите на Monero също имат публичен адрес, който е публикуван в блокчейна, но повечето (ако не всички) от техните транзакции ще бъдат предадени през уникални стелт адреси.

С тези по своята същност ясни и лесни за разбиране функции, Monero успя да остане релевантен в крипто пространството, като същевременно предлага на потребителите напълно непроследима платформа за криптовалута.

За да научите повече за Monero, вижте „ [Пътна карта за Monero 2018: Бъдещето на частната цифрова валута изглежда светло](https://www.investinblockchain.com/monero-2018-roadmap/" \o "Пътна карта на Monero 2018: Бъдещето на частната цифрова валута изглежда светло" \t "_blank) “ и „ [Трябва ли да инвестирате в Monero? (Мнение)](https://www.investinblockchain.com/invest-in-monero/" \o "Трябва ли да инвестирате в Monero?  (Мнение)" \t "_blank) “.

## **Zcash**



**[Zcash](https://www.investinblockchain.com/zcash-what-the-future-holds/" \o "Zcash)** е друга биткойн раздвоена монета за поверителност, но има само няколко функции за поверителност. Основната функция за поверителност, която Zcash използва, са кратки неинтерактивни аргументи на доказателства с нулево знание (zk-SNARKs).

Това име може да е залък за произнасяне, но основната функционалност, която този метод за поверителност предлага, е лесна за артикулиране. zk-SNARKS криптира всички транзакционни данни, които се съхраняват в мрежата. Този метод проверява дали данните, които се обменят, са точни, но го прави, без да разкрива всички подробности за транзакцията.

Но е важно да се отбележи, че използването на тези функции за поверителност не е задължително, тъй като потребителите могат да изберат прозрачни (публични) или частни адреси. Някои критици смятат, че потребителите, които решат да не активират функциите за поверителност, могат да компрометират цялостната сигурност на цялата мрежа.

## **Тире**

Dash е малко по-различен от споменатите по-рано монети. Основана след разклонение на биткойн през 2014 г., тя е криптовалута тип равностойна връзка с отворен код, която предлага много от същите функции като [биткойн](https://www.investinblockchain.com/what-is-bitcoin/" \o "Биткойн" \t "_blank) . Но в допълнение към основните функции на биткойн, Dash включва и опция за незабавни и частни транзакции.

За да гарантират целостта на своята система, разработчиците на Dash избраха да внедрят и протокол Proof-of-Stake. Тази част от системата е предназначена да осигури допълнителна поддръжка на миньорите, които валидират транзакции на първото ниво на услугата.

Masternodes се въвеждат в мрежата с цел валидиране на транзакции на второто ниво на услугата, което улеснява частни и незабавни транзакции, както и функции за управление. За да стартира masternode, потребителят трябва да има поне 1000 токена в портфейла си.

Функцията за незабавно изпращане изпраща транзакции по второто ниво на блокчейна на Dash, което им позволява бързо да бъдат потвърдени.

Частните транзакции се изпращат с помощта на метода CoinJoin. Този метод се състои в свързване на транзакции заедно за извършване на „съвместни плащания“. Но за разлика от традиционното съвместно плащане, стойността, която е била разменена от всяка страна, и мястото, където е приключило плащането, са напълно неоткриваеми от трети страни.

Можете да [научите повече за Dash тук](https://www.investinblockchain.com/what-is-dash/" \o "научете повече за Dash тук" \t "_blank) . Запознайте се с най-новото от Dash и прочетете „ [Ще постигне ли Dash своя напредък през 2018 г. въпреки закъсненията в разработката?](https://www.investinblockchain.com/dash-progress/" \o "Ще успее ли Dash през 2018 г. въпреки закъсненията в разработката?" \t "_blank)“.

## **PIVX**



**[PIVX](https://pivx.org/zpiv/" \o "PIVX" \t "_blank)** е друга нова монета за поверителност, която работи подобно на Dash, но работи на Proof-of-Stake, а не на Proof-of-Work. На потребителите на PIVX е разрешено да стартират главни възли, които помагат за гладкото функциониране на мрежата. Командването на един от тези възли изисква залог от поне 10 000 токена (за сравнение, Dash изисква само 1000 DASH). С този много по-висок праг PIVX разполага с повече от наличните си токени, свързани в различни главни възли.

PIVX има бърза проверка на транзакциите и поддържа както частни, така и незабавни транзакции. Транзакциите могат да бъдат направени напълно анонимни, предотвратявайки откриването на реалната самоличност на дадено лице чрез анализиране на блокчейна.

Към момента на писане времето за блокиране е около 60 секунди. Таксите за транзакции също са доста малки. Тези качества правят PIVX достоен за споменаване в разговора за монети за поверителност.

Посетете [уебсайта на PIVX,](https://pivx.org/" \o "Уеб сайт на PIVX" \t "_blank) за да научите повече за този проект.

## **NavCoin**

NavCoin е децентрализирана криптовалута, която е раздвоена от биткойн. Той има за цел да разреши 2 проблема, които обикновено се срещат в блокчейн платформите:

* Данните се оповестяват публично в блокчейна, което го прави уязвим за злонамерени атаки от незаконни потребители.
* Повечето блокчейни използват „връщане назад“ като решение за уязвимостта на данните. Те нулират блокчейна до резервна точка след нарушение на данните, което означава, че направените транзакции, водещи до връщането назад, се изтриват.

Системата NavTech е комбинация от традиционната биткойн блокчейн и подверига NAV. Използването на две вериги позволява на потребителите да изпращат транзакции с пълна анонимност.

През 2017 г. NAV успя да постигне значителен растеж и сега управлява общност от повече от 50 000 потребители. През 2018 г. те се стремят да внедрят платформа за изграждане на блокчейн приложения в мрежата. В допълнение към тази цел те също се надяват да добавят поддръжка за незабавен обмен на различни валути.

Научете повече за NavCoin на техния [уебсайт](https://navcoin.org/" \o "уебсайт" \t "_blank) .

## **CloakCoin**



Cloak е ветеран монета за поверителност, която расте бавно, въпреки че е активна в нишата за поверителност от приблизително 4 години. Блокчейнът се управлява с помощта на консенсусен протокол Proof-of-Stake. Има сравнително кратки времена на блокиране и бързо обработва транзакции.

Платформата също така предлага 2 различни метода, за да направите вашите транзакции непроследими. Първият е техният протокол за поверителност за маршрутизиране на лук. Луковото маршрутизиране включва криптиране на съобщения с много слоеве (подобно на лук).

Той също така предлага процеса Enigma за осигуряване на допълнително прикриване на поверителността на транзакциите. Прикриването на Enigma се прилага, когато потребител поиска прикрита транзакция на Enigma. Тези транзакции се пренасят през специални възли на Enigma, които са проектирани да прикриват данните за транзакциите, като ги разбъркват с други произволни данни. Само тези възли на Enigma са в състояние да идентифицират дали входните и изходните данни са точни.

За да научите повече за CloakCoin, вижте **[тяхната бяла книга](https://www.cloakcoin.com/resources/CloakCoin_Whitepaper_v2.1.pdf" \o "тяхната бяла книга" \t "_blank)** .

## **Енигма**

  
Проектът Enigma е напълно отделен от процеса на прикриване на Enigma, използван при транзакции с CloakCoin. Enigma не е криптовалута, нито блокчейн; вместо това, това е протокол за поверителност, който може да бъде разгърнат в блокчейни и децентрализирани приложения. Следователно неговият токен, ENG, е отделно допълнение към списъка с най-добрите монети за поверителност.

Мрежата Enigma осигурява поверителност, като прави възлите неспособни да виждат данните, които изчисляват. Въпреки че не са в състояние ясно да видят върху какво точно работят, тези възли все пак са в състояние да проверят дали изчисленията им са извършени правилно. С данните, маскирани по този начин, Enigma се надява да отвори вратата за това, което те наричат ​​нов тип интелигентни договори – „тайни договори“ – при които основните данни, обработени в интелигентен договор, остават криптирани през цялото време.

Токенът на Enigma трябва да бъде закупен, за да стартирате възел в тяхната мрежа. След като закупите токена Enigma, можете да получите награди за обработка на данни. Но за да обработва данни, всеки възел трябва да направи гаранционен депозит. Ако данните бъдат подправени по време на процеса на проверка, депозитът ще бъде разделен между всички възли, които са обработили данните без грешка.

Всъщност притежаването на ENG позволява на хората да започнат да използват мрежата. ENG служи и като награда за участие в мрежата.

За да научите повече за Enigma, **[щракнете тук](https://enigma.co/" \o "Натисни тук" \t "_blank)** .

## **DeepOnion**

  
DeepOnion е нов проект за монети за поверителност, който предизвиква известен интерес в общността. Подобно на някои от другите монети в този списък, DeepOnion използва TOR за изпращане на непроследими транзакции. Той също така използва комбинация от протоколи Proof-of-Stake и Proof-of-Work, за да предложи бързо време за потвърждение.

DeepOnion също използва скрити адреси, за да запази транзакциите поверителни. Както бе споменато по-горе, скритият адрес позволява на подателя да използва еднократен потребителски адрес за своите транзакции. Получателят се нуждае само от един адрес, но преди да получи изпратената стойност, този блок се изпраща до уникални адреси във веригата, където не могат да бъдат свързани с личния адрес на изпращача или получателя. Това гарантира, че само подателят и получателят могат постоянно да знаят откъде произхождат плащанията и къде са изпратени.

Екипът на DeepOnion в момента работи върху DeepSend и DeepVault. DeepSend ще използва метод с множество подписи, за да предотврати проследяването на плащанията. DeepVault е услуга за съхранение на информация, която позволява на потребителите да съхраняват данни в блокчейна завинаги. За да бъдем по-точни, DeepVault позволява на потребителите да съхраняват хешове на файлове в блокчейна. За да провери целостта на файл, потребителят трябва само да сравни текущата си версия на файла с архива. Това може да бъде от полза за целите на проверката на целостта на важни документи.

С развитието на общността DeepOnion също ще стартира своята функция VoteCentral. Това ще позволи на потребителите на платформата да гласуват за нови разработки и да представят своите идеи за бъдещи проекти. Този проект сега е малък, но в някои отношения е обещаващ.

Посетете [уебсайта на DeepOnion,](https://deeponion.org/" \o "Уебсайт на DeepOnion" \t "_blank) за да научите повече.

## **Заключение**

Монетите за поверителност са нишова група от криптовалути. Някои хора може да не се притесняват дали историята на транзакциите им може да бъде открита от трети страни. Но други може категорично да откажат да участват във всяка платформа за криптовалута, която не може да им гарантира пълна поверителност.

Ако се интересувате от инвестиране в блокчейн, но имате притеснения относно личната поверителност, обмислете да започнете с някои от споменатите тук монети за поверителност.