

HB Token

В настоящият момент има голям подем в интереса към криптовалутите и криптотехнологията като цяло. Като компания, която се е насочила към добива на криптовалuti и хардуерното подsigуряване на блокчейн технологиите, искаме да променим начина на облачно базираните договори за майнинг мощност чрез нашият HB token.

Добиването на криптовалuti и самата технология на блокчейна е дългосрочен и рентабилен бизнес. Добиването на биткойн например е започнало преди 9 години и все още не е загубило уместност и до днес. Има едно голямо но обаче, добивът на биткойн е започнал с процесори, преминал е на видеокарти, след което на ASIC. Тоест, за да се задържите в този бизнес трябва постоянно да се реинвестира във все по-нова технология. Същевременно винаги съществуват рискове при добиването само на 1 криптовалута – риск от бъг при първоначалното ѝ проектиране, риск от излизането на пазара на алтернатива, която избягва недостатъците и въвежда нови екстри, и разбира се риск от драстичен спад в цената. За да диверсифицираме риска, инвестираме в различни алгоритми за добив.

I. Equihash:

Equihash е схема за доказателство за извършена работа. Решава изчислителен пъзел, алгоритмите за който имат необходимост от определени изчислителни и памет ресурси. Има три параметъра – n , k и d , които определят схемата Equihash- $n/k/d$, времето и сложността на пъзела. Параметър S – seed, който придава уникалност на всеки пъзел. Най-добрите алгоритми за Equihash- $n/k/d$ изискват наличие на време $O(2n/(k+1)+d)$ и памет $O(2n/(k+1))$. Решение на Equihash пъзел може да бъде открито чрез алгоритъмът на Wagner за Общовалидният проблем на рождения ден (GBP). Алгоритъмът на Wagner изисква памет $O(2n/(k+1))$ като всяко намаляване на паметта увеличава сложността във времето. Equihash не се нуждае от

прогрес и не се амортизира. Изисква повече време и повече хардуер. Equihash е асиметричен. Чрез Equihash е възможно постигането на две цели:

1. Намаляване предимствата на специализирани машини за добив на криптовалута спрямо обикновени компютри и смартфони;

2. Лека верификация при контракти като при Етериум. За постигането на тези две цели е необходимо доказателство за извършена работа (proof-of-work), което се нуждае от по-малко памет и време за верифициране – тъй нареченото асиметрично доказателство за работа, каквото е Equihash. Освен това Equihash е по-опростен заради своята сравнително определена необходимост от памет. Чрез Equihash могат да бъдат решавани алгоритми с много естествен паралелизъм като времеви фактор може да бъде значително намален.

Предимства и недостатъци на Equihash

1. Предимства:

- ефикасна верификация. Това се очаква да бъде изключително важно поради използване от потребители с мобилни устройства за Етериум договори;
- базиран е върху наличие на компютърна памет. Това е предимство, защото специализираните машини за добив на криптовалута са скъпи;
- не се очакват следващи оптимизации;
- предотвратява възможност за централизация на процеса по добив на криптовалута. С това допринася за демократизацията на дигиталните валути;
- спомага за развитие на компютърните науки;
- гъвкав е, не е лимитиран до определени криптовалута.

2. Недостатъци:

- изисква по-голямо количество компютърна памет;
- не е създаден специализиран хардуер за работа с Equihash;

- има вероятност да бъде използван в по-мощни ASIC машини.

Монети:

1.Zcash

Zcash е криптовалута, ползваща криптография и осигуряваща подобрена в сравнение с други криптовалути сигурност за своите потребители. Zerocoin протоколът е подобрен и преобразуван в система Zerocash, която е разработена до Zcash криптовалута през 2016-та година. Разработката и подобренията на протокола са извършени от Zerocoin Electric Coin Company или по-накратко Zcash Company. Създателят и управител на Zcash Company е Zooko Wilcox-O`Hearn. Екипа на компанията включва специалиста по криптография Matthew D. Green от университета Johns Hopkins, а един от първоначалните инвеститори е Roger Ver.

Zcash плащанията се извършват в общодостъпен блокчейн, но потребителите имат възможност да се възползват от допълнителна опция, позволяваща им да скрият изпращач, получател и сума, която се изпраща. Също като Биткойн, Zcash има фиксирано количество от двадесет и един милиона единици. През първите четири години от създаването си, 20% от количеството единици са преразпределени между инвеститори, разработчици и неправителствени организации. Транзакциите могат да бъдат видими както при Биткойн, но могат да бъдат и с нулева информация, наречени zk-SNARKs. Ако са от вторият тип, то те се наричат „защитени“ и се контролират от z-addr. Количествата Zcash са или във видими басейни или в защитени такива. От месец декември 2017-та година само 4% от Zcash количествата са в защитени басейни поради невъзможност на софтуери за портфейли да ги поддържат.

Официален уебсайт: <https://z.cash/>

Предимства и недостатъци на Zcash.

1.Предимства:

- технология с по-високо ниво на сигурност за потребителите;

- технология с по-високо ниво на анонимност за потребителите;
- добив чрез GPU за предотвратяване на централизация;

2. Недостатъци:

- вероятност за възможна зловредна атака през не добре разработени zk-SNARKS;
- волатилност на цената;
- организацията зад криптовалутата не е общество с отворен код, а юридическо лице;
- екипът зад криптовалутата получава такси от копаенето, наречени „Награда за създателите“;
- не е форк на Биткойн. Това означава, че някои от характеристиките на Биткойн е възможно да не могат да бъдат приложени;
- ключ, който е в основата на криптовалутата и се смята за унищожен, е възможно да бъде наличен и с него да се създадат неограничено количество монети;
- изпълнителният директор на криптовалутата е бивш член на активистка групировка cypherpunks.

2. BTCGold

Bitcoin Gold е форк на Биткойн блокчейн. С блок 491407 Bitcoin Gold копачите започват да създават блокове с нов proof-of-work алгоритъм. Това от своя страна създава разделяне на Биткойн блокчейн. Оригиналният Биткойн блокчейн продължава непроменен, но ново разклонение на блокчейн разделя оригиналния чейн. Новото разклонение е отделен блокчейн със същата история на транзакциите както Биткойн до форка, но от там нататък се отличава. В резултат от този процес се „ражда“ нова криптовалута. Целта на Bitcoin Gold е да направи отново Биткойн децентрализиран. Идеалистичното виждане на Сатоши Накамото за „един CPU – един глас“ е компрометирано от отделни копачи и ферми за добив на

Биткойн. С промяната на Биткойн алгоритъмът от SHA256 към Equihash, техниката за добив с SHA256 става неизползваема за добив на Bitcoin Gold. Така, Bitcoin Gold ще даде възможност на безброй нови хора по света да участват в процеса по добив с общодостъпни оборудване и технологии. По-децентрализираната и демократичната инфраструктура е по-устойчива и съвременна към оригиналните виждания на Сатоши.

Официален уебсайт: <https://bitcoingold.org>

Предимства и недостатъци на Bitcoin Gold

1. Предимства:

- стреми се към промяна на начина за добиване на криптовалута чрез прекратяване ползването на скъпи машини за добив;
- стреми се към премахване на корпоративни манипулации на пазара на Биткойн чрез привличане на повече обикновени потребители;
- ползва Equihash алгоритъм.

2. Недостатъци:

- около един процент от количествата монети ще се използва за заплащане на екипа зад криптовалутата;
- една от големите борси за криптовалути, Coinbase, заяви, че няма да поддържа криптовалутата;
- една от големите борси за криптовалути, Bittrex, не поддържа криптовалутата.

3. BTCGold-cash

Bitcoin Cash е форк на Биткойн блокчейн от 01.08.2017-та година. Група копачи не са съгласни с предложенията на SegWit2x и създават отделен блокчейн код. Новият код не е съвместим с този на Биткойн. Bitcoin Cash използва SHA256 алгоритъм. Този алгоритъм изисква по-голяма компютърна мощ за да бъде добиван. Компютърната техника, използвана за добив е ASIC. Големината на блока е увеличена от 1MB до 8MB, а интервалът му е десет минути. Количеството на Bitcoin Cash е 21 милиона токена. Промяната в трудността се извършва на всеки две седмици.

Предимства и недостатъци на Bitcoin Cash

1. Предимства:

- подкрепя SegWit2x;
- ползва алгоритъм SHA256;
- ползва машини ASIC;
- има по-голям блок – 8 мегабайта;
- трудността се регулира на всеки две седмици;
- притежава допълнителна защита срещу повторения на транзакциите – SigHash;
- децентрализирана криптовалута, устойчива на политически и социални атаки;
- таксите при транзакции са по-ниски.

2. Недостатъци:

- възможност за измама от злонамерени потребители, които лъжат, че могат да удвоят Биткойн с Bitcoin Cash;
- тъй като криптовалутата е сравнително нова, някои от дигиталните портфейли все още не я поддържат;
- по-малко позната криптовалута;
- по-малко приложения за изразходване.

II. Cryptonote

CryptoNote е приложна платформа за създаване на семейство анонимни криптовалUTI, най-известните от които са Bytecoin, Monero и DarkNote. Анонимността в CryptoNote е реализирана чрез използване на колективен подпис на изпращача и еднократен адрес (скриващ получателя).

Протоколът е разработен през 2012 г. от група разработчици под псевдонима Николас ван Саберхаген. Bytecoin, стартиран през лятото на 2012 г. е първата криптовалута, използваща тази технология. По-късно са стартирани и други криптовалUTI, използващи кода на Bytecoin.

Както и при Биткойн, майнерите получават награда за намерените решения. Но постъпковото усложняване на изчисленията характерно за Биткойн, в CryptoNote е заменено с постепенно плаващо усложнение: наградата намалява при всеки нов обработен блок.

Направено е от съображения да не влияе драстично върху пазарната стойност на криптовалутата. Bytecoin и Monero използват различни параметри на кривата на емисията. Разработчиците на DarkNote решават да използват отново стълбово усложнение на изчисленията, съкращавайки два пъти емисията всеки месец.

Официален уебсайт: <https://cryptonote.org/>

Предимства и недостатъци на Cryptonote

1. Предимства:

- подобрена сигурност – изисква няколко ключа за извършване на верификация;
- предотвратява двойните транзакции с един и същи ключ;
- гъвкави лимити. Големината на всеки блок се настройва автоматично.

2. Недостатъци:

- наличие на системни грешки с низове при работа с Poloniex;
- наличие на системни грешки при работа с Ubuntu;
- наличие на системни грешки при компилиране;
- наличие на системни грешки при извършване на по-големи транзакции;
- наличие на невалидни timestamp на блокове.

Монети:

1. Monero

Монеро е криптовалута с отворен код, създадена през април 2014 г., която се фокусира върху поверителност, децентрализация и мащабируемост. За разлика от други криптовалути, които са разновидности на Биткойн, Monero е базиран на „CryptoNote“ протоколът и притежава значителни разлики в алгоритъма, свързан с еквилибристика на блокчейна.

Monero е стартиран на 18 април 2014 г., първоначално с името „BitMonero“, което е съединение на „Bit“ (от Bitcoin) и Monero (което буквално означава „монета“ на Есперанто). Пет дни по-късно общността

избрала името да се скъси на „Monero“. Бива пуснат като първото разклонение („форк“ или „fork“ на английски) на базирана на „CryptoNote“ валута наречена „Bytecoin“, обаче с два важни отличителни белега. Първият е, че времето за създаване на блок бива скъсено от 120 минути на 60 минути. Вторият е, че скоростта на излъчване бива намалена с 50% (по-късно Monero се върна към 120 минути време за създаване на блок, докато запазва графика за излъчване, като бива удвоена наградата за откриване на нов блок). В допълнение, Monero разработчиците са намерили многобройни инциденти на код с лошо качество, които в последствие биват изчистени и реконструирани.

Няколко седмици след това, оптимизиран GPU „копач“ за CryptoNight Proof-of-work (доказателство за изпълнение на работата) функцията, бива разработен.

На 4 септември 2014 г., Monero се е възстановил от необичайна и нова атака изпълнена срещу мрежата на криптовалутата.

На 10 януари 2017 г., поверителността на Monero транзакциите се е затвърдила допълнително с ползването по избор на алгоритъма „Ring Confidential Transactions“, създаден от Gregory Maxwell, който е един от разработчиците на „Bitcoin Core“. „Ring signature algorithm“ въвежда допълнителен слой на конфиденциалност, като скрива количествата замесени в транзакция към някой, който не участва директно в нея. „RingCT“ транзакциите са включени по подразбиране, но все още е възможно да се прати транзакция без „RingCT“ до следващото „твърдо разклоняване“ („хард форк“ или „hard fork“, на английски) на 17 септември 2017 г. До началото на Февруари, над 95% от всички „non-coinbase“ транзакции използвали функцията по избор „RingCT“.

Официален уебсайт: <https://getmonero.org/>

Предимства и недостатъци на Monero

1. Предимства:

- с отворен код е;

- създателите не са отделили количества за себе си;
- използва непроследими (stealth) адреси при транзакциите;
- потребителите имат възможност да споделят историята на транзакциите си;
- всяка от монетите има еднаква стойност.

2. Недостатъци:

- волатилност на цената;
- Apple онлайн магазини не приемат плащания чрез мобилни приложения с тази криптовалута;
- проблеми в графичния интерфейс на портфейла на дигиталната валута;
- поради анонимността си, бива често използвана за непозволен добив чрез вградени кодове в уебсайтове;
- наличие на невалидни timestamp на блокове;
- криптовалутата се ползва за раплащания в магазини от Dark Web пространството.

2. Electroneum

Electroneum е сравнително нова британска криптовалута, създадена на 14-ти септември 2017-та година чрез първично публично предлагане (ICO). Разработена да се използва при онлайн залагания и игри, се счита за една от най-улеснената за ползване от страна на потребителите. С едно приложение в мобилното устройство, Electroneum може да се управлява със своите портфейл и добив. Криптовалутата е разработена върху свой уникален блокчейн с главна цел да обхване всички дейности, свързани с онлайн игри и залагания през мобилни устройства. Едно от най-силните предимства се състои в това, че може да се управлява и дори добива от мобилно приложение. Това ѝ предоставя възможност да се превърне в нов и лесен

начин за извършване на инстантни транзакции от мобилни устройства – от купуване на мобилни игри и изпращане на пари до други хора, до залагане на спортове в реално време. Това я отличава значително от други криптовалути, които са по-трудни за изразходване или закупуване. Количеството на Electroneum също е значително – 21 милиарда. Създател и предприемач на криптовалутата е Richard Ellis. Криптовалутата представлява и интересна възможност за инвестиции.

Официален уебсайт: <http://electroneum.com/>

Предимства и недостатъци на Electroneum

1. Предимства:

- криптовалутата подписа договор с един от най-големите телеком оператори при мобилни разплащания - XIUS;
- лесна за ползване;
- може да се добива и от мобилно устройство;
- може да се търгува на голямата борса за криптовалути Binance.

2. Недостатъци:

- извършването на транзакции понякога отнема прекалено дълго време или транзакциите просто биват прекъсвани без причина;
- липса на достатъчно търговци, приемащи плащания с Electroneum;
- мобилното ѝ приложение е било атакувано и успешно клонирано;
- няма разработено приложение за iOS.

III. Scrypt

Scrypt представлява криптографски защитена с парола функция, създадена от Colin Percival за онлайн услуга на Tarsnap. Алгоритъмът е

създаден с цел предотвратяване на хардуерни атаки. Опростена версия на scrypt се използва криптовалута за proof-of-work като за първи път е използван от анонимен програмист ArtForz. За да бъде изпълен scrypt е необходимо значителен период от време. Оторизирани потребители могат да изпълнят scrypt за кратко време, но неоторизирани (хакери), които желаят да достъпят функции, биха им били нужни множество на брой операции.

По-стари функции (PBKDF2) имат нужда от значително по-малко оборудване и ресурси. Затова те са по-лесно изпълними от злонамерени потребители. Това позволява наличието на атаки, изградени със стотици, дори хиляди имплементации на алгоритъма в хардуера. Scrypt е създаден за да намали подобен тип атаки чрез създаване на почти неизпълнима необходимост от хардуерни и други ресурси.

Голямата необходимост за ресурси на scrypt е породена от изкуствено генерирани списъци низове, които са част от алгоритъма. Веднъж след като е генериран списъка от низове, елементите му се достъпват по случаен принцип, комбинират се и така „произвеждат“ необходимата информация.

Тъй като елементите от списъка са генерирани алгоритмично, всеки елемент може да бъде генериран бързо чрез наличие само на един от елементите. Това намаля значително необходимостта от RAM.

Параметри на алгоритъмът:

1. Ключова фраза – низът от символи, които да бъдат хашнати;
2. Salt – низ от символи, които модифицират хаш срещу атаки от тип Rainbow table;
3. N – параметър за стойност на CPU и памет;
4. P – паралелизиращ параметър;
5. dkLen – изходна дължина на октетите;
6. r – параметър за големина на блоковете. Най-често се използва 8;
7. hLen – дължина на октетите на хаш функцията (32 за SHA256);
8. MfLen – дължина на октетите изходната смесена функция.

Scrypt се използва при криптовалюти като Litecoin и Dogecoin. За добивът им се използват ASIC машини за scrypt алгоритми.

Предимства и недостатъци на Scrypt

1. Предимства:

- по-бърз и по-опростен алгоритъм;
- по-лесен за използване с налични CPU;
- необходима му е по-малко електроенергия;
- дава възможност за добив чрез обикновени компютри;
- ползва се за добив на една от най-популярните криптовалюти – Litecoin.

2. Недостатъци:

- цената на Scrypt машини би била по-висока;
- необходимо му е значително количество компютърна памет.

Монети:

1. LTC

Litecoin е криптовалюта от тип peer-to-peer, с отворен код и с лиценз MIT/X11. Създаването и прехвърлянето на количества са базирани на криптографски протокол с отворен код, който не се управлява централизирано. Създаването на Litecoin е вдъхновено от и се сравнява по технически параметри с Bitcoin. Litecoin е стартиран в публичното пространство на седми октомври, 2011-та година от Charlie Lee, бивш служител на Google. Мрежата на Litecoin става достъпна на 13-ти октомври, 2011-та година. Представлява форк на Bitcoin Core, различаващ се основно по намаленото време за създаване на блок (2,5 минути), увеличен брой

единици, различен хаш алгоритъм (scrypt, вместо SHA-256) и малко променен графичен потребителски интерфейс. Litecoin достига пазарна капитализация от двадесет милиард долара през 2017-та година. Лайткойн може да бъде лесно закупен и продаден от много борси с всички видове валути. Лайткойн може да бъде идентифициран на борсите под валутните символи LTC или XLT.

Официален уебсайт: <https://litecoin.org/>

Предимства и недостатъци на Litecoin

1. Предимства:

- с отворен код е;
- не се управлява от една компания/организация;
- създадена е от бивш служител на Google;
- с намалено време за генериране на блок – 2.5 минути;
- ползва алгоритъм Scrypt;
- може да работи с по-големи количества транзакции;
- по-краткото време за генериране на блок предпазва от риск от атаки за двойни транзакции;
- втората по големина на пазарен дял след Bitcoin.

2. Недостатъци:

- създателят на криптовалутата продаде своите монети;
- машините, които добиват Биткойн не могат да се настроят за добив и на Litecoin;
- по-малко ликвидна от Биткойн.

IV. X11

X11 е широко използван хаш алгоритъм, създаден от разработчикът на Dash – Evan Duffield. X11 верижния хаш алгоритъм притежава поредица от единадесет хаш алгоритъма за доказване на извършената работа. Целта е да се осигури справедливо разпределение на криптовалюти, както са били разпределяни Bitcoin. X11 прави ASIC машините по-трудни за създаване, като по този начин дава повече време за разработка на криптовалутите преди да се случи централизиран добив. В днешно време X11 ASIC машините съставляват значителна част от цялостния мрежови хашрейт, но не са повлияли върху нивото на централизация на Bitcoin. X11 е представен през януари, 2014-та година под името „Xcoin“. Създаването му отчасти е вдъхновено от верижния хаш Quark, добавящ по-задълбочен и комплексен метод, увеличаващ броя хашове. Въпреки това се отличава от Quark по това, че сериите хашове се определят предварително, а не на случаен принцип. X11 използва множество серии от единадесет различни хашове (blake, bmw, groestl, jh, кескак, skein, luffa, cubehash, shavite, simd, echo), което го прави един от най-сигурните и сложни при модерните криптовалюти. Името X11 не е свързано с потребителският интерфейс за Unix/Linux потребителите. Алгоритъмът се ползва за добив на:

Dash (DASH)

CannabisCoin (CANN)

StartCoin (START)

MonetaryUnit (MUE)

Karmacoin (Karma)

XCurrency (XC)

Предимства и недостатъци на X11

1. Предимства:

- Увеличената комплексност и подобрения на верижния алгоритъм предоставя по-високо ефективни нива на сигурност и по-малко несигурност за дигиталните валути в сравнение с решения от тип proof-of-work, които не са защитени от SPOF. Например при пробив на SHA-256 е възможно застрашаване на цялата Bitcoin мрежа. В такъв случай криптовалутата с алгоритъм X11 ще продължи да функционира с високи нива на сигурност. Дори и единадесетте хаша да бъдат компрометирани, ще има време за да бъдат предприети мерки;
- Имайки предвид спекулативният характер на криптовалутите, X11 може да осигури високо ниво на защита и сигурност, които не могат да бъдат постигнати от алгоритми с един хаш;
- Графичните видео карти не се нуждаят от голяма мощност за да работят. Това води до по-ниски такси за електроенергия;
- Поради високата си комплексност, алгоритъмът ще даде по-дълъг период за копаене на потребители, добиващи с CPU/GPU.
- използва поредица от единадесет хаш алгоритъма за доказване на свършена работа;
- енергийно ефективен;
- използва се за добив на една от популярните криптовалути – Dash;
- държи ниски температури на използваната техника;
- дава възможност на потребители с обикновени компютри да се включат в добив на криптовалути.

2. Недостатъци:

- CPU добиват с хашрейт на Scrypto, което го прави уязвим при ботнет атаки;
- От финансова гледна точка не всички нови потребители биха могли да си позволят ползването на X11 алгоритъм.

Предимства и недостатъци на X11

Предимства:

- използва поредица от единадесет хаш алгоритъма за доказване на свършена работа;
- енергийно ефективен;
- използва се за добив на една от популярните криптовалути – Dash;
- държи ниски температури на използваната техника;
- дава възможност на потребители с обикновени компютри да се включат в добив на криптовалути;
- необходими са специфични знания за сглобяване на риг;
- с изключение на Dash могат да се добиват не толкова популярни криптовалути;
- съмнения за уязвимост към ботнет атаки;
- новите по-големи потребители на X11 ще се нуждаят от значителни количества оборудване.

Монети:

1. Dash

Dash (предишни названия Darkcoin и XCoin) е криптовалута от тип peer-to-peer с отворен код. Криптовалутата дава възможност за извършване на инстантни транзакции и защитени лични транзакции. Притежава модел за самофинансиране и самоуправление, което дава възможност на физически

лица и бизнеси да извършват работа с добавена стойност в мрежа. Децентрализираното управление и бюджетна система на криптовалутата я правят децентрализирана автономна организация.

Dash е представена с името XCoin (XCO) на 18.01.2014 г. На 28.01.2014 г. името ѝ е променено на Darkcoin. На 25.03.2015 г. името ѝ е променено на Dash. През

През първите два дни от стартирането си са били добити 1.9 милиона единици, което е около 10% от общото количество, които ще бъдат добити.

За разлика от Bitcoin мрежата, в която добитото се получава с ферми за копаене, Dash се развива чрез двустепенна мрежа. Някои от функциите, като например създаването на нови блокове се определя от копачите. Втората степен на управление се осъществява от „главни възли“, които отговарят за функциите PrivateSend и InstantSend.

На главните възли са им необходими 1 000 Dash за да предотвратяват атаки. Тази такса може да се изразходва по всяко време, но когато това се случи, се премахва главен възел от мрежата. Тъй като главните възли предоставят важни функции за мрежата, наградата от блока се разделя измежду копачите и главни възли по равно с 45% от блока. Останалите 10% финансират „бюджет“ и „хазна“.

PrivateSend е услуга за смесване на монети, базирана на CoinJoin с безброй модификации. Те включват използване на главни възли вместо един уебсайт, създаване на верига чрез смесване на множество главни възли. Максималното количество за транзакция е 1 000 Dash. Използването на PrivateSend позволява на главните възли да одобряват транзакции посредством специален мрежови код, наречен DSTX. Това дава допълнителна сигурност за потребителите.

InstaSend е услуга, която позволява почти моментално осъществяване на транзакции. Посредством тази система, входящата информация се заключава към определени транзакции и се верифицира от мрежа от главни възли. Проблемните транзакции и блокове се отхвърлят.

Официален уебсайт: <https://www.dash.org/>

Предимства и недостатъци на Dash

1. Предимства:

- една от най-иновативните и бързоразвиващи се криптовалюти;
- притежава специален протокол за скриване на произхода на авоарите – анонимизиращи трансакции (DarkSend);
- възли от втори ред, т.нар. „главни възли“;
- моментални трансакции. Криптовалутата предоставя механизъм, чрез който плащанията в мрежата се потвърждават в рамките на 4 секунди;
- вграден механизъм за гласуване. Всеки може да направи предложение в мрежата и да получи положителен или отрицателен отговор от даш общността;
- притежава портфейл.

2. Недостатъци:

- заради главните възли реално наличните количества монети са по-малко от обявените;
- няма достатъчно търговци, приемащи плащания с Dash;
- има слухове, че създателите на криптовалутата са си запазили значително количество за себе си;
- името на криптовалутата звучи тривиално – като почистващ препарат и това според някои влияе негативно върху маркетинга ѝ;
- не е напълно анонимна;
- главните възли причиняват до някаква степен централизация;
- високи такси за InstantSend;
- ползва ASIC машини;

- добивът с GPU води до загуби.

2. B2X

На 19.12.2017 г. са стартирани фючърси за търговия. На 28.12.2017 г. е стартиран форк. Общото количество монети е 21 милиона. Използва X11 алгоритъм. Големината на блока се увеличава до четири мегабайта. Блока се генерира за 2.5 минути. Има наличие на защита Replay – срещу повторени транзакции. Извършва се преизчисляване на сложността след всеки блок. Има уникален формат на адресите. Анонимност на транзакциите посредством ZkSnarks технология. Използване на интелигентни договори. Поддържа портфейли Zumminer и Freewallet.

Официален уебсайт: <https://b2x-segwit.io>

Предимства и недостатъци на B2X

1. Предимства:

- ползва X11 криптиращ алгоритъм;
- големината на блока е до четири мегабайта;
- бързо генериране на блокове – 2.5 минути;
- защита от двойно заплащане на транзакции – Replay;
- преизчисляване на сложността на добив след всеки блок;
- уникален формат на адреса;
- ползва се от онлайн платформа за обмяна на криптовалута ChangeNOW;
- решава проблем с бъг на Биткойн, наречен Malleability.

2. Недостатъци:

- не е дългосрочно решение поради необходимост от по-големи блокове;
- непотвърдена информация за собственост на шест милиона единици от разработчиците;
- популярният портфейл Trezor предупреди за потенциални проблеми с криптовалутата.

Монети:

3.Madesafe

Safecoin е дигитален криптовалутен токен, който е сърцето на мрежата Safe. Може да се възприеме като горивото в двигателя на мрежата Safe и се използва за заплащане на потребителите на мрежата срещу стойността, която те предоставят. Safecoin наподобява по своята същност на Steem долари и Steem мощност – потребителите биват възнаградени за своето участие в мрежата. Safecoin монетите се разпространяват изцяло по автоматизиран път без човешка намеса – чрез алгоритми. Общото количество монети е 4.3 милиарда като всяка една от тях има своя уникална идентичност. Монетите се „рециклират“, когато се обменят за услуги, за да има нови наличности монети за новите потребители. Safecoin монети се дават на потребители срещу предоставяне на неизползвани компютърни ресурси в мрежата. Такива включват безплатно дисково пространство, процесорна мощност и Интернет свързаност. Този процес се нарича „Фермерство“. Safecoin монетите могат да бъдат използвани за достъп и ползване на мрежови приложения като с част от монетите се заплаща директно на софтуерния програмист, разработил съответното приложение. Монетите могат да бъдат закупени и от потребители, които не желаят или нямат възможност да споделят ресурс в мрежата. По този начин се създава пазар, в който „фермери“ могат да продадат своите монети. Тези транзакции се осъществяват чрез Safe приложение или директно между потребителите.

Официален уебсайт: <https://maidsafe.net/>

Предимства и недостатъци на Madesafe

1. Предимства:

- разпространява се без човешка намеса;
- всяка от единиците притежава уникална идентичност;
- при обмен, единиците се рециклират, което подsigурява непрекъснато наличие от криптовалутата;
- наличие на приложение Safe Network за покупко-продажба на монети.

2. Недостатъци:

- не са известни до момента.

Бизнес план за токена:

Откъде идва повишаването цената на токена

Основен източник: добив на криптовалута

Допълнителни източници:

- разработване на софтуерни приложения, свързани с блокчейн
- такса от басейните ни за добив криптовалута
- листване на борсите за криптовалута

Разпределение на приходите:

- 70% се реинвестират в техника свързана с блокчейн;
- 20% за поддръжка и увеличение цената на токена;
- 5% за подобрене и увеличаване на инфраструктурата;
- 5% за разработка на софтуерни технологии свързани с блокчейн.