

Blockchain. Поколения. Криптовалути

проф. д-р инж. Венета Алексиева

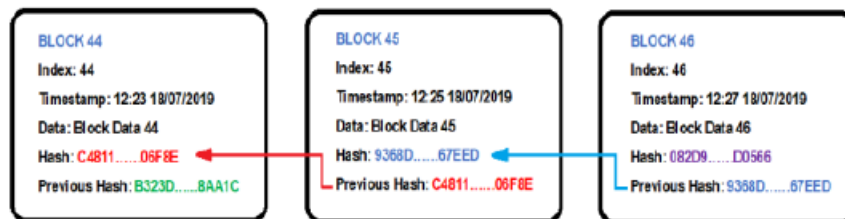
ОСНОВНИ МОМЕНТИ

- Поколения блокчейни. Характеристики
- Криптовалути
- Умни договори

Blockchain- същност

- DLT и блокчейн не са синоними.
- Не всички DLT използват blockchains
- Blockchain е верига от блокове за предаване на данни, използваща криптография и алгоритми за записването им по неизменен начин.

Блокова верига



- Блоковата верига се съхранява в мрежата в разпределен вид – с копия на структурата в компютъра на всеки участник в мрежата.
- Няма точно определено едно главно копие.
- Използва се връзка от типа всеки към всеки (Peer to Peer)
- Спазва се протокол за валидиране на новите блокове. Веднъж валидиран и записан никой блок не може да бъде променян без одобрение (консенсус) на останалите участници в блокчейн веригата.

Първо поколение Blockchain

приложения

- Цел - Сигурни, анонимни и децентрализирани финансови трансакции
- Използва се само консенсусният механизъм **Proof of Work (PoW)**, който изисква огромна изчислителна мощност, но осигурява изключително висока защита.
- Недостатъци:
 - Ниска скорост на трансакциите (скалируемост)
 - Високи такси при натоварване на мрежата.

 Bitcoin BTC

 Ethereum ETH

 Tether USDT

 BNB BNB

 USD Coin USDC

 XRP XRP

Първо поколение Blockchain приложения

 Bitcoin BTC

- Повече от 22 400 криптовалути

 Ethereum ETH

- Пазарна капитализация:

\$1,048,631,859,911

 Tether USDT

- Търгуван обем за 24 часа:

\$62,653,536,702

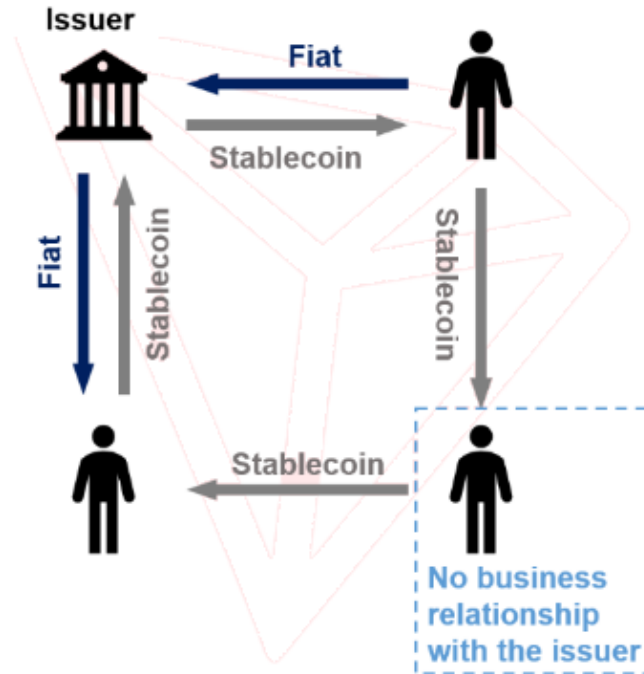
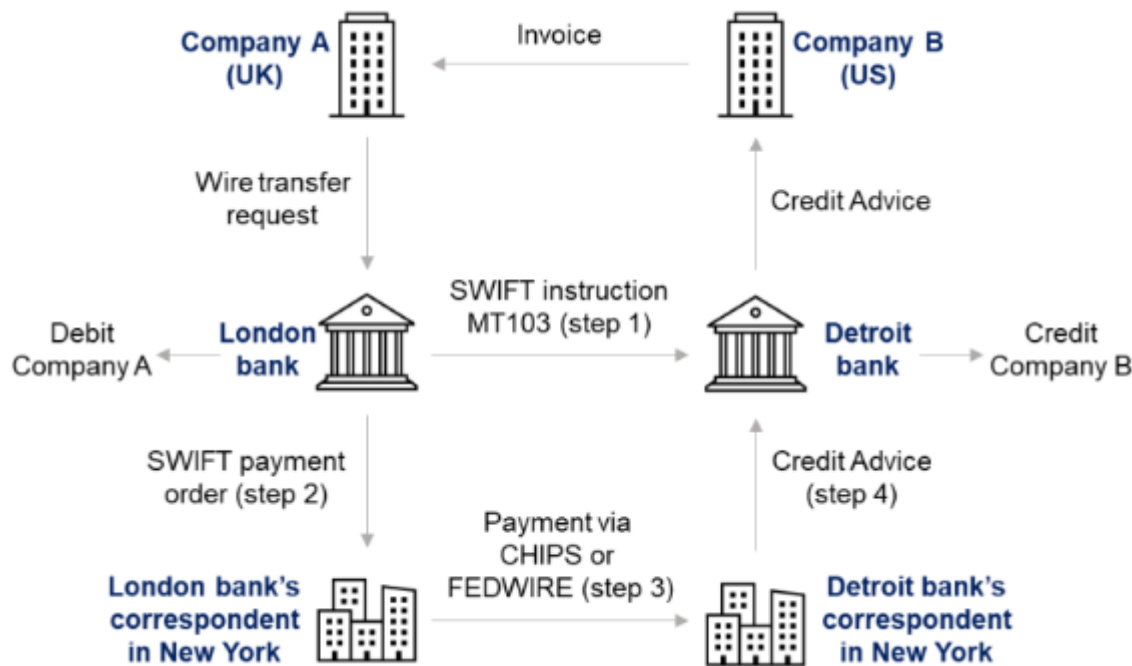
 BNB BNB

- Трансгранични плащания

 USD Coin USDC

 XRP XRP

Трансгранични плащания



- Традиционен подход - трансграничният превод на средства включва дълъг списък от посредници, включително финансови институции и доставчици на инфраструктурни услуги като SWIFT.
- SWIFT все повече се оказва неадекватен със своята висока цена, ниска ефективност и податливост на риск от хакерство.

Society for Worldwide Interbank Financial Telecommunications (SWIFT)

- SWIFT е глобална финансова съобщителна система за сигурен обмен на данни между банките по цял свят.
- SWIFT **не превежда реални пари**, а изпраща стандартизирани платежни нареждания, които банките изпълняват чрез своите кореспондентски сметки.
- Всяка банка в мрежата притежава уникален **BIC / SWIFT код** (от 8 или 11 символа) за точна идентификация.
- Използва криптирана мрежа за предаване на съобщения, които съдържат еднократни клиентски преводи.
- Ако между две банки няма директна връзка, плащането преминава през междинни (кореспондентски) банки.

SWIFT плащания

- Глобален обхват - свързва над 11 000 финансови институции в повече от 200 държави.
- Време за обработка - между 1 и 4 работни дни за трансакция в зависимост от часовите зони и броя междинни банки.
- Поддържани валути - практически всяка конвертируема валута по света.
- Висока сигурност - прилага строги международни стандарти за киберсигурност и защита срещу измами.
- Таксуване:
 - OUR (За сметка на платеща) – изпращача плаща всички такси по превода
 - SHA (Споделени такси) – изпращача плаща таксата на своята банка, а таксите на междинните и приемащата банка се удържат от изпратената сума.
 - BEN (За сметка на получателя) - Всички такси по трасето се удържат от сумата на превода.

SWIFT предимства и недостатъци

- Предимства:
 - Универсален стандарт,
 - възможност за изпращане на големи суми
 - проследимост на трансакциите чрез системата SWIFT gpi.
- Недостатъци:
 - По-бавни спрямо модерните локални системи (като SEPA в Европа)
 - по-високи такси и потенциални скрити разходи от междинни банки.

Single Euro Payments Area (SEPA)

- SEPA позволява извършването на трансгранични банкови преводи в евро при абсолютно същите условия, ниски такси и сигурност, каквито важат за вътрешните плащания в рамките на една държава.
- Включва всички 27 страни членки на ЕС (включително **България**), страните от ЕАСТ (Исландия, Лихтенщайн, Норвегия, Швейцария) и Обединеното кралство.
- Преводите се извършват **единствено и само в евро (EUR)**. Ако сметката е в друга валута, банката прави автоматично превалутиране.

SEPA плащания

- SEPA Кредитен трансфер (Standard) - класически превод за единични плащания.
- SEPA Незабавни плащания (Instant) - Светкавични трансфери, налични по всяко време.
- SEPA Директен дебит - Автоматично плащане на битови сметки или абонаменти към чуждестранни търговци.

Single Euro Payments Area (SEPA)

- **Предимства:**
 - Цена - Таксите са равни на таксите за вътрешен превод в съответната страна (т.е. ниски такси)
 - Скорост - Standard -1 работен ден; . Instant- под 10 секунди
 - Идентификация - IBAN код на получателя. BIC (SWIFT) кодът не е задължителен за повечето трансакции.
 - Пълна сума: Прилага се правилото за споделени такси (SHA). Изпратената сума винаги пристига при получателя в пълен размер, без междинни банки да удържат такси..
- **Недостатъци:**
 - Само за Европа
 - Все още има банки в Европа, които не са интегрирали Instant SEPA
 - Задължително превалутиране към Евро
 - Лимит на сумата при Instant SEPA до 100 000 евро
 - По-слаба защита при Instant SEPA - веднъж изпратени, парите не могат да бъдат спрени или отменени от банката, ако е фишинг или измама.

Blockchain-SWIFT-SEPA

	Blockchain	SWIFT	SEPA
Правна сигурност и регулация	Не още	да	да
Стабилност на стойността	Търгуват се като стоки – търсенето определя цената	да	да
Такси за превалутиране	Да (gas fee)	да	Не (за Европа)
Масово приемане	Не още	да	Да
Глобален обхват	да	да	Не (само в Европа)
Наличие на банкови посредници	не	да	да
Постоянен достъп	да	не	Да (за незабавните)
скорост	До 30 минути според криптовалутата	1-4 работни дни	До 1 работен ден
Анонимност	Да	Не	Не
Обръщаемост на трансакциите	не	да	Да (за стандартните)

Стейблкоини

- Стейблкоини - криптовалути, обвързани с долара или еврото като USDT, USDC и EURC
- Предлагат стабилността на фиатните пари(традиционните валути) със скоростта и сигурността на блокчейн.
- Те се съвременни и не са се появили в 1-во поколение, а в 3-то и позволяват автоматизация с умни договори
- Поддържат фиксирано съотношение 1:1 с фиатна валута (например $1 \text{ USDT} = 1 \text{ USD}$)
- Инвеститорите ги използват, за да „заклучат“ печалбите си в стабилен актив, без да се налага физически да изтеглят парите си в традиционна банкова сметка.
- Това е критично важно за инвеститори в развиващи се страни или държави с хиперинфлация (като Аржентина, Венецуела, Турция), които нямат достъп до стабилни банкови системи.

Стейблкоини- рискове

- **Риск от загуба на фиксираната стойност - срив на съотношението 1:1**
- **Алгоритмичен риск** - TerraUSD (UST) се срина през 2022 г. и се обезцени до нула, така заличи милиарди долари на вложителите.
- **2. Риск от липса на реално обезпечение (Резерви)** - при масово теглене компанията може да не успее да изплати средствата ако няма резерви.
- **3. Централизация и риск от замразяване на активи** - компаниите зад масовите стейблкоини (като Tether и Circle) имат софтуерната възможност и законовото задължение да **замразяват адреси на портфейли** по искане на правителства или регулаторни органи. Така се губи достъп до средствата завинаги.
- **4. Регулаторен риск** - Ако даден стейблкоин бъде обявен за незаконен или не отговаря на MiCA, крипто борсите ще бъдат принудени да го премахнат, което ще затрудни продажбата му.
- **5. Риск от фалит на посредник или борса** - стейблкоините са на централизирана борса (като Binance, Crypto.com) или платформа за заемане, при фалит на платформата (както се случи с FTX), вложителите може да загубят активите си.
- **6. Технологичен риск (Смарт договори)** - ако в кода на договора или в т.нар. bridges между отделните мрежи има софтуерна уязвимост, хакери могат да откраднат обезпечението.

Второ поколение Blockchain

- Цел - Автоматизиране на споразумения и изграждане на финансови приложения без централен орган.
- Появяват се децентрализираните финанси (**DeFi**) и незаменяемите токени (**NFT**)
- Blockchain от регистър се превръща в програмируема платформа със **смайт договори** (самоизпълняващ се софтуерен код) и децентрализирани приложения (dApps)
- Появява се енергийно ефективния модел Proof of Stake (за пръв път в Ethereum)

Второ поколение Blockchain

приложения

- Поява на интелигентни договори в Ethereum Blockchain;
- Основният проблем на Blockchain - времето за мащабиране и обработка на транзакциите;
- Първоначално предлагане на капитал - Initial Coin Offering(ICO);
- Първоначално предлагане на обмен - Initial Exchange Offering (IEO).

Initial Coin Offering(ICO)

- Това е метод за групово финансиране (crowdfunding) в криптовалутния свят, при който нов проект продава свои собствени дигитални токени на инвеститори, за да събере капитал за развитието си.
- Риск - висок процент на измами (scams) и неуспешни проекти, в началото липсват строги регулации
- Рестрикции срещу ICO - Китай и Южна Корея (Септември 2017 г.) – пълна забрана; САЩ (2017-18 г.) класифицира по-голямата част от ICO токениите като **ценни книжа** (т.е. сложна и скъпа регистрация като акции на фондовата борса); Европа – MiCA не забранява ICO, но изисква публикуване на Whitepaper и самоличност

Initial Exchange Offering (IEO)

- **IEO** - Първоначално предлагане за обмен е модел за групово финансиране, при който крипто проект продава своите токени не директно както при ICO, а чрез посредничеството на утвърдена крипто борса.
- Борсата (напр. Binance) управлява продажбите, проверява легитимността на проекта и листва токена веднага след приключване на кампанията
- Тя гарантира, че не става въпрос за явна измама.
- Затихва през 2021-2022г. Т.к. борси като Binance преминават към Launchpools (Стейкинг), появява се IDO и MiCA налага строг контрол над платформите, предлагащи подобни услуги

ІЕО – предимства и недостатъци

- Предимства:
 - По-високо доверие за инвеститорите
 - Токените се появяват за продажба веднага след края на продажбата
 - Потребителите купуват токените директно от интерфейса на борсата
 - Проектите получават готова база от потенциални потребители
 - Борсата рекламира събитието
- Недостатъци:
 - Изключително високи такси за проектите
 - Борсата противоречи на децентрализацията на блокчейна
 - Инвеститорите задължително трябва да преминат през идентификация (KYC) на съответната борса и спират инвеститори от Китай или САЩ, които имат рестрикции
 - Няма гаранция за печалба
 - Изискване за притежание на токени на самата борса (например BNB за Binance)

Initial DEX Offering (IDO)

- Съвременен модел за групово финансиране в крипто сферата, при който нов проект пуска и продава своите токени чрез **децентрализирана борса (DEX)** или специализирани децентрализирани платформи (т.нар. Launchpads) като *Polkastarter*, *DAO Maker*, *Seedify* и др.
- Потребителите участват директно през свои лични портфейли (като MetaMask, Trust Wallet, Phantom), без да депозират средства в чужди платформи.
- Няма централизиран посредник – борса, а се управлява от умен договор
- Потребителите сами поемат риска, но смарт договорите автоматично разпределят токениите.

IDO – предимства и недостатъци

- Предимства
 - Равен старт за инвеститорите
 - Self-Custody – средствата са в портфейла до момента на трансакцията и фалит на платформата не може да се случи
 - Незабавна търговия с токени след края на набирането на средства
 - Ниски разходи за проектите
 - Гъвкавост и бързина при отключване на токените
- Недостатъци
 - Rug Pulls – по-висок риск от измами с фалшиви проекти, за да се изтеглят парите на инвеститорите
 - Сложен достъп за малки инвеститори
 - Технологичен риск от софтуерни грешки в умния договор или хакерски атаки
 - Наличие на такси за трансакции
 - Няма клиентска поддръжка при проблемни трансакции

IDO днес

- Появата на IDO 2021г. го прави най-предпочитан формат за публично набиране на средства от нови Web3 и крипто проекти
- Активни платформи са **DAO Maker**, **Polkastarter**, **Seedify** и **TrustSwap**
- Подбор на проекти по умните договори и идентификация на екипите
- Въвеждат се политики за възстановяване на средства
- Изискването за пълна идентификация намалява предимството на анонимността на децентрализираните приложения
- Новите токени имат ниска доходност
- Инвеститорите предпочитат Launchpool

Launchpool платформи

- **Launchpool (Пул за стартиране)** е иновативен модел за разпределение на криптовалюти, който позволява на потребителите да получават безплатно нови токени в замяна на временно "заклучване" (стейкване) на свои съществуващи крипто активи.
- Появява се 2020г. от Binance през "DeFi лято" (появата на децентрализираните финанси)
- Не се изисква покупка за разлика от ICO, IEO и IDO, а се заключва свой актив за 3-30 дни. Умния договор изчислява наградите за час.
- Натрупаните награди се дават като пасивен доход (Yield Farming), а първоначално стейкнатите активи се връщат в пълен размер на потребителя
- Потребителят може да прекрати стейкинга и да изтегли парите си по всяко време без наказателни такси.

Launchpool – предимства и недостатъци

- Предимства
 - Нулев директен риск за капитала
 - Гъвкавост и ликвидност - позволяват да "отключване" (unstake) на активите си за броени секунди, при нужда от тях за спешна търговия.
 - Гарантирано листване на борсата
 - Пасивен доход от "спящи" активи
- Недостатъци
 - Минимална доходност за малки капитали
 - Риск от спад на стейкнатия актив
 - Екстремна волатилност при старта-първоначален скок, последван от бърза разпродажба от страна на участниците
 - Пропуснати ползи (Opportunity Cost) докато активите са заключени в пула

Интелигентни договори

- Умните договори представляват самоизпълняващи се програми, които работят върху блокчейн мрежа.
- Предназначени са да улесняват, проверят и наложат условията при изпълнението на договор между две или повече страни, без нуждата от посредници.
- Умните договори са компютърни програми, съхранявани на блокчейните и изпълняващи се автоматично, при определни обстоятелства.
- Умните договори могат да автоматизират някои процеси, като плащане и потвърждения за събития, което увеличава ефикасността на системата и намалява разходите на бизнеса.

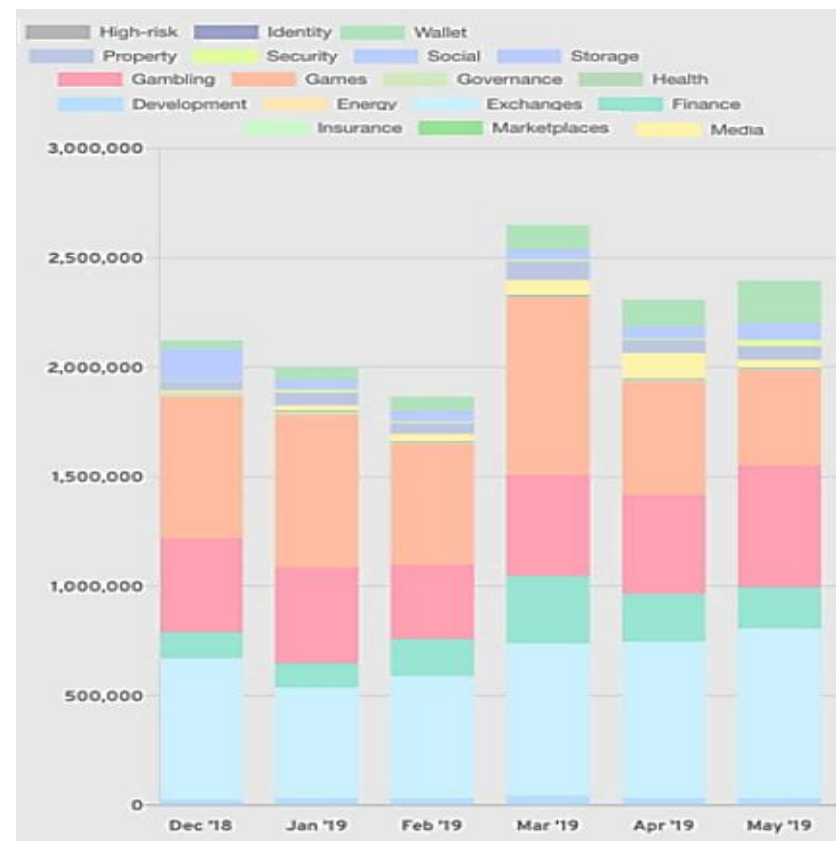
Трето поколение Blockchain

- Цел – постигане на баланс между децентрализация, сигурност и мащабируемост.
- Използване на усъвършенствани консенсусни протоколи като **Proof of Stake (PoS)** и **Delegated Proof of Stake (DPoS)**
- Преодоляване на високите такси, ниската скорост и въвеждане на крос-чейн (cross-chain) комуникация между различни мрежи.
- Примери - Cardano, EOS, Polkadot и Solana

Трето поколение Blockchain

приложения

- Нови приложения на Blockchain технологията – частни и публични решения;
- Интелигентните договори могат да бъдат разработени и внедрени в различни Blockchain платформи.



Четвърто поколение Blockchain

- Цел - пълна интеграция на blockchain в реалния бизнес, глобалната икономика и концепцията за децентрализиран Интернет (Web3)
- Лесно внедряване на блокчейн в корпоративни процеси, изкуствен интелект (AI) и Интернет на обектите (IoT).
- Поява на частни и хибридни блокчейн мрежи,
- висока скорост,
- Сигурност от институционален клас
- Пълно съответствие с европейските регулации digital-strategy.ec.europa.eu.
- Примери - Hyperledger, Avalanche, EBSI

Хибридни платформи - Avalanche

- **Основната мрежа на Avalanche** е публичен, децентрализиран блокчейн с отворен код, но платформата позволява създаването на напълно частни и корпоративни подмрежи (Subnets / Avalanche L1s)
- Всеки потребител може да купува, продава и превежда токена AVAX.
- Всеки разработчик може да създава децентрализирани приложения (dApps).
- Основната мрежа е съставена от 3 вградени блокчейна (X-Chain, P-Chain и C-Chain), които са публични и прозрачни.
- **Възможността за Частни подмрежи** (Evergreen Subnets / Avalanche L1s) - може да стартира собствена изолирана подмрежа в рамките на Avalanche
- Предлага:
 - контролиран достъп: Само одобрени (KYC/верифицирани) потребители или валидатори могат да имат достъп до мрежата.
 - Конфиденциалност на данните
 - Собствени правила - Бизнесът може сам да определи какви да бъдат таксите, какъв токен да се използва за газ и кои закони и регулации да се спазват

Други хибридни платформи

- **Cosmos** - Това е мрежа от независими блокчейни, наречени "зони", които се свързват помежду си. Чрез инструмента Cosmos SDK, компаниите могат да създават напълно частни или публични блокчейни (App-Chains), които имат собствени правила, но могат лесно да комуникират с останалата част от екосистемата.
- **Polkadot** - Използва подобна структура, наречена "парачейни" (Parachains). Основната мрежа осигурява сигурност, докато отделните парачейни могат да бъдат конфигурирани като частни, корпоративни мрежи със специфични правила за достъп.
- **Polygon** - Платформата предлага Polygon CDK (Chain Development Kit), който позволява на бизнесите да разработват свои собствени Layer 2 мрежи. Те могат да бъдат изцяло частни (за вътрешни банкови или корпоративни нужди) с контролиран достъп, но свързани с публичната мрежа на Ethereum за допълнителна сигурност.

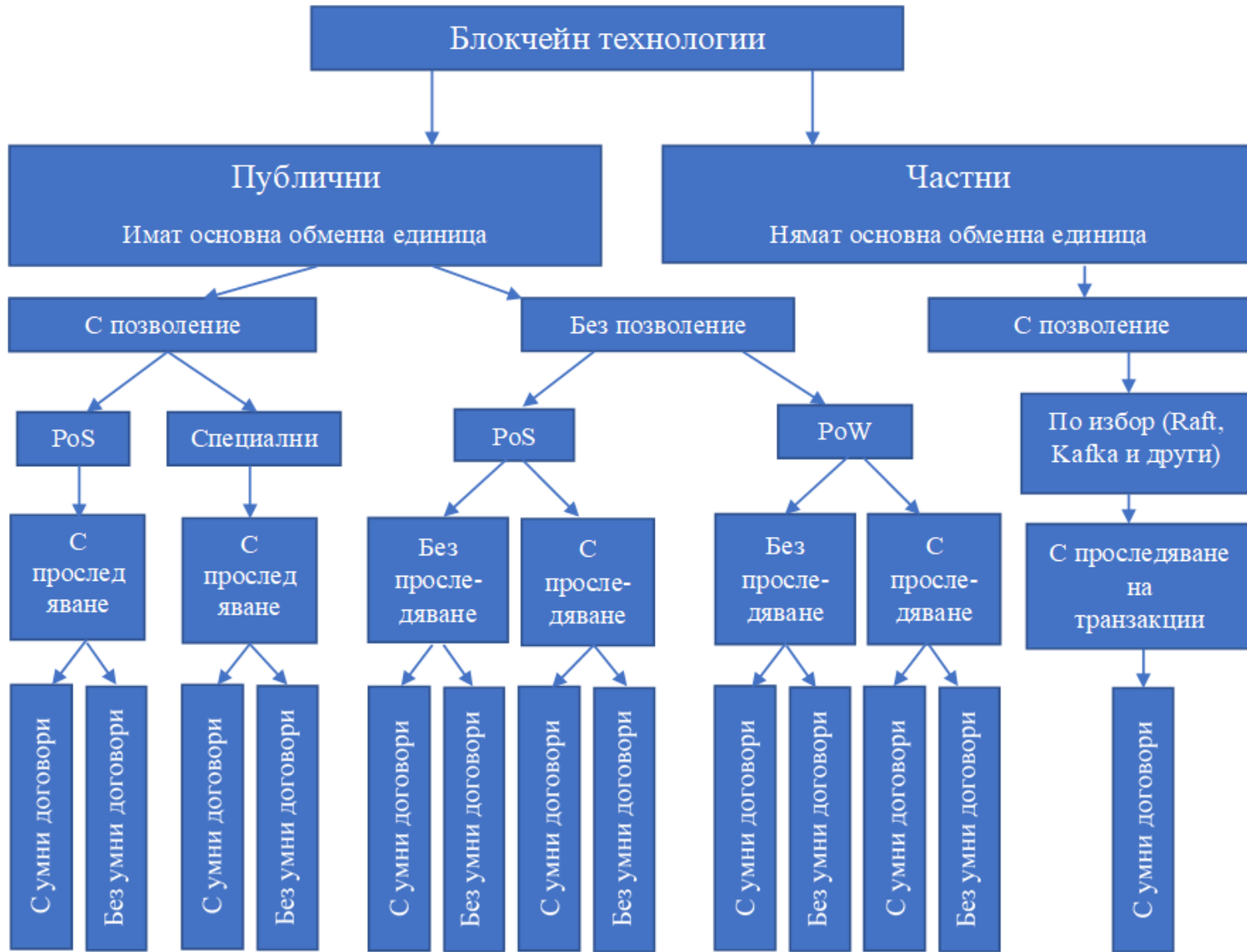
Частни – Hyper Ledger Fabric

- Проект на Linux Foundation & IBM
- Hyperledger не е публичен блокчейн, а изцяло корпоративна рамка с отворен код.
- Тя е създадена изключително за изграждане на частни мрежи с разрешение за достъп (permissioned), където само одобрени участници могат да виждат и записват трансакции.

Други частни blockchain

- **R3 Corda** - Специализиран за финансовия сектор, но е DLT, а не blockchain
- Hyperledger Besu & GoQuorum (Частният Ethereum) - базирани на кода на публичния Ethereum, но модифицирани за частни корпоративни мрежи. Зад тях стои Enterprise Ethereum Alliance
- **Canton Network** (Блокчейнът на институциите) - частна мрежа, създадена от компанията Digital Asset. Тя осигурява абсолютна поверителност на данните между различните финансови институции, като същевременно им позволява да си разменят активи без риск от изтичане на търговска тайна..

Класификация на Blockchain

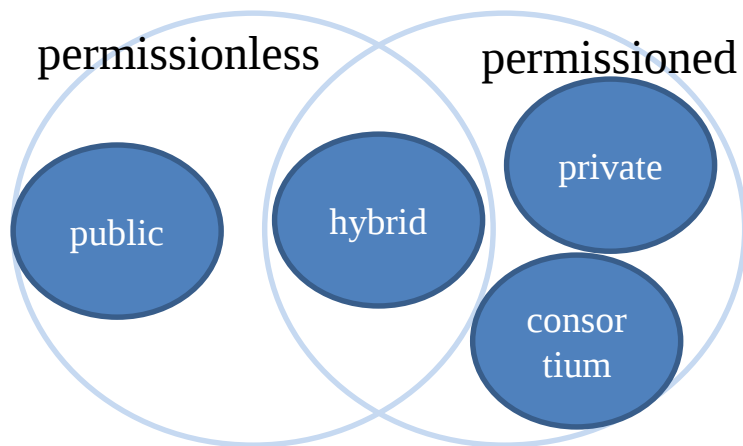


Публични и частни Blockchain

- Частният Blockchain е по-доброто решение за бизнеса:
 - доверени възли;
 - няма изискване за консенсусен протокол;
 - предлага бърз достъп до информация;
 - по-евтини транзакции;
 - контрол на ниво поверителност.



С позволения и без позволения



- **Публичен Блокчейн**

- децентрализирана мрежа, към която всеки може да се присъедини и да участва в нея
- всички възли имат равен достъп до блоковата верига за добавяне на нови блокове от данни и за валидиране на съществуващи блокове от данни.

- **Частен Блокчейн**

- централизирани и управлявани от лице или организация, която решава кой може да има достъп до блокчейна и да бъде добавен като възел.
- Трансакциите в частната блок верига не са публично видими, но се проверяват чрез процес на консенсус между членовете на мрежата.

- **Хибриден блокчейн**

- споделя публично определена информация, като същевременно запазва друга информация поверителна.

Популярни блокчейни-криптовалути

Таблица 1. Сравнение на едни от най-популярните блокчейн технологии

Блокчейн	Достъп на участниците до мрежата	Консенсусен механизъм	Основна обменна единица	Проследяване на транзакциите	Умни договори
Bitcoin (BTC)	Публичен, без позволение	PoW	Да Максимум:21млн	Да	Не
Ripple	Публичен, с позволение	RPCA	Да ∞	Да	Не
Ethereum(ETH)	Публичен, без позволение	PoW	Да ∞	Да	Да
Litecoin(LTC)	Публичен, без позволение	PoW	Да Максимум:84млн	Да	Не
Cardano(ADA)	Публичен, с позволение	PoS	Да Максимум:45млрд	Да	Да
EOS (EOS)	Публичен, с позволение	DPoS	Да ∞	Да	Да
Monero(XMR)	Публичен, без позволение	PoW	Да ∞	Не	Не
TRON (TRX)	Публичен, с позволение	PoS	Да ∞	Да	Да
Stellar(XLM)	Публичен, с позволение	The Stellar Consensus Protocol (SCP)	Да ∞	Да	Да
Neo(NEO)	Публичен, с позволение	dBFT	Да Максимум:100млн	Да	Да
Zcash(ZEC)	Публичен, без позволение	PoW	Да Максимум:21млн	Не	Не
Hyperledger Fabric	Частен	Raft, Kafka	Няма	Да	Да
Corda	Частен	По избор	Няма	Да	Да

Криптовалути

- В момента има над 17 400 активни криптовалути
- Липса на централен емитент
- Малък сектор от глобалните финанси
- Активи за съхраняване на стойност
- Проблеми – сигурност, надеждност...
- Реализират се с блок-чейн технология – **публичен** регистър на криптосметките и сделките с криптовалути.
- Сделките се извършват p2p – директно между двамата участници без посредници
- От края на 2017г Чикагската финансова борса SWOT търгува с финансови инструменти, базирани на биткойни.
- През 2008г. 1 биткойн е струвал няколко цента. През август 2017г. 1 биткойн = 2730\$. На 30.09.2018 1 биткойн = 6602\$
- На 29.07.2020 1 биткойн = 11112.79\$
- На 28.07.2026 1 биткойн = 63453.94\$

https://coinmarketcap.com/ (22.07.2026)

CoinMarketCap

CryptocurrenciesDashboardsDexScanExchangesCommunityMore

PortfolioWatchlist

Search

Log In

Top

Trending

Watchlist

Stocks

Prediction Markets

Most Visited

New

Gainers

More

Market Cap >

\$2.25T ▼ 0.51%

CMC20 >

\$134.29 ▼ 0.69%

Fear & Greed >

Altcoin Season >

50/100

Average Crypto RSI >

51.3

Rei Researcher · 2h

\$BTC TBBI is in a Very Low Sentiment Zone

Topic Trump rumor: Clarity odds 32% → 43%

New Top News

Add AI alert

Russia passes sweeping crypto regulation framework

Are altcoins outperforming Bitcoin?

All Networks

BSC

Solana

Base

Ethereum

More

Market Cap

Volume(24h)

Filters

Columns

#	Name	Price	1h %	24h %	7d %	Market Cap	Volume(24h)	Circulating Supply	7d Price%
	CoinMarketCap 20 Index DTF	\$133.47	▼ 0.00%	▼ 0.25%	▲ 1.90%	\$6.28M	\$1.3M	47.08K CMC20	
1	Bitcoin BTC	\$65,854.46	▼ 0.19%	▼ 0.71%	▲ 1.93%	\$1.32T	\$32.42B	20.05M BTC	
2	Ethereum ETH	\$1,923.31	▼ 0.30%	▼ 0.52%	▲ 2.31%	\$232.11B	\$10.66B	120.68M ETH	
3	Tether USDT	\$0.9992	▲ 0.02%	▲ 0.00%	▲ 0.02%	\$184.08B	\$59.74B	184.22B USDT	
4	BNB BNB	\$569.96	▼ 0.01%	▼ 1.13%	▼ 1.39%	\$75.89B	\$1.02B	133.16M BNB	
5	USDC USDC	\$0.9998	▲ 0.00%	▼ 0.00%	▲ 0.02%	\$73.13B	\$9.35B	73.14B USDC	
6	XRP XRP	\$					\$1.38B	62.46B XRP	

Ask CMC AI

Shift + /

Bitcoin- криптовалута



- Съзателят на Биткойн е японският програмист Сатоши Накамото.
- Появява се 2008г.
- Биткойн е първата по рода си дигитална валута, която притежава качества липсващи при всички останали валути познати на човечеството до сега:
 - **Липса на централна институция** или орган, който да я контролира или обслужва.
 - **Цената** се определя единствено от търсенето и предлагането.
 - Работи на принципа **peer-to-peer (p2p)**- всички транзакции се извършват между самите участници без посредничество от трета страна. По този начин транзакциите се извършват много бързо и без допълнителни разходи.
 - **Анонимност.** Благодарение на p2p принципа, идентифицирането на участниците в Биткойн системата е много трудно.
 - **Сигурност.** Биткойн транзакциите са напълно сигурни и необратими, като цялото функциониране се базира на сложни криптографски алгоритми, което е и същността на Биткойн.
 - **Производство и самоконтрол** - всеки може да я произвежда самостоятелно. Това става като се използва изчислителна мощ, която пък от своя страна е необходима за функционирането на системата. Всеки който се включи в „производството“ бива възнаграждаван с биткойни.

Bitcoin продажби

- Към 2014 в обръщение има над 12 милиона биткойни, като на всеки 10 минути се създават приблизително 25 биткойна.
- Общото им количество има установена горна граница от 21 милиона и на всеки четири години скоростта на добиване се намалява наполовина. Това означава, че нови биткойни ще продължат да се създават в бъдещите сто години.
- През юни 2014 търговската марка Bitcoin, регистрирана в Япония и Европейския съюз, е обявена за продажба.
- Биткойн работи единствено с пълното съгласие и единодушие на всички потребители, поради което промяната на протокола е много трудна и изисква преобладаващото мнозинство да приеме промените по такъв начин, че останалите потребители да нямат никаква друга възможност, освен да ги последват.
- WordPress налагат плащания с bitcoin.

Bitcoin- употреба

- **Биткойн клиент** – софтуерът с отворен код , който представлява личен Биткойн портфейл.
- Достъпен е безплатно на официалния сайт <http://bitcoin.org>.
- **Цената** на койните се формира от големите борси, функциониращи на международно ниво, а към актуалната цена се прибавя малка надценка от локалната борса
- Т.к. това не е официално призната валута, се третира като стока, с която се търгува и **трябва да се платят данъци** върху продажбите ѝ.
- Съхраняването на капитали в Bitcoin е голям **риск**, т.к. цената ѝ варира постоянно в широки граници поради нисколиквидни пазари, затова ако се получават плащания с Bitcoin, трябва да се обръщат в местна реална валута.
- **Биткойн** (с главно Б) с обществено достъпен списък на всички извършени транзакции, наречен блокова верига (*block chain*). Тя се записва като файл на всеки компютър, свързан с Биткойн мрежата.
- Валутата **биткойн** (с малко б) е балансът по индивидуалната сметка. Това позволява на всеки потребител да провери (валидира) валидността на всяка транзакция.
- За функционирането и защитата на платежната система се използват криптографски методи, а автентичността на всички транзакции е защитена с цифрови подписи.

Добиване(mining) на bitcoin

- Създават се като възнаграждение за извършена изчислителна работа по криптиране.
- При всеки успешно преминат етап на изчисление на масив от големи числа (хеширане) се получават по 25 биткойна. Участниците в изчисленията обаче обикновено са повече от един и биткойните се делят помежду им, в зависимост от тяхното участие.
- Популярни програми за добив са: CGminer и BFGminer.

Е-търговия с bitcoin

- **Биткойн фосет сайтове** - подаряват биткойни (или други крипто валути) на всеки свой посетител за всяко негово посещение в рамките на определено време – най-често между 5 минути и 1 час.
- Идеята на фосет сайтовете е показване на банери срещу заплащане (на момента или 1 път седмично).
- Примери:
 - <https://cointiply.com/>
 - <https://firefaucet.win/>
 - <https://faucetpay.io/>
 - <https://www.coinpayu.com/>

Bitcoin портфейл

- Bitcoin портфейлът е съвкупност от множество биткойн адреси, в които може да се съхраняват различни баланси от биткойни.
- Bitcoin портфейлите са софтуерни програми, които дават възможност за лесно управление на биткойни, без да е необходимо техническо познаване на биткойн протокола.
- Потребителите могат да се сдобиват с нови bitcoin адреси, които се съхраняват в портфейл с линкове към криптографски пароли или „частни ключове“, които осигуряват достъп до трансфер на биткойни
- За всеки потребител, който си инсталира BitCoin софтуера, се генерира виртуален портфейл.

Bitcoin cash



- Bitcoin cash – създадена юли 2017г. след разделяне на bitcoin, което е известно като „голямата ножица” (hard fork).
- Притежателите на bitcoin в този момент получиха безплатни токени bitcoin cash.
- Много разработчици са притеснени от дългото време за транзакции на мрежата за bitcoin. Затова те предлагат решение, което ще повиши размера на всяка транзакция, но след това ще се увеличи скоростта.
- Не цялата общност обаче е съгласна с предложението, затова се стига и до разделянето на двете валути.
- Групата зад bitcoin cash казва, че сега транзакциите са по-бързи, отколкото при оригиналния bitcoin.

Ether



- Блокчейн технологията Етериум се появи
- Ethereum - блокчейн компания, създава виртуалната валута Ether.
- Ether също се базира на блокчейн технология, като bitcoin, но има специална цел- т.нар. умни договори.
- Умният договор е записан със специален код в блокчейн. Веднъж, след като всяка от страните одобри условията на договора, сделката се изпълнява.
- Консорциумът Enterprise Ethereum Alliance, в който влизат компании като Microsoft и JPMorgan, разработва различни приложения за употребата на блокчейна на Ethereum.
- 96 308 851 броя етери циркулират в обращение, като това е и максималният заложен брой.

Ripple = XRP



- Блокчейн системата Ripple и криптовалутата, нея - XRP, се зараждат през 2012 г.
- В системата е предвидено да циркулират 100 000 000 000 XRP
- Ripple се представя като трансгранично решение за плащания за големи финансови институции, базирано на блокчейн технология.
- Ripple стартира с редица финансови институции, сред които American Express и Santander.
- Ripple (XRP), може да се използва от фирми, за да се получи незабавна ликвидност, необходима в сделка с висока стойност, без да се налага да се плащат такси.
- XRP действа като мост между одобрените валути по време на сделка.
- Транзакциите в XRP могат да бъдат уредени в рамките на четири секунди, по-бързо от която и да е голяма криптовалута към края на 2017г.

Litecoin



- Litecoin се появява през 2011 г.
- Litecoin е най-близкият съперник на Bitcoin и се използва за плащания, защото е по-бърза от Bitcoin.
- Litecoin транзакциите отнемат малко повече от две минути, в сравнение със средно около 300 минути за bitcoin.
- Налице е ограничено предлагане на 84 млн. Litecoin, в сравнение с 21 млн. bitcoin.
- Litecoin е насочен повече към плащания, по-бързи транзакции и по-ниски такси.

Публични blockchain с умни договори

- Децентрализирани и прозрачни мрежи, които позволяват на всеки разработчик да създаде умен договор.
- **Ethereum (ETH)**: Пионерът и най-голямата платформа за смарт договори в света. Използва езика за програмиране Solidity и виртуалната машина EVM. Тя е стандартът за DeFi и NFT.
- **Solana (SOL)**: Известна със своята изключително висока скорост (хиляди трансакции в секунда) и ниски такси. Смарт договорите тук (наричани програми) се пишат основно на езика Rust.
- **Cardano (ADA)**: Платформа, фокусирана върху сигурността и научния подход. Използва езика Plutus (базиран на Haskell), който позволява математическо доказване на коректността на кода, намалявайки риска от грешки.
- **BNB Chain (BNB)**: Силно скалируема мрежа, напълно съвместима с EVM на Ethereum. Тя предлага бързо изпълнение и ниски разходи, което я прави много популярна за потребителски приложения.
- **Avalanche (AVAX) - C-Chain**: Специфичното ядро (Contract Chain) на Avalanche е изцяло предназначено за смарт договори и работи с EVM, съчетавайки бърз консенсус с позната среда за разработчици.

Частни blockchain с умни договори

- Техните умни договори се изпълняват само между одобрени участници.
- **Hyperledger Fabric:** Позволява писането на смарт договори (наричани chaincode) на стандартни езици като Go, Java и JavaScript. Договорите могат да бъдат скрити в частни канали за конфиденциалност.
- **R3 Corda:** Нейните смарт договори са уникални, защото съчетават софтуерен код с традиционен правен текст (т.нар. Ricardian Contracts), което ги прави юридически обвързващи за финансовите институции. (но е DLT, а не blockchain)
- **Hyperledger Besu / GoQuorum:** Частни версии на Ethereum, които поддържат същите смарт договори (Solidity/EVM), но работят в затворени корпоративни мрежи с криптиране на трансакциите.

Въпроси ?

Благодаря за вниманието !