

Blockchain и Distributed Ledger технологии. Правна регламентация

проф. д-р инж. Венета Алексиева

ОСНОВНИ МОМЕНТИ

- Указания за изпита
- Същност на дисциплината “Blockchain технологии”
- Дефиниции – DLT, Blockchain Криптовалути, DAG и Tempo
- Blockchain и Big Data
- Предимства и недостатъци на Blockchain
- Правни аспекти на Blockchain

Изпит задочно обучение

- Време за работа:
 - 90 минути
- Формат:
 - Тестът съдържа 35 въпроса.
 - Въпросите са с един или няколко отговора.
 - Навигацията е само напред и не може да се връща към преминал въпрос, независимо дали е посочен отговор или не.
- Оценяване:
 - До 30 точки от текущ контрол от упражнения
 - До 70 точки от изпита
- Конспект и презентации:
 - На cs.tu-varna.bg
- Консултации:
 - Обявени пред 207-4Е

Изпит редовно обучение

- Време за работа:
 - 40 минути
- Формат:
 - Тестът съдържа 20 въпроса.
 - Въпросите са с един или няколко отговора.
 - Навигацията е само напред и не може да се връща към преминат въпрос, независимо дали е посочен отговор или не.
- Оценяване:
 - До 60 точки от текущ контрол от упражнения
 - До 40 точки от изпита
- Конспект:
 - На cs.tu-varna.bg

Упражненията

Няма ръководство:

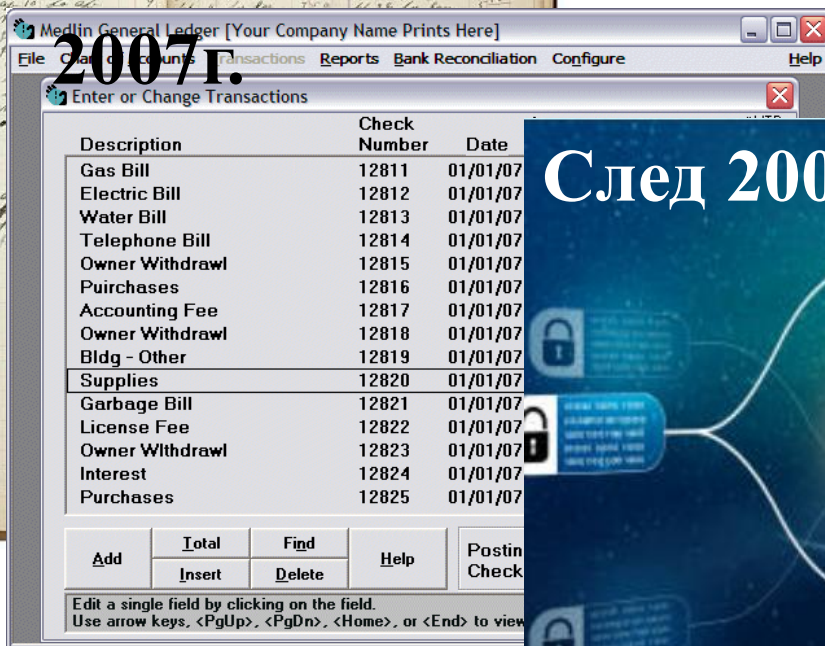
- Указания в MSTeams

Текущ контрол:

- Изработване на система с HyperLedger Fabric на VM в ТУ
- Достъп до VM само от ТУ в рамките на упражнението
- Общо – до 60 т. за РО и до 30т. за ЗО
(критериите се дават на упражнения)

Основни дефиниции

- **DLT** - дистрибутиран регистър на трансакции, който се управлява от P2P мрежи с помощта на алгоритми за консенсус. Чрез тях потребителите на мрежата постигат съгласие при валидирането на записите.



След 2008г.

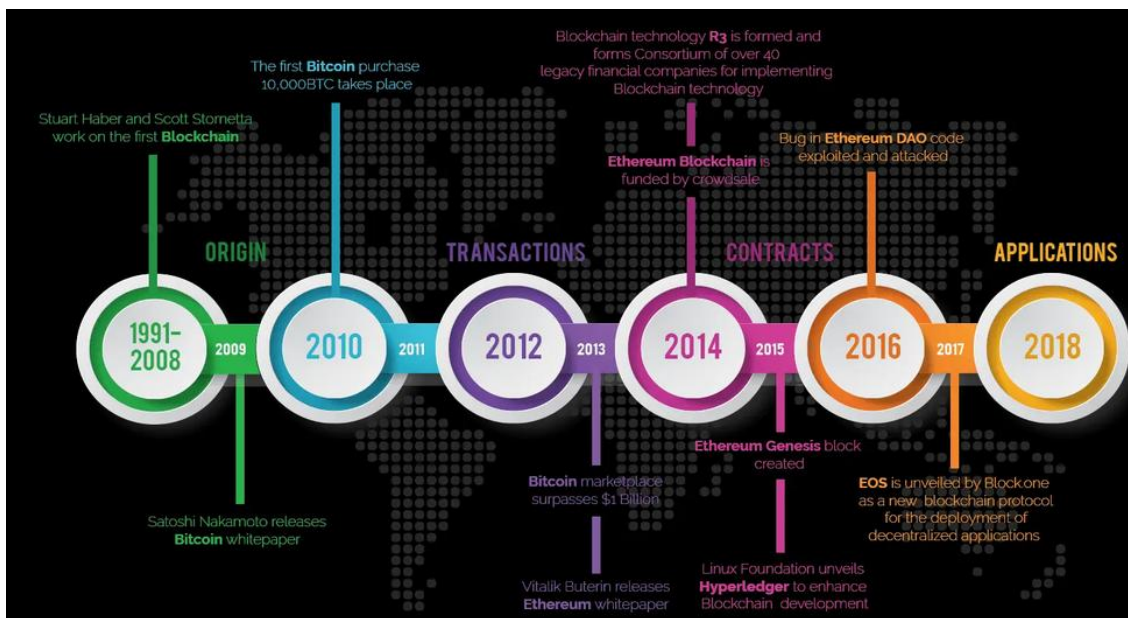


Основни дефиниции

- **Блокчейн** - децентрализирана система (база данни) за сигурно и прозрачно записване на трансакции в блокове. Тези записи не могат да бъдат лесно променяни и фалшифицирани.

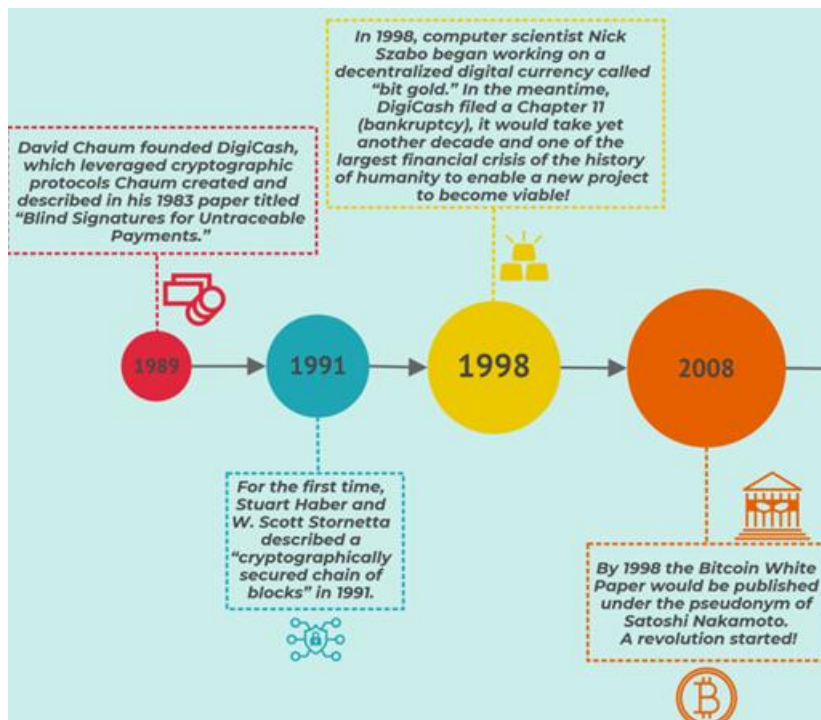
<https://blockchain.mit.edu/how-blockchain-works/>

<https://101blockchains.com/history-of-blockchain-timeline/>



Основни дефиниции

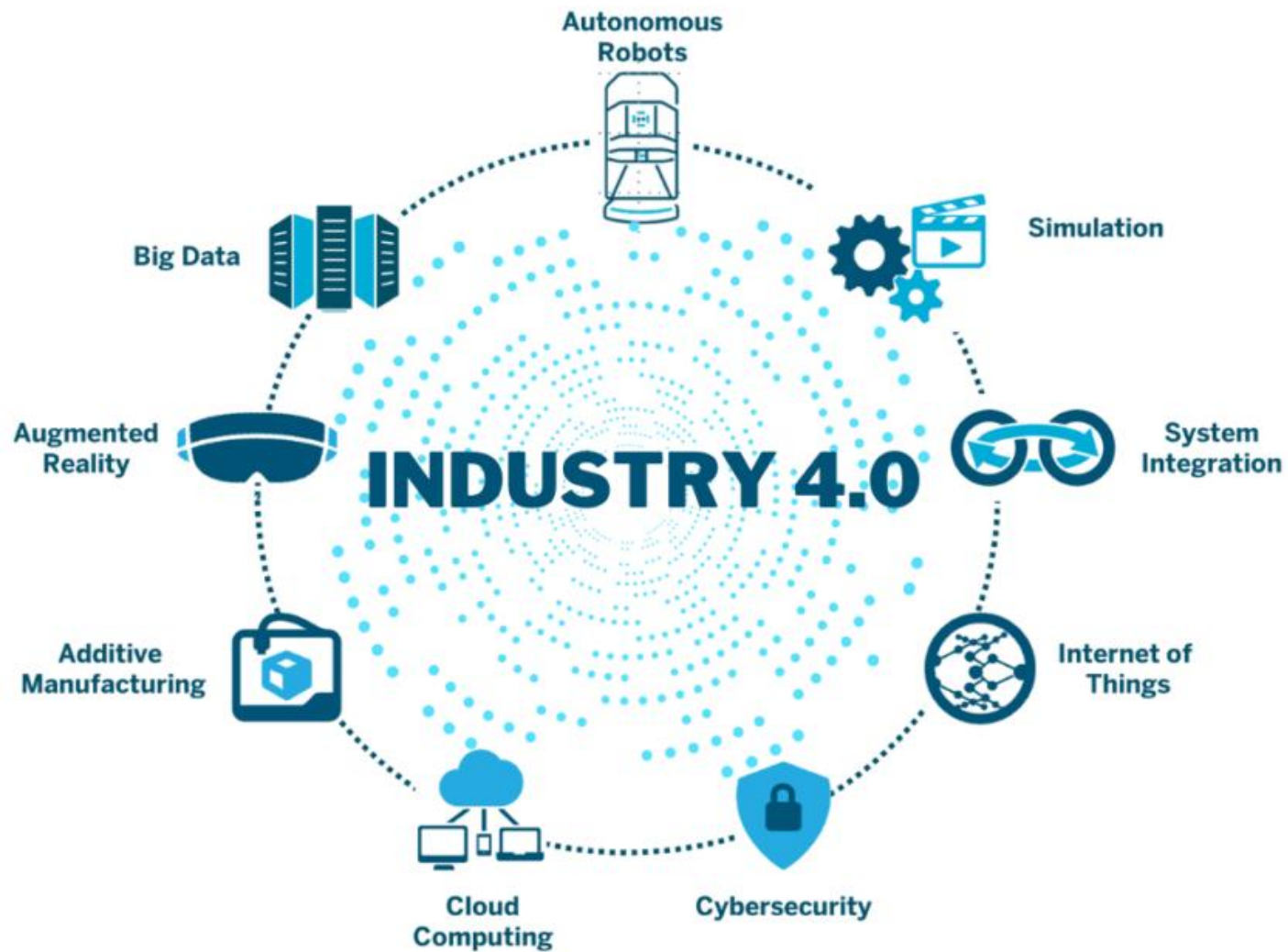
- **Криптовалута**- дигитална валута, която функционира като средство за размяна. Тя използва силно криптиране за защита на трансакциите и децентрализирана блокчейн технология, за да записва и проверява преводите, без да разчита на централни банки или финансови институции.



Характеристики

	Distributed Ledger Technology	Blockchain	Cryptocurrency
същност	Технологична архитектура – БД, репликирана на множество компютри, като чрез консенсусен механизъм участниците одобряват актуализациите заедно	Конкретна форма на DLT	Дигитален актив, използващ блокчейн
структура на данните	Споделен разпределен регистър	Последователни блокове, като всеки нов съдържа хронологичен отпечатък от предходния	Трансакционни записи в блокчейн
управление	Не изисква криптовалута или токен	Може да съществува с и без токен (публични и частни)	Публично достъпна за търговия
приложение	от банкови консорциуми и корпорации	Бизнес приложения, криптовалута, дигитална идентичност, здравеопазване	Дигитално средство за размяна, съхранение на стойност

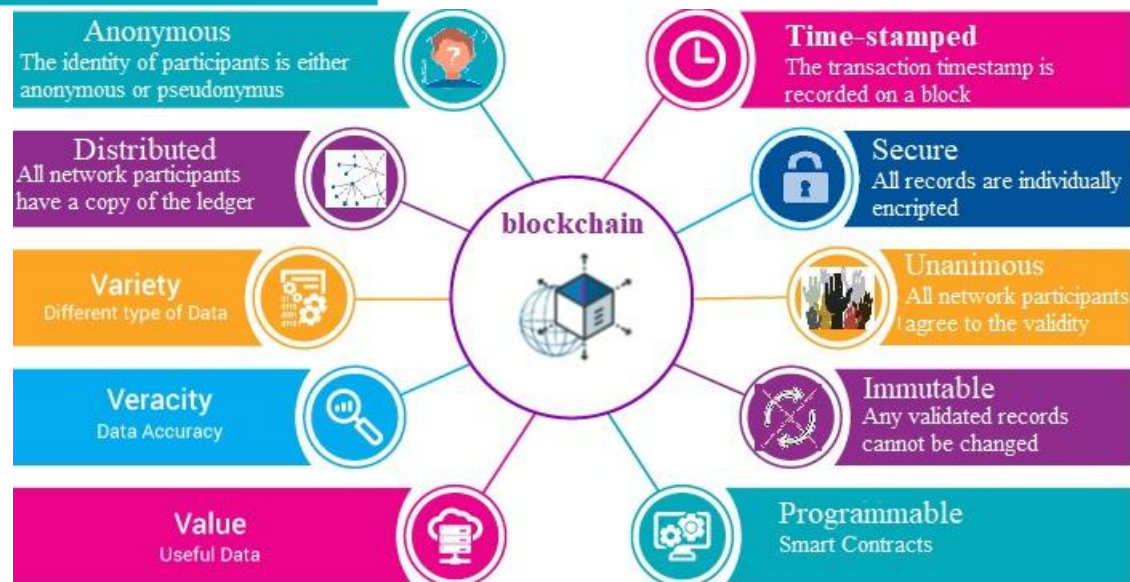
Big Data и Blockchain



Развитието на Интернет и блокчейн

- Web 1.0 (само за четене) - приблизително от 1991 до 2004 г е– статични страници, без възможност за коментари или създаване на собствено съдържание, прост дизайн, търсене чрез уеб указатели и каталози
- Web 2.0 (четене-писане) - 2004 г. до днес – потребителите сами създават съдържанието – клипове, блогове, статии, появяват се социални мрежи, интерактивност- харесване, споделяне, коментари, облачни услуги и адаптивен дизайн
- Web 3.0 (четене-писане-притежаване), където блокчейни с умни договори, NFT и криптовалутите са ключови в прехода от централизирани към децентрализирани уеб модели, липса на цензура, без посредници, потребителите притежават своите дигитални активи и данни чрез криптографски ключове и токени, ИИ за контекста на търсената информация.

Big Data и Blockchain



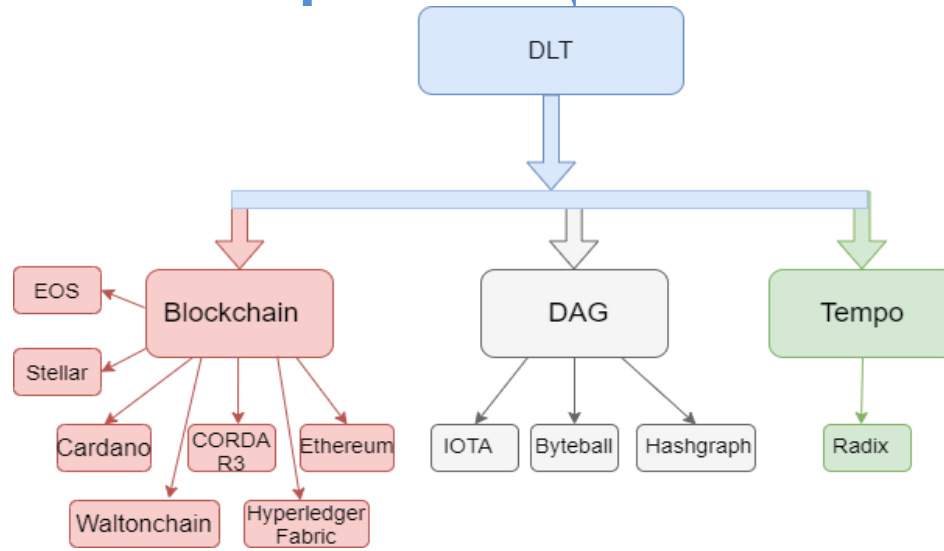
Бази данни и Blockchain

	Бази данни	blockchain
Структура на данните	В таблици, еднотипни	В блокове, разнородни
Промяна на записите	Лесна, без следа, контролирано от администратора на БД	След запис в блок е невъзможно
съхранение	централизирано	Децентрализирано, разпределено
Изтриване на данни	Лесно, без следа, контролирано от администратора на БД	След запис в блок е невъзможно
Сигурност	чрез пароли, защитни стени и други мерки за сигурност	Висока сигурност, С криптиране
Проследяване на оригиналните данни	Невъзможно, ако няма одитни следи	лесно
контрол	1 точка за достъп	Всеки пиър вижда цялата верига записи

Distributed Ledger Technology (DLT)

- Системата, изградена на базата на DLT, събира и предава данни на различни обекти, които са с разпределена структура.
- “Ledger” означава „регистър (разпределена книга)“, в който се отчита промяната на състоянието на обектите.
- Съществуват няколко регистъра, които притежават идентични записи от обекти.
- Разпределената инфраструктурата се характеризира с:
 - Способност за съхраняване, записване и обмен на информация между участници без да е необходим централен архитект (т.е. peer-to-peer) и доверие между тях при ясно определен източник.
 - Осигурена липса на „дублиран разход“ (т.е. едни и същи данни или маркер не могат да бъдат изпращани на множество страни)

Класификация на DLT



- DL е технология за съхраняване, синхронизиране и споделяне на данни между множество разпределени хранилища за данни (възли).
- Всеки възел действа едновременно и като клиент, и като сървър, като държи едно и също копие на разпределения регистър.
- Има три основни архитектури: blockchain, Directed Acyclic Graph (DAG) и Tempo

DLT

Параметър за сравнение	Blockchain	DAG	Tempo
Структура на данните	Свързани чрез хеш функция блокове	Топологично подредени насочени графи	Разпределена с консенсусен механизъм
тип	Публичен/ частен	частен	публичен
Време за верификация (проверка)	Няколко минути	Минути	< 5 s
Приложения	Bitcoin, Corda, Litecoin, Ripple, Ethereum и други	IOTA, Byteball, Raiblocks, Hashgraph, Hylochain	RadixDLT
Масшабируемост	ниска	висока	висока
Конфиденциалност	Разрешени и без разрешение	липсва	липсва
Такса за транзакция	висока	ниска	ниска
Процес на добиване	Изисква се	Не се изисква	Не се изисква
Консумация на енергия	Висока консумация при добиване	Ниска, при липса на добив	Ниска, при липса на добив
Популярност	Старт 2008	Старт 2017	Старт 2018

Критерии за избор на DLT

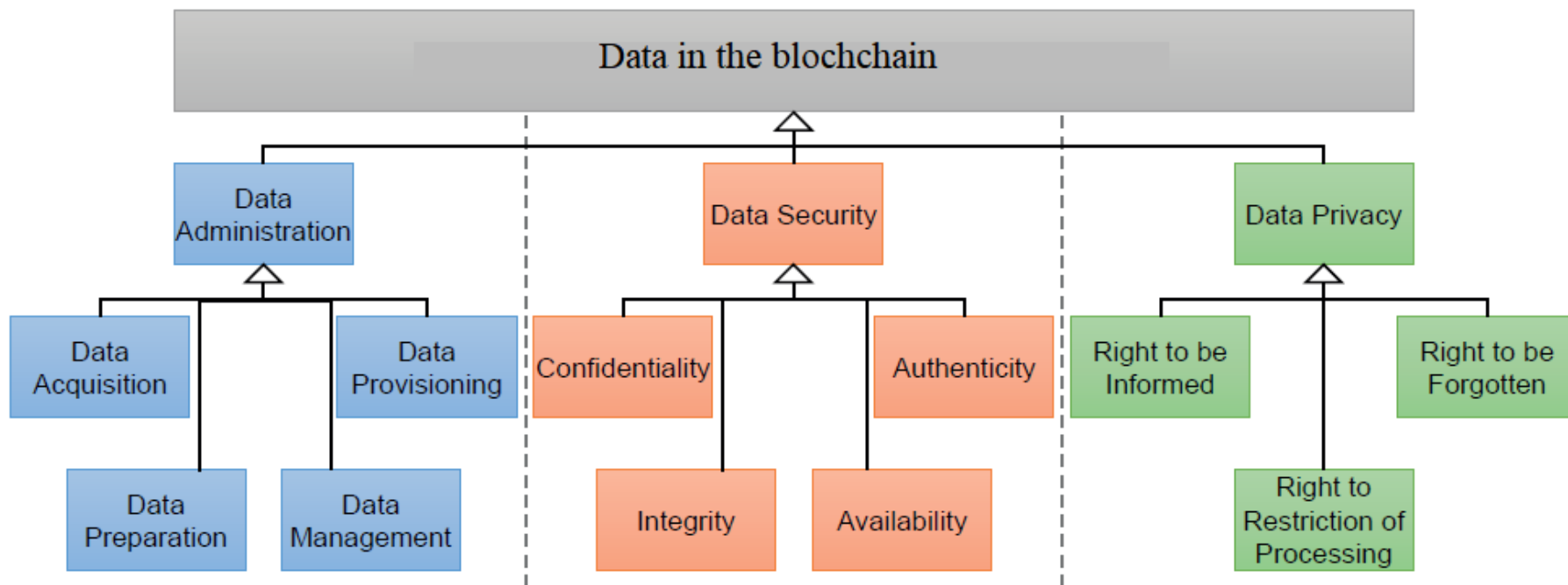
- скорост на транзакции
- големина на предаваните пакети
- права на достъп за избор на мрежа с или без разрешения
- поверителност на записите
- перманентност
- сигурност на средата
- проверка по Consistency, Availability, Partition Tolerance (CAP)- спазване на определен ред на операциите, отговаря на получена заявка дори при частичен срив на системата

Технологията Blockchain

- Метод за разпределено съхранение на информация в компютърна мрежа.
- Представява непрекъснато растящ списък (верига) от кодирани записи (блокове), свързани помежду си.
- Осигурява интегритет – блоковете са хронологични и съдържат информация за предходния блок
- Не позволява модифициране на данните.
- Записват се транзакции между двама участници по начин, който е устойчив и подлежи на проверка.
- Участниците в мрежата са равноправни (peer to peer) и спазват определен протокол за валидиране на новите блокове.
- Веднъж валидиран и записан, никой блок не може да бъде променян без да се променят всички следващи го блокове.

Надеждност при блокчейн

- 1962 – криптографски подписи
- 1991 - хеширане на цифрови документи (Stuart Haber и Scott Stornetta) – изпращат се на сървър, където с хеш-печат се валидират и всяка седмица се генерира нов хеш-печат
- 1999 - прилагане на разпределена и устойчива на грешки файлова система с отчитане на разходите при репликация (Кастро и Лисков)
- 2008 - peer-to-peer (P2P) метод за повишаване на прозрачността на транзакциите и доверието между партньорите (Сатоши Накамото)



Предимства на blockchain

- Максимална сигурност
 - Криптографията защитава данните от фалшифициране.
- Липса на посредници
 - Директните трансакции (P2P) намаляват банковите такси.
- Пълна прозрачност
 - Всеки участник вижда историята на записите.
- Неизменимост на данните
 - Веднъж записана, информацията не може да се изтрие.
- Постоянна наличност
 - Децентрализираната мрежа работи без прекъсване 24/7.
- Автоматизация
 - Смарт договорите изпълняват споразумения без човешка намеса.

Недостатъци на blockchain

- Ограничена скорост
 - Потвърждаването на трансакциите изисква време за консенсус.
- Проблем с мащабируемостта
 - Мрежите се забавят при огромен брой потребители.
- Висок разход на енергия
 - Механизми като Proof of Work хабят огромно количество ток.
- Необратимост на грешките
 - Загубата на частен ключ означава окончателна загуба на активите.
- Сложна интеграция
 - Трудно се свързва с традиционни бизнес софтуери.
- Правна неяснота
 - Липсва единна глобална регулация и правна рамка.

Правни аспекти на blockchain

- **Регламентът MiCA** (Пазари на криптоактиви) на Европейския съюз от 2024г. , предстои през 2027г. MiCA II да обхване и страни извън ЕС
 - Доставчиците на услуги за криптоактиви (CASP) — като борси и криптопортфейли — подлежат на задължително лицензиране след 1 юли 2026 г.
- Directive 2014/65/EU - Директива за пазарите на финансови инструменти на ЕС
- COM/2020/594 final - директива за пазарни инфраструктури за търговия с криптоактиви под distributed ledger technology
- **Закон за пазарите на криптоактиви (ЗПКА)-27.06.2025г.**
бр.54 на ДВ
- Процедура 2018/2085 (INI) Blockchain a forward looking trade policy“. European Parliament – за open source
- **Европейският акт за ИИ (EU AI Act) и Web3** – влиза в сила 02.08.2026г.
- **White paper**
 - за всеки криптоактив

В САЩ

- Законът GENIUS (GENIUS Act):
 - Приет през юли 2025 г., този закон въведе задължително изискване стейбълкойните да бъдат обезпечени 1-към-1 с щатски долари или други нискорискови активи.
- Данъчна прозрачност и споделяне на данни:
 - Въведени са строги стандарти за автоматизирано отчитане на трансакциите и разширяване на фидуциарните задължения на институциите.
- Съвместна рамка на SEC и CFTC:
 - През март 2026 г. Комисията по ценните книжа и фондовите борси (SEC) и Комисията за търговия със стокови фючърси (CFTC) издадоха съвместна интерпретация с 5-степенна таксономия. Тя ясно разграничава кога един блокчейн актив е „ценна книга“ (под надзора на SEC) и кога е „стока“ (децентрализиран актив под надзора на CFTC), заимствайки принципи от акта FIT21.
- Забрана за CBDC:
 - Със специален закон (Anti-CBDC Surveillance State Act) на Федералния резерв е изрично забранено да емитира дигитална валута на централната банка за крайни граждани.

В Азия

- Хонконг (Project Ensemble):
 - Създадена е цялостна нормативна среда и регулаторен „пясъчник“ за тестване на токенизирани банкови депозити и дигитални валути на централни банки на едро (wholesale CBDC).
- Сингапур (Project Guardian):
 - Паричният орган на Сингапур (MAS) развива правна рамка за токенизация на активи с фиксирана доходност, управление на активи и чуждестранна валута чрез междугранично сътрудничество.
- Япония и Южна Корея:
 - Двете страни имат едни от най-старите и стриктни закони за защита на инвеститорите в криптоактиви, изискващи пълно отделяне на клиентските активи от балансите на борсите.
- Китай:
 - Държи курс на пълна забрана за трансакции и копаене на криптовалути, но държавата силно субсидира и регулира използването на не-криптовалутни блокчейн технологии за индустриални цели и развива дигиталния юан (e-CNY).

Други страни

- Обединеното кралство:
 - Борсите и попечителите на дигитални активи подлежат на строг режим за борба с прането на пари (AML) и финансирането на тероризма под надзора на FCA.
 - Налагат се затегнати правила за маркетинг и реклама на блокчейн продукти пред масови потребители.
- Ел Салвадор:
 - Първата държава в света, която прие Биткойн като законно платежно средство (заедно с щатския долар) чрез своя „Закон за Биткойн“, придружен от регулации за издаване на вулканични облигации, обезпечени с криптовалута.
- Бразилия:
 - Централната банка има изградена лицензионна рамка за доставчици на дигитални активи, а страната активно развива мащабни блокчейн пилоти за токенизация на държавни ценни книжа.
- Дубай:
 - **VAR Act (Virtual Assets Regulatory Authority):** Дубай създаде първия в света специализиран, независим регулаторен орган само за дигитални активи (VARA). Тяхната нормативна уредба предоставя ясни правила за лицензиране на блокчейн бизнеси, емитиране на токени и метавселени, което я прави магнит за индустрията.

Глобални препоръки на FATF

- Financial Action Task Force (FATF)
- блокчейн компаниите са длъжни по закон да прилагат **„Правилото за пътуване“ (Travel Rule)** – изискване за събиране и предаване на идентичността на изпращача и получателя при трансфер на криптоактиви.

Blockchain и DNS

- Блокчейн домейните не се признават от ICANN, т.к. не са част от DNS системата от имена
- Нито един от регулаторните органи, свързани с Интернет, няма правомощия по отношение на блокчейн домейните
- ICANN е организация, ENS е smart contract, но и двете разпределят поддомейни и резолват име на домейн към собственик, като записите са за определен срок.

Но....

- Както DNS домейните, така и ENS (Ethereum Name Service) домейн имената са буквено-цифрови обозначения.
- Те се подразделят на TLD (Top level domain) и 2LD(second-level *domain* - SLD или 2LD).
- ENS управлява специфични за ENS TLD - ".eth" , ".test", и всички TLD със специално предназначение.
- ENS домейните са електронни адреси в Интернет, но са и идентификатор на портфейл в блокчейн

Blockchain домейн имена

- Няма закони за откраднати имена на Web3 домейни, но **интелигентният договор може да предостави възможност за принудително връщане на недобросъвестно придобит домейн при определени условия.**
- Всеки има право да закупи всеки блокчейн домейн.
- Всеки собственик има право да освободи за закупуване блокчейн домейн.
- Има политика за защитени марки при закупуване на блокчейн домейни- sunrise (изтече 2022г.)
- Блокчейн домейнът за известни търговски марки се закупува веднъж и не се подновява – защитава утвърдени търговски марки.
- Регистрирането на домейн в ENS екосистемата, който е чужда марка, не е нарушение на интелектуална собственост.

Blockchain и Internet

- Internet е оперативно съвместима мрежа от мрежи за предаване на данни, Blockchain мрежата е една единствена P2P компютърна мрежа
- Достъпът до Blockchain мрежата е през Internet по име на блокчейн домейна, т.к. това е децентрализирано приложение и копия на всички данни са налични във всеки самостоятелен блок от мрежата, а не на един единствен сървър

ENS и NFT

- ENS и “Unstoppable Domains” позволяват на всеки да запази уникално име на блокчейн домейн като NFT(от англ. “Non fungible tokens”).
- Тези NFT могат да бъдат продавани, например през платформа „OpenSea“.
- По искане на реалния притежател върху правата на дадена търговска марка, платформата „OpenSea“ може да изтегли токена(NFT) от продажба в случай на предполагаемо нарушение на правата върху търговска марка или други права на интелектуална собственост.
- В ENS домейните трябва да бъдат подновявани, а в „Unstoppable Domains“ не е необходимо да се подновяват блокчейн домейни.

GDPR и blockchain

- Европейският комитет по защита на данните (EDPB) прие официалната версия 2.0 на своите *Насоки 02/2025 за обработка на лични данни чрез блокчейн технологии.*
- Неизменимост и вечно съхранение влиза в директен конфликт с общия регламент за защита на данните на ЕС (GDPR)
- **Насоки за обработка на лични данни чрез блокчейн** на Европейският комитет по защита на данните (EDPB)
 - Организацията се насърчават да съхраняват самите лични данни извън веригата (*off-chain*), а в блокчейна да записват само криптографски кодове (хешове) или да използват частни блокчейн мрежи с контролиран достъп.

Blockchain и „изпиране на пари“

- През 2026 г. започва работа новият Европейски орган за борба с изпирането на пари (**AMLA - Anti-Money Laundering Authority**).
- AMLA ще има правомощията директно да контролира най-големите трансгранични криптиоплатформи и финансови посредници в ЕС, за да гарантира спазването на правилата за идентификация (KYC) и проследяване на трансакциите (Travel Rule).
- Правилото за трансфер на средства (Travel Rule)
 - Изисква от доставчиците на крипто услуги да събират и споделят информация за наредителя и бенефициента при всяка трансакция.
- Идентификация (KYC)
 - Анонимното търгуване през регулирани платформи вече е невъзможно, защото се изисква задължителна проверка на самоличността на потребителите

Правен статут на умните договори

- Смарт договорите (самоизпълняващ се код в блокчейн) все още нямат статут на класически писмени договори в традиционното право.
- Правното предизвикателство е в разпределянето на отговорността при софтуерни грешки, пробиви в сигурността или уязвими кодове.
- Директивите на ЕС се стремят да наложат стандарти за одит на кода при използването им в търговски отношения.
- При публичните блокчейни страните са анонимни (криптографски адреси). Ако възникне спор, е изключително трудно да се установи кой реално е сключил договора, за да бъде съден.
- Териториална юрисдикция - блокчейн мрежите са разпределени на хиляди сървъри по целия свят, затова е трудно да се определи съдът на коя държава е компетентен да разреши спор между страните.

Моделът на "Хибридните договори" (Ricardian Contracts)

- Страните подписват традиционен хартиен или дигитален договор (PDF), съставен от юристи.
- В този договор изрично се посочва, че определени клаузи (например автоматично плащане при доставка) ще бъдат изпълнени от конкретен смарт договор.
- Ако кодът се "бъгне" или възникне спор, традиционният договор има правно превъзходство пред блокчейн изпълнението.

Регулацията в Европейския съюз

- Законът за данните - Data Act:
- Клауза за прекратяване (Kill Switch) - всеки смарт договор, който споделя данни, да има вграден механизъм за безопасно спиране или прекратяване на действието му, ако възникне грешка или съдебен спор.
- Това изискване предизвика сериозни дебати в Web3 общността, тъй като **нарушава принципа за "неизменяемост" на блокчейна, но за традиционния бизнес е задължителна гаранция.**

"Оракули" (Oracles) - дигитални свидетели

- Смарт договорите разчитат на **Оракули** (като Chainlink), които подават външни данни към блокчейна – за "форсмажор", "добросъвестност" или "промяна в обстоятелствата".
- От правна гледна точка, изборът и надеждността на Оракула се договарят предварително от страните като официален източник на истината.

Законова уредба за умните договори в България

- В България смарт договорите нямат отделна дефиниция в Закона за задълженията и договорите
- Договорът е съглашение между две страни.
- Писмената форма се смята за спазена, ако е извършено електронно изявление (съгласно Закона за електронния документ и електронните удостоверителни услуги).
- Следователно, **смарт договорите се тълкуват като форма на автоматизирано изпълнение на вече сключено електронно споразумение.**

Данъчно облагане при търговия с криптовалути

- **Данъчна прозрачност и международни стандарти (CARF) - старт през 2027 г-внедряването на рамката на ОИСР за докладване на криптоактиви — CARF (Crypto-Asset Reporting Framework).**

В България приходите от продажба или замяна на криптовалути се облагат по общия ред:

- **За физически лица:** доходите се облагат с 10% данък върху реализираната печалба съгласно ЗДДФЛ.
- **За юридически лица:** печалбите се облагат с корпоративен данък по ЗКПО.

Стандарти за умни договори

- Стандартите за умни договори дефинират общи правила и програмни интерфейси, които позволяват на различните приложения да взаимодействат помежду си безпроблемно.
- Това са софтуерни шаблони и Fabric Contract API

За Ethereum – smart contract	За HyperLedger Fabric – chaincode
ERC-20 (Fungible Tokens)	Fungible Token Sample
ERC-721 (Non-Fungible Tokens)	NFT Sample
ERC-1155 (Multi-Token Standard)	
ERC-4626 (Tokenized Vaults)	
ERC-4337 (Account Abstraction)	
	State-Based Endorsement
	Private Data Collections

Въпроси ?

Благодаря за вниманието !