České vysoké učení technické v Praze
Fakulta elektrotechnická

Bakalářská práce

# Využití technologie blockchain v prostředí internetu věcí

Martin Javorský

Praha, Prosinec 2021

**Prohlášení**

Prohlašuji, že jsem předloženou práci vypracoval samostatně a že jsem uvedl veškeré použité informační zdroje v souladu s Metodickým pokynem o dodržování etických principů při přípravě vysokoškolských závěrečných prací.

V Praze dne ..... .....

**Poděkování**

Rád bych poděkoval svému vedoucímu diplomové práce doc. Ing. Stanislav Vítek, Ph.D. za odborné vedení práce a mnoho cenných rad.

# ZADÁNÍ BAKALÁŘSKÉ PRÁCE

## I. OSOBNÍ A STUDIJNÍ ÚDAJE

Příjmení: **Javorský** Jméno: **Martin** Osobní číslo: **492019**

Fakulta/ústav: **Fakulta elektrotechnická**

Zadávající katedra/ústav: **Katedra radioelektroniky**

Studijní program: **Elektronika a komunikace**

## II. ÚDAJE K BAKALÁŘSKÉ PRÁCI

Název bakalářské práce:

**Využití technologie blockchain v prostředí internetu věcí**

Název bakalářské práce anglicky:

**Using Blockchain Technology in the IoT Environment**

Pokyny pro vypracování:

1. Prostudujte možnosti využití technologie Blockchain. Zaměřte se na technologii chytrých kontraktu (Smart contracts) a existujících implementací, které chytré kontrakty umožnují.
2. Navrhněte modelovou aplikaci, která využívá chytré kontrakty v prostředí internetu věcí.
3. Modelovou aplikaci implementujte.

Seznam doporučené literatury:

[1] WU, Mingli, et al. A comprehensive survey of blockchain: From theory to IoT applications and beyond. IEEE Internet of Things Journal, 2019, 6.5: 8114-8154.
[2] LAO, Laphou, et al. A survey of IoT applications in blockchain systems: Architecture, consensus, and traffic modeling. ACM Computing Surveys (CSUR), 2020, 53.1: 1-32.

Jméno a pracoviště vedoucí(ho) bakalářské práce:

**doc. Ing. Stanislav Vítek, Ph.D. katedra radioelektroniky FEL**

Jméno a pracoviště druhé(ho) vedoucí(ho) nebo konzultanta(ky) bakalářské práce:

Datum zadání bakalářské práce: **30.01.2022** Termín odevzdání bakalářské práce: **20.05.2022**

Platnost zadání bakalářské práce: **30.09.2023**

| doc. Ing. Stanislav Vítek, Ph.D.<br>podpis vedoucí(ho) práce | doc. Ing. Stanislav Vítek, Ph.D.<br>podpis vedoucí(ho) ústavu/katedry | prof. Mgr. Petr Páta, Ph.D.<br>podpis děkana(ky) |
|---|---|---|

## III. PŘEVZETÍ ZADÁNÍ

Student bere na vědomí, že je povinen vypracovat bakalářskou práci samostatně, bez cizí pomoci, s výjimkou poskytnutých konzultací. Seznam použité literatury, jiných pramenů a jmen konzultantů je třeba uvést v bakalářské práci.

. Datum převzetí zadání

Podpis studenta

# Abstrakt

Tato bakalářská práce se zabývá využitím technologie blockchain v IoT systémech. Obsahuje vysvětlení principů fungování blockchainu/Tangleu a internetu věcí. Výhody a nevýhody jejich propojení, možnosti využití a v neposlední řadě realizaci IoT systému fungujícím na blockchainu.

# Abstract

This bachelor thesis deals with the use of blockchain technology in IoT systems. It includes an explanation of the principles of blockchain/Tangle and IoT. Advantages and disadvantages of their interconnection, the possibilities of their use and last but not least, the implementation of IoT system operating on blockchain.

# Klíčová slova

Technologie blockchain, IOTA, chytrý kontrakt, Iot systémy

# Keywords

Blockchain technology, IOTA, smart contract, IoT systems

# Obsah

# 1 Úvod

Od vzniku a komercializace internetu již uplynulo více jak 25 let a internet se stal nedílnou a každodenní součástí našich životů, ať už internet využíváme přímo, nebo jej používají zařízení, se kterými se každý den setkáváme, bez naší pomoci. Žijeme v době čtvrté průmyslové revoluce a dá se očekávat, že elektronických systémů, které využívají internet bude přibývat. Ono je to logické, lidé mají rádi věci, které jim ulehčují život, a to internet prostřednictvím internetu věcí, dále jen IoT z anglického názvu „internet of things“, určitě ulehčuje. IoT systémy se dostávají do všech oblastí života, a tím počet připojených zařízení prudce narůstá. Současná infrastruktura je zatím schopná zvládat nárůst zařízení v síti, ale s množstvím dat, která musí cloudy zvládat, rostou i náklady na jejich provoz a náročnost na technologie. Očekávaný nárůst připojených IoT zařízení do internetu je exponenciální, a tím i očekávané náklady. Budoucí potenciální problém se neskrývá jen v nákladech, ale také v rychlosti sítě. Jako příklad použiji autonomní auta, takovýto IoT systém musí fungovat v reálném čase a zdržení dat v síti může znamenat otázku života a smrti. Tedy nastává otázka, zda je současný systém udržitelný. V roce 2008 se ve světě objevila nová technologie zvaná blockchain, která nepřišla sama o sobě, ale přišla v podobě jedné své implementace zvané „Bitcoin“. Tato implementace rozšířila technologii blockchain do podvědomí, ale svými specifiky technologii jako takovou zastínila. Technologie blockchain se díky svým vlastnostem hodí pro některá řešení IoT systémů a mohla by v této oblasti zastínit cloudová řešení a vyřešit problémy budoucnosti.

Tato bakalářská práce se věnuje popisu technologie blockchain, a jejímu fungování. Pro lepší náhled do problematiky je v práci vysvětleno fungování IoT systémů. Základním kamenem této bakalářské práce je ověřit vhodnost technologie blockchain v IoT systémech. Výhody a nevýhody propojení těchto dvou technologií a ukázání již existujících implementacích. Práce se řídí rčením, že ukázka je více než tisíc slov, proto v praktické části této práce je návrh modelové aplikace IoT systému s využitím technologie blockchain či technologii podobné. Jedním z vedlejších cílů je, aby práce sloužila jako náhled do problematiky blockchainu, jelikož se jedná o pozoruhodnou technologii, která otevírá dveře zajímavým možnostem, ale její krása je v dnešní době pro veřejnost schována za představou rychlého zisku, který umožnují některé její implementace. Je dost pravděpodobné, že technologie, jako taková, tu s námi bude a čím dříve se závoj nejasností odkryje, tím jednoduší bude rozšiřování technologie do světa.

# 2 Technologie blockchain

Tato kapitola poskytne náhled do problematiky blockchain, co blockchain představuje, základní principy fungování, vybrané implementace a jejich odlišnosti. Na implementacích je nejlépe ukázána síla této technologie. A nakonec možnosti využití a jejich výhody a nevýhody.

## 2.1 Co je blockchain

Technologie blockchain je druh distribuované decentralizované databáze s neustále se rozšiřujícím záznamovým řetězcem. Řetězec je rozšiřován o blok dat, který je zašifrován asymetrickou kryptografií a zařazen chronologicky do řetězce těchto bloků. Proto tedy blockchain v překladu řetězec bloků. Definice jsou samozřejmě všeříkající, ale malinko ji rozeberu na dvě části, distribuovaná decentralizovaná databáze a řetězec s bloky[20].

## 2.2 Základní rozdělení databází dle architektury

Pro pochopení distribuované decentralizované databáze je nejlepší podívat se, jaké jsou i jiné možnosti databází.

### 2.2.1 Centralizovaná databáze

Jedná se o databázi, která se nachází na jednom centrálním místě. To znamená, data se nacházejí pod jednou střechou a všichni, kdo chtějí do databáze přistoupit, tak přistupují do jednoho uzlu sítě. Příkladem je třeba banka, nebo webová stránka jako je facebook. Vždy, když chcete přistoupit k datům uloženým na facebooku, připojíte se do facebookového datového centra a tam na pevných discích jsou data uložena. Takováto databáze se lépe udržuje, ale tím, jak jsou data pohromadě, je více náchylná na hackerské útoky, nebo ztrátu či poškození dat při poškození disku. Dále takováto databáze je spravována centrální autoritou, tedy uživatel musí svěřit svoji důvěru do rukou třetí osoby a věřit, že data nezneužije, nebo nepozmění. Každá databáze vyžaduje jednou za čas údržbu a s tím někdy spojené odpojení od sítě, což pro uživatele znamená dočasnou nedostupnost dat, což může být mnohdy nepříjemné a nežádoucí.

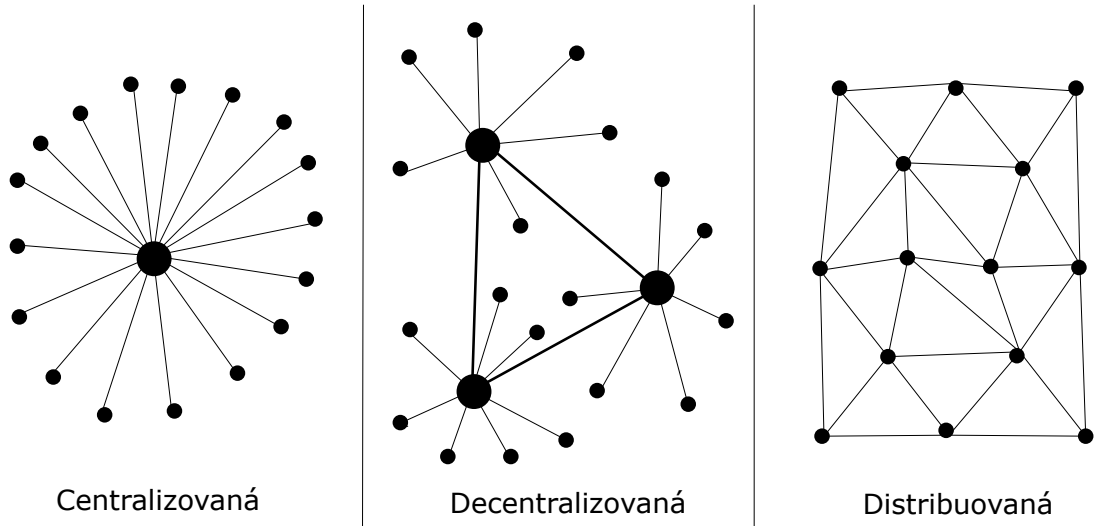
### 2.2.2 Decentralizovaná databáze

Decentralizovaná databáze se již nachází na několika místech. Vyřazení jednoho serveru nemusí znamenat nedostupnost dat, jen musí dojít k přepojení komunikační cesty přes jiné uzly. V praxi to funguje tak, že stejná data se nacházejí na více serverech a podle jejich vytíženosti jste nasměrováni na ten nejméně využívaný. Tato databáze je náročnější na údržbu, ale je již méně náchylná na výpadky a je složitější data napadnout, nebo je manipulovat. Ale i decentralizovaná databáze může být vlastněna jednou centrální autoritou [26].

### 2.2.3 Distribuovaná decentralizovaná databáze

Vychází z decentralizované databáze. Decentralizovaná databáze je rozšířena o distribuci dat mezi všemi uživateli v reálném čase, tím se databáze stává nenáročnou na údržbu. Distribuci zajišťují mezi sebou jednotlivé uzly sítě (v krypto světě těžaři), tím je vyřazena třetí autorita, která by mohla tuto síť ovlivňovat. Data jsou uložena současně na všech uzlech sítě, tedy k situaci, že data nebudou přístupná nemůže skoro dojít. Pro změnu dat v síti by bylo třeba změnit 51% sítě, takže čím je síť větší, tím je vlastně bezpečnější [26].

Na této databázi je založen blockchain, což mu poskytuje ještě v souvislosti s řetězcem a bloky, kterým je věnována další podkapitola, bezpečný a stabilní charakter. Dále z decentralizované databáze vyplývá decentralizace blockchainové sítě. Představte si, že by existovaly služby bez centrální autority. Sociální sítě, kde by nehrozilo, že vám jen tak smažou nebo zablokují účet, pokud se vedení zrovna nehodíte, jak to udělal Twitter po volbách prezidenta USA, nebo že majetky, které budujete celý život, vám nebudu odebrány kvůli politické situaci. Je běžnou praxí, že vlastníci centralizovaných sítí prodávají data, která spravují, dalším firmám. S decentralizací přichází zas o trošku méně regulace a tím více svobody, ale s tím i zodpovědnosti.




Obrázek 1: Druhy databází

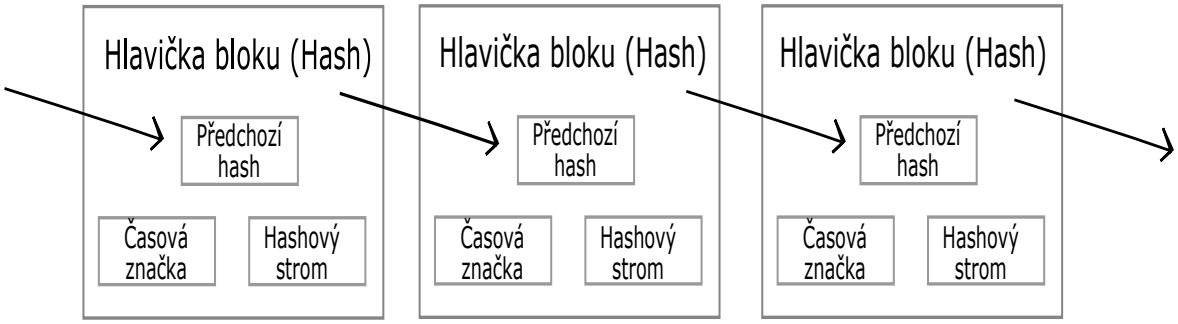
## 2.3 Řetězec a bloky

Většina světa v dnešní době používá jako hlavní platební nástroj fiat měnu. Fiat měna není na nic vázána (dříve byly peníze vázané na zlato), to znamená, že si je centrální banky (stát) mohou tisknut nebo připočítat v online světě, jak chtějí. Peněz je nekonečně mnoho a tím dochází k inflaci a znehodnocování peněz. Proto první implementací blockchainu se stal Bitcoin. Digitální měna postavená na blockchainu s pevně daným množstvím a jeho uvolňováním. Bitcoin si v posledních letech získal pozornost široké veřejnosti, proto si drtivá většina lidí spojí s blockchainem kryptoměny, a tedy finanční transakce. Jednotlivým blockchainům je věnována jiná část práce. Bitcoin je

zde uveden, jelikož na něm vysvětlím řetězec a bloky.

Bitcoin si můžeme představit jako účetní knihu, kde zapisujeme transakce. Každý uzel decentralizované sítě má kopii tohoto seznamu. Po uplynutí časového úseku, u Bitcoinu 10 minut, se uzavře účetní kniha do bloku a začíná se zapisovat do nové účetní knihy. Takto uzavřený blok je přidán do řetězce bloků v chronologickém pořadí, proto se to nazývá blockchain (řetězec bloků)[27].

Blok se skládá z hlavičky a mnoha transakcí. V hlavičce je hash hodnota předchozího bloku, časová značka, hashový strom a další. Schéma tohoto systému je znázorněno na obrázku 2.




Obrázek 2: Schéma propojení řetězce

Hash se dá chápat jako otisk prstu digitálního souboru. Časová značka udává, kdy byl blok do řetězce zařazen a kdy s daty v bloku bylo naposledy manipulováno. Hashový strom je datová struktura uchovávající strukturu hasů a umožnuje ověřit integritu dat v čase. Takto poskládaný řetězec prakticky neumožňuje pozměnit data v řetězci, jelikož by bylo nutné změnit tuto informaci na 51% zařízeních v systému a, pokud by se měnil blok, který není na kraji, ale je níže v řetězci, bylo by nutné pozměnit i všechny bloky následující a tato změna by byla vidět na časové značce. Tím se blockchain stává bezpečným a důvěryhodným [18].

### 2.3.1 Systémy potvrzování transakcí

Procesu, kdy se blok uzavírá se říká těžení. Cílem procesu je, aby se jednotlivé uzly shodly na hodnotách v bloku, aby uzly měly stejné hodnoty. Systémů potvrzování transakcí je hned několik a v této kapitole jsou uvedeny ty nejzákladnější z nich.

Proof of work - PoW

Tento systém přišel s Bitcoinem. Jedná se o potvrzení prací (výpočetním výkonem). Uzly (stroje), tvořící síť, při uzavírání bloku závodí, kdo jako první vyřeší matematický problém. Řekněme, že účetní kniha s daty je zašifrována maticí a uzly se snaží najít takovou inverzní matici, aby dostaly svůj seznam, když na ni přijdou, oznámí to ostatním uzlům a ty ji aplikují, dostanou-li správný seznam, potvrdí správný výsledek. Je-li potvrzení dost (více jak polovina uzlů), blok je uzavřen a přidán do řetězce. Uzel, který vytěžil blok, je odměněn tokenem, který má hodnotu i v současném finančním systému. Uzel s větší výpočetní silou má větší šanci na úspěch. Těžaři se proto seskupují do takzvaných poolů, kde spojí svoji výpočetní sílu, a zisk si pak dělí v poměru,

jakým přispěli do celkového výpočetního výkonu. Tento systém je nejjednodušší, ale potýká se s náročností na spotřebu vnějších zdrojů, jako je elektrická energie, jelikož stroje v uzlech jsou napájeny elektrickou energií. Tento systém používá kromě Bitcoinu i Ethereum blockchain, o kterém je zmínka později [28].

Proof of stake – PoS Druhý systém, dnes nejpoužívanější, který řeší největší problém PoW, je proof of stake (PoS). Tento systém využívají blockchain Cardano, Neblio a mnoho dalších. Ethereum blockchain by na něj měl přejít se svojí verzí 2.0. V tomto systému spolu nesoupeří všechny uzly, kdo bude nejrychlejší, ale každý uzel zastaví počet tokenů, které má, a podle jejich množství a délky držení se vyhodnotí, kdo daný problém vyřeší. Poté, co jej vyřeší, nabídne řešení ostatním a ti jej potvrdí. V tomto řešení, řeší složitou úlohu jen jeden uzel, a tedy spotřeba energie je mnohonásobně menší než u varianty PoW. Zároveň v PoS jsou vyřešeny některé bezpečnostní problémy, které PoW obsahuje, ale u těchto systémů nejde pouze o schvalování bloků, ale také o rozhodování o systému (hlasování o aktualizacích blockchainu), tedy u PoW platí rozhodnutí, které udělalo více jak 50% techniky a u PoS více jak 50% hodnoty zastavených mincí [5].

Proof of Burn – PoB Systém vycházející z PoW metody, ale energeticky nenáročný. Opět dochází k přiřazení bloku vybranému uzlu k vytěžení jako u systému PoS. Uzly spalují tokeny a tím, si předkupují právo na těžení, čím více mincí spálí, tím mají větší šanci, že jim bude blok přidělen a získají odměnu. Tím se přirozeně redukuje počet tokenů v oběhu, což v případě, že by tokeny byly kryptoměnou, redukuje inflaci [1].

Systémů, jako jsou tyto, je více, například různé jejich kombinace a variace, ale pro úvod do problematiky a potřeby této práce stačí tyto 3 příklady.

## 2.4 Implementace blockchainu

Tato kapitola je zaměřená na popsání pár vybraných implementací blockchainu, jejich vlastností a potenciálu jejich využití.

### 2.4.1 Bitcoin

O tomto blockchainu jsem se v tato práce zmínila už několikrát, tady jsou poznatky o Bitcoinu shrnuty, uceleny a doplněny. Bitcoin je první implementací blockchainu, jedná se o digitální měnu zveřejněnou v roce 2008 Satoshi Nakamotou jako peer-to-peer elektronický peněžní systém. Tento systém je decentralizovaný, anonymní a je definovaný přesný počet tokenů také Bitcoinů, které budou v oběhu. Počet Bitcoinů je necelých 21 000 000. Bitcoiny se do oběhu přidávají těžbou a množství Bitcoinů, které je takhle vytěženo, se s časem snižuje. Poslední Bitcoin bude vytěžen v roce 2140, ale drtivá většina všech Bitcoinů bude v oběhu v roce 2030. Bitcoin zvládne provést 7 transakcí za sekundu, což ve srovnání s dnešními platebními systémy není moc. Potvrzení transakce trvá 10 minut, což je i interval, ve kterém se uzavírají bloky. Potvrzování funguje na principu PoW, vysvětleném v předcházející kapitole. Výhodou blockchainu je, že se neustále vyvíjí, proto pro zapojení kryptoměn do běžného života vznikla druhá vrstva blockchainu Lightning Network (LN). LN je protokol pro platby, vyřešil problém rychlosti platby a počtu transakcí za vteřinu. V půlce roku 2021 se

stal Bitcoin oficiální měnou v El Salvadoru, zde můžete pomocí peněženky na telefonu zaplatit tokenem Bitcoin jako kartou. Token Bitcoin jako platidlo je v počátcích, ale nelze vyloučit, že se neprosadí, jeho neměnný počet může být příjemnou alternativou oproti fiatu, ale zatím je cena Tokenu Bitcoinu odvozena od ceny na burze (převážně davovou psychologií), což dělá Bitcoin jako token dosti volatilním [27].

### 2.4.2 Ethereum

Ethereum je open-source blockchain framework vyvinutý Buterin Vitalkem. Je to druhá nejznámější implementace blockchainu. Na rozdíl od Bitcoinu není počet tokenů, Etherů, omezen a nevznikl za účelem kryptoměny. Funguje také na principu PoW, ale měl by ve druhém čtvrtletí roku 2022 přejít na PoS, což by jej udělalo méně energeticky náročným na těžbu a tedy i fungování. Zvládne 15 transakcí za sekundu, což je dvojnásobné oproti Bitcoinu a uzavření jednoho bloku trvá pouhých 14-15 sekund. Ethereum byl jeden z první blockchainů, který začal podporovat chytré kontrakty (anglicky smart contracts). Chytré kontrakty umožňují, aby se do účetní knihy daného blockchainu nezapisovaly pouze transakce, ale mohou se do této knihy zapisovat i celé programy, které pak využívají výpočetní sílu svých uzlů. Díky tomu můžeme o Ethereu mluvit jako o světovém počítači. Tím se otevírá nový svět možností nejen pro převody peněz mezi peněženkami, ale pro vytváření decentralizovaných aplikací(DAP - decentralized application) a systémů bez centrální autority nebo také nové možnosti ukládání dat jednoduše dostupných po celém světě [19].

### 2.4.3 Neblio

Další ukázkovou implementací je Neblio. Neblio je oproti dvěma předchozím implementacím podstatně méně známé, jelikož se jedná o mladší implementaci založenou v roce 2017 Edwardem Smithem a Ann Jacksonem. Tito dva pánové byli špičkami ve svých oborech, Smith pracoval dlouhá léta pro Cisco a Jackson byl 6 let vývojářem firmy Hewlett Packard's. Tito pánové díky svým zkušenostem viděli využití blockchainu v industriálním odvětví a s vizí změnit zavedené postupy nehledě na cenu Neblia tvrdě pracovali s týmem a vyvinuli velice bezpečný a silný blockchain podporující 8 programovacích jazyků, tokenizaci protokolem NTP1 a rychlé transakce. Blockchain Neblio má za sebou zkušený tým, který nabízí podporu vývojářům. Neblio funguje na PoS systému a s podporováním API se stává skvělým blockchainem pro vytváření decentralizovaných aplikací [15] [16].

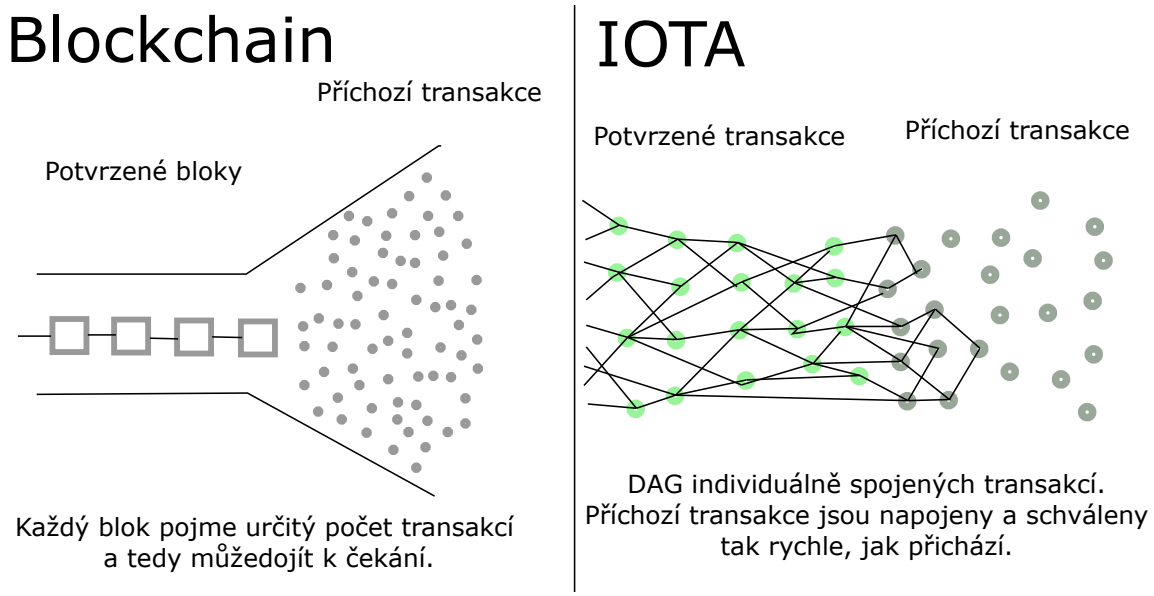
Blockchainy jako Ethereum a Neblio mají všeobecné použití, tedy dají se použít pro IoT systémy, ale nemusí být k tomuto užití vždy optimální, proto vznikají i decentralizované sítě, které se specializují přímo na IoT systémy. Naschvál jsme zde neuvedl termín blockchain, jelikož se v těchto případech o blockchain nejedná. V předchozí kapitole je popsáno, jak blockchain funguje, jak rychle vyhodnocuje transakce a co je třeba udělat, aby transakce byla uložena. Tyto kroky vykonávají validátoři a vezmou si za to odměnu, to znamená poplatek pro žadatele o transakci. V IoT systémech některá zařízení provádějí transakce v rámci sekund, tedy náklady spojené s těmito zařízeními by převážili výhody blockchainu. Proto jsou zde uvedeny dva zástupci systému, který

vyšel z blockchainu, ponechal jeho výhody důležité pro IoT jako je bezpečnost, důvěryhodnost a decentralizace, ale řeší problém rychlosti, škálovatelnosti a některé další. Prvním je IOTA, na této decentralizované databázi je v této práci koncept představen, ale za zmínku stojí i konkurenční projekt IoT Chain od čínských developerů, který funguje na velmi podobných principech jako IOTA, ale co se týče informací o jeho fungování a vývoji na něm, je méně uživatelsky přívětivý [17].

### 2.4.4 IOTA

Je navržena pro specifické potřeby systémů internetu věcí. Jak už bylo zmíněno, IOTA je stejně jako blockchain distribuovaná decentralizovaná síť podporující transakce a chytré kontrakty, ale liší se v několika věcech. První rozdíl je, že IOTA nemá těžaře, díky tomu nemá poplatky za transakce a je nenákladová. Aby bylo zajištěno potvrzování, každý účastník sítě schvaluje transakce (propůjčí malou část výpočetního výkonu síti), u blockchainu toto dělají jen těžaři za odměnu.

Druhý rozdíl je v tom, že schválené transakce nejsou shromažďovány v bazénech (poolech) a pak vybírány do bloků, kde jsou schváleny, ale jsou ihned zapojovány do sítě DAG systémem. DAG je přímý necyklický graf, anglicky Direct Acycle Graph. Tento systém funguje tak, že nová transakce je ihned přidána do sítě napojením na některé dvě již schválené transakce, rozšiřuje se jen jedním směrem a necyklický, jelikož není možné tvořit smyčky. Tímto systémem je možné přidávat několik transakcí najednou a tím výrazně navýšit počet transakcí schválených za jednotku času. Pro lepší pochopení je systém DAGu v porovnání s blockchainem zobrazen na obrázku 2. Dá se vypozorovat, že jednotlivé transakce čekají na vytvoření bloku a schválení celou sítí, zatímco u DAGu se příchozí transakce zapojují do celku hromadně a okamžitě.




Obrázek 3: Porovnání Blockchainu a IOTA

Třetí rozdíl je spojen s důvěryhodností. Ta je v blockchainu vytvořena tím, že se celá síť shodne na uzavřeném bloku a přidá ho do řetězce, kdežto u tangleu, tangle je

pojmenování pro tento systém alternativy blockchainu, je nová transakce jen napojena na síť dvěma uzly. Schvalování transakcí ukáži na příkladu. Alice chce poslat zprávu Bobovi. Alice si vyžádá schválené transakce, na které by se mohla napojit, algoritmus jí vybere transakci, která zná hledaný uzel a je jeden až osm transakcí od konce sítě. Pak začíná kontrola proti spamu tím, že každý, kdo posílá transakci, ji musí konceptem PoW schválit. Tato metoda by pro výkonově slabé účastníky, jako jsou senzory, byla smrtelná, proto je možné senzor napojit na uzel, který senzoru věří a PoW vykoná za něj. Náročnost je v rámci setin wattů. Alice tedy schválí svoji transakci a transakce napojených uzlů i s jejich historií, tím je zachována bezpečnost sítě. Ukáže-li se nějaká transakce jako neplatná, celá větev se stává neplatnou a tedy nenapojitelnou. Poté Alice svým privátním klíčem podepíše zprávu a pošle ji Bobovi do sítě. Transakce se napojí na dvě předchozí vybrané transakce a čeká na propojení s takzvaným milníkem (milestone), což je transakce vytvořená koordinátorem, což je uzel, který je ověřený a vytváří milníky pro ověření transakcí v síti. Koordinátor nabourává decentralizovaný koncept, ale je to jen dočasné řešení. Již teď je na cvičné síti k dispozici decentralizovaný systém, který koordinátora vynechá.

Čtvrtým rozdílem zásadním pro IoT aplikace je, že každý účastník sítě neobsahuje databázi všech transakcí, které byly provedeny, ale jen jednu větev ze sítě. Tím je ušetřeno velké množství paměti, kterou IoT zařízení nemusejí mít. Pro příklad účetní kniha Bitcoinu má přes 500Gb dat paměti a Ethereum přes 300 a stále rostou [10][7][11][8].

V souvislosti s IoT je vhodné zmínit ještě jeden blockchain a to Helium.

### 2.4.5 Helium

Helium se významně liší od blockchainů, které jsou uvedeny výše, jelikož tyto blockchainy na rozdíl od Helia řeší problematiku ukládání, vyhodnocování a dostupnosti dat. Tedy zařízení je připojeno k internetu a data jsou místo do databáze zaslána do blockchainu. Kdežto Helium se zaměřuje na distribuci dat mezi zařízeními. Jinými slovy staví síť, která umožní vynechat internetové připojení v rámci IoT sítí. Tuto síť tvoří těžaři. Těžaři mají zařízení podobná routerům, která vzájemným propojením tvoří LoRaWan síť. Cílem hélia je vytvořit celosvětovou infrastrukturu, která by na rádiových vlnách umožnila propojení všech IoT zařízení. Ideální systém pro sdílenou ekonomiku, nebo do tovární výroby [9].

## 2.5 Peněženky

V předchozích kapitolách bylo popsáno, jak fungují bloky a všeobecně blockchain, teď je nutné více zmínit, jak fungují transakce. Zatím víme, že se ukládají do bloků po určitém čase a samotnou transakci nám potvrdí těžaři, ale to, jak je transakce zadána uživatelem, je obsahem této kapitoly. Pro další potřeby této práce si danou problematiku ukážeme na Ethereu. K propojení uživatelů a sítě slouží peněženky. Peněženky jsou vlastně softwareové aplikace, které pomáhají řídit blockchainový účet. Jednoduše řečeno, jedná se o bránu (gateway) pro ethereum systém. Brána je v informatice název aktivního zařízení, které zajišťuje propojení mezi dvěma sítěmi, které používají jiné ko-

munikační protokoly. Jednotlivé peněženky drží privátní klíč, který představuje vnitřní identifikaci peněženky. Vnitřní proto, že tento klíč není dostupný pro nikoho jiného než pro vás a představuje potvrzení prostředků na peněžence. Privátní klíč umožňuje kontrolu nad majetkem a chytrými kontrakty. Pro lepší představu jeden příklad. Bob posílá Alici jeden Ether. Bobova peněženka potvrdí (podepíše) privátním klíčem, že Bob má jeden Ether a že je skutečně jeho. Aby privátní klíč nebyl viditelný pro okolní uzly, asymetrickou kryptografií ho schová a pošle okolním uzlům. Každý z těchto uzlů veřejným klíčem zkontroluje, zda byla transakce podepsána privátním klíčem bez toho, aby daný uzel viděl soukromý klíč Boba, a pošle ji dál okolním uzlům. Tím se transakce rozšíří mezi všechny uzly sítě. V rámci potvrzování veřejným účtem je známo, i pro koho Ether je, a poplatek těžařům, po potvrzení každý uzel přidá transakci do poolu (místo pro nepotvrzené transakce) a počká, až jej těžaři vytěží. Ve chvíli vytěžení jsou transakce z poolu vymazány a Bobův Ether je připsán Alici. Takže peněženku můžeme brát jako bankovní účet v běžném světě. Uchovává hodnotu účtu a umožňuje transakce. Tento systém má spoustu výhod, ale jak už bylo několikrát řečeno, je decentralizovaný, ztratí-li uživatel privátní klíč, přichází o kontrolu nad svým účtem [19] [6].

## 2.6 Chytré kontrakty

Chytré kontrakty (smart contracts) jsou programy, funkce a data, fungující na blockchainu, V blockchainu jsou také uložena, takže mají svoji specifickou adresu stejně jako peněženky. Jsou druhem účtu v síti, vidí, posílají a přijímají transakce, ale na rozdíl od peněženek, nejsou ovládány uživatelem, ale fungují, jak byly naprogramovány. Jedním z hlavních a původních účelů chytrých kontraktů je kontrola tokenů (peněz), jako je například Ether, v síti. Chytrý kontrakt zní, jako že se jedná o něco složitého, ale vůbec tomu tak nemusí být. S chytrými kontrakty se většina lidí setkává celý život, jen nebyly na blockchainu. Jednoduchým příkladem je automat na pití. Do automatu vložíte mince (tokeny), jako zástavu a vyberete si nápoj, chytrý kontrakt zkontroluje, zda máte dostatečný obnos mincí (tokenů) na nákup nápoje, podle předem stanovených pravidel (programu). Pokud máte, dá vám nápoj, pokud ne, můžete vybrat jiný nápoj, nebo jsou vám vráceny mince. Stejně jako do automatu, můžete do chytrých kontraktů vkládat tokeny a navíc data, ta se podle předem stanovených (naprogramovaných) podmínek vyhodnotí a realizuje se akce, co se má stát. Jako příklad užití chytrých kontraktů v praxi uvedu nákup nemovitosti. Při této transakci se často využívá třetí strana, která uchová peněžní prostředky kupujícího, než prodávající převede nemovitost na kupujícího, a až pak jsou prostředky vyplaceny prodávajícímu. Tímto procesem se zvyšují náklady na koupi nemovitosti, jelikož je třeba zaplatit třetí stranu. V tomto případě by šla nahradit třetí strana chytrým kontraktem. Kupující strana složí peníze do chytrého kontraktu. Prodávající strana převede na katastru nemovitostí nemovitost kupující straně a autorizuje převod předem definovaným způsobem. Následně jsou chytrým kontraktem vyplaceny peněžní prostředky prodávající straně. Tím se stane obchod levnějším, nezávislým na třetí straně, to znamená méně komunikace s dalšími lidmi, tím se zrychlí proces. A není třeba třetí stranu hledat, stačí když bude takový chytrý kontrakt, jeden v celé síti. Pak oběma stranám stačí mít přístup do sítě, tedy peněženku a je to. Dále se chytré kontrakty hodí pro právní smlouvy, jelikož jsou díky vlastnostem blockchainu neměnitelné a nesmazatelné a interakce s chytrými kontrakty

je nevratná [12] [19].

Vytvoření chytrého kontraktu probíhá v několika krocích, nejprve je třeba chytrý kontrakt vytvořit, pro Ethereum je nejpopulárnější programovací jazyk Solidity, jedná se o relativně podobný jazyk jako je Java nebo C++. Po dopsání programu se program zkompiluje, převede do bytového kódu. Poté je vhodné chytrý kontrakt otestovat, zda funguje, jak má, než se nahraje do blockchainu. To se dá udělat přes některé peněženky, které umožnují cvičné prostředí s reálnými vlastnostmi blockchainu. Nahrání do blockchainu se dělá odesláním chytrého kontraktu jako transakce na nulovou adresu (0x0000000000000000000000000000000000000000). Nahrání trvá cca 15-30 vteřin, jelikož těžaři musejí program uložit. Tím má chytrý kontrakt svoji adresu jako peněženka, jak už bylo zmíněno. Smart kontrakt zpustím tím, že pošlu tokeny nebo data podle typu kontraktu na adresu kontraktu, jako kdybych dělal převod mezi peněženkami. Jakmile chytrý kontrakt přijme transakci, vykoná svoji činnost na decentralizovaném stroji. Chytrý kontrakt má svoji historii transakcí, která je přes něj dostupná [13] [19].

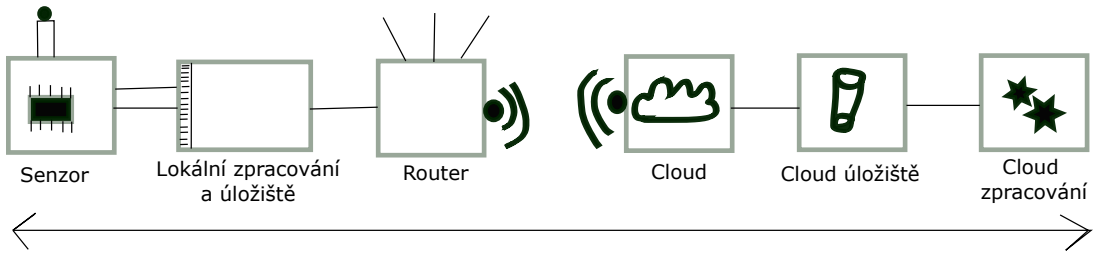
Při práci s blockchainem používáme cizí výpočetní techniku (stroje těžařů), ať už pro transakce nebo chytré kontrakty, a to něco stojí. Ethereum má poplatky pro těžaře vyřešené přes gass. Gass anglicky plyn je výpočetní jednotka pro nastavení poplatku. Je odvozena od náročnosti operace, tedy při kompilaci chytrého kontraktu se vezme v úvahu velikost zkompilovaného kódu a náročnost provedení programu. Tímto způsobem jsou vývojáři chytrých kontraktů motivováni, aby dělali programy, co nejefektivnější, protože každý zbytečný cyklus v cyklu bude stát něco navíc. Token Etherea je Ether, platit poplatky v Etherech by bylo celkem drahé, proto základní vyjadřovací jednotkou pro platby je Wei. Jeden Ether je $10^{18}$ Weiu. Poplatek za chytrý kontrakt může být v jednotkách Gigaweiu, tedy deseti tisíciny Etheru [19].

# 3 Internet věcí

Internet věcí neboli IoT (internet of things) je evoluční krok internetu, který tvoří světově rozšířenou infrastrukturu propojující stroje a lidi. Jednou z hlavních činností IoT je sbírání a následné zpracování dat a signálů. Tato data a signály jsou po zpracování předána zpět, ať už v podobě dat, která nám něco oznamují, nebo v podobě signálu, který prostřednictvím jiného zařízení dá pokyn k vykonání nějaké činnosti. IoT systémy se staly nedílnou součástí našich životů, ať už se jedná o chytrá auta, telefony, sdílená kola nebo třeba meteorologické stanice, které sbírají data o počasí, kvalitě vzduchu, hluku a tak dále. Stále více a více se uplatňuje nasazení IoT systémů do výroby, průmyslu, zemědělství, a dokonce i lékařství. Nesmím ovšem zapomenout na stále populárnější chytré domácnosti, budovy a do budoucna i celá chytrá města. Jak je z tohoto vyčerpávajícího výčtu zřejmé, IoT systémy jsou všude kolem nás a jejich využití v budoucnu bude ještě větší [21].

## 3.1 Požadavky na IoT

V této části se práce zaměřuje na to, z čeho se takový IoT systém skládá. Jak už bylo zmíněno, funkcí IoT je získat vstupy, vstupy zpracovat a pak vrátit v podobě výstupů. Vstupy obstarávají všemožné mikro elektromechanické senzory, ať už se jedná o teploměry, gyroskopy, chemické senzory, senzory pohybu nebo třeba i kamery. Data ze vstupních zařízení jsou v ideálním případě poslána do mikrokontroleru, který data upraví a ve smysluplné podobě jsou data následně poslána přes spojovací zařízení většinou na cloud, kde dochází ke zpracování a vyhodnocení dat. Tato data jsou pak vrácena zpět, buďto na uživatelské rozhraní, například v podobě grafu nebo se na displeji zobrazí aktuální hodnoty nebo jsou data vstupem pro jiný senzor či zařízení, které vykoná nějakou činnost, například se spustí ventilace, zatáhnou se rolety, zapne se topení, součástka ve výrobě je otočena motůrkem a tak dále. Schéma zapojení IoT systému je znázorněno na obrázku 4.




Obrázek 4: Schéma zapojení IoT systému

Při návrhu IoT systému je kladen důraz na pět základních aspektů: funkčnost, bezpečnost, rychlost škálovatelnost a cena.

### 3.1.1 Funkčnost

Funkčnost je myšlena jako vyřešení problému, něco od systému očekávám, tak aby systém poskytl očekávání na kvalitní úrovni. Tedy zvolení vhodných součástek, jejich propojení, napájení systému, jelikož mám-li IoT systém, který sbírá data o vlhkosti půdy uprostřed pole, kde není dostupná elektrická přípojka, tak musím nevrhnou systém tak, aby byl méně energeticky náročný, aby se nemusela každý den měnit baterka. Všeobecně se dá očekávat, že každé zařízení bude komunikovat s několika dalšími, tak vzít v úvahu infrastrukturu takovéto sítě.

### 3.1.2 Bezpečnost

V IoT je bezpečnost občas opomíjená, hlavně u komponent, kde na první pohled není jesné, co by mohl útočník získat, jako je například chytrý kávovar. Jenomže tento kávovar je připojen v lokální síti, a tak tím útočník získá přístup i k důležitějším částem sítě jako jsou chytré zámky nebo router. Nemluvně o hodnotě dat. Již teď je zpracování dat na značné úrovni a dá se předpokládat, že data porostou na ceně, a tedy i pokusy o jejich získání nebudou ojedinělé.

### 3.1.3 Rychlost

Rychlost reakce systému by se dala zahrnout do funkčnosti, ale považuji ji za tak důležitou kategorii, že ji udávám samostatně. Stále více IoT zařízení potřebuje reagovat v reálném čase, tedy nemůže se stát, aby se síť zahltila a systém čekal na odpověď několik sekund.

### 3.1.4 Škálovatelnost

Jelikož se očekává velký nárůst připojených zařízení je třeba počítat s větším zatížením sítě, ideálně aby se celá síť dala jednoduše rozšiřovat bez zpomalování vnitřních procesů.

### 3.1.5 Cena

Dalším faktorem je nákladnost systému, nejedná se anitak o počáteční náklady, které jsou zatím díky dostupnosti elektroniky poměrně malé, jako o pravidelné náklady za zpracování, ukládání a přenos dat.

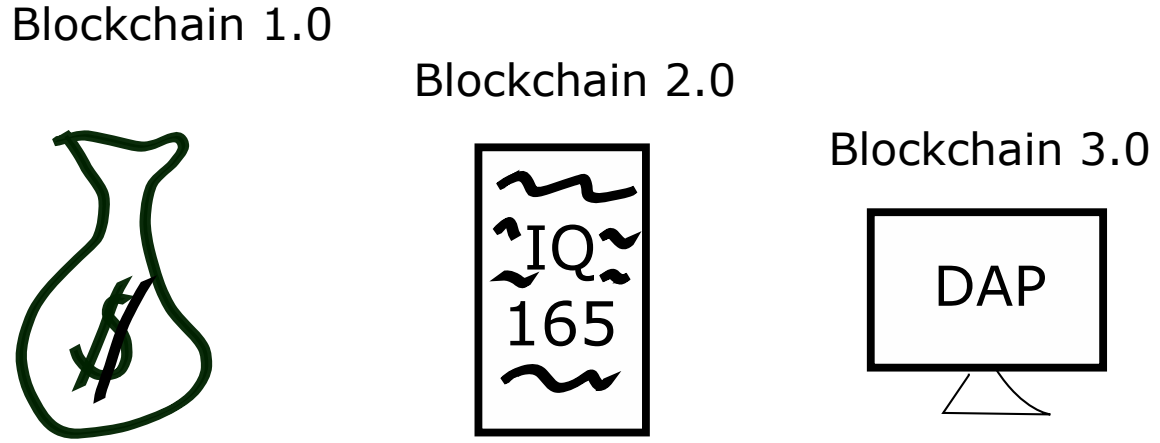
Požadavků je mnohem více, ale tyto považuji za hlavní. Všeobecně platí, že čím větší je brán důraz na první čtyři, tím víc cena roste, a proto může být lákavé některý z nich zanedbat.

V minulém roce přesáhl počet připojených IoT zařízení do sítě cifru 10 bilionů zařízení. Toto číslo se do pěti let ztrojnásobí a v roce 2030 se nejspíš přiblíží k hranici 80 bilionů zařízení. S tím, že několik stovek tisíc možná i miliónů se připojuje k internetu každou minutu. Potenciálem rozšíření IoT zařízení je kladen tlak na metody práce s daty a infrastrukturu, která zajišťuje komunikaci. Protože spousta IoT systémů vyžaduje komunikaci ideálně v reálném čase, což znamená, že zpoždění mezi vygenerováním

signálu a doručením výstupu musí být minimální, ale v cestě přitom je topologie sítě, zpracování dat cloudem a opětovné vrácení signálu. Zpoždění takovéto sítě může do budoucna znamenat otázku života a smrti. Aby mohla současná infrastruktura zvládnout takový nápor, je třeba nemalých finančních prostředků investovaných do hardware, i tak je možné, že to nebude do budoucna stačit [21].

# 4 Implementace blockchainu v IoT

V této kapitole se podíváme na to, jak se blockchain vyvíjel a jak s tím přicházely jeho implementace. Schéma vývoje je znázorněno na obrázku 5. Jako každá nová




Obrázek 5: Schéma evoluce blockchainu

technologie, blockchain se neobjevil v podobě, jak jej známe dnes, ale postupně se vyvíjel. Začalo to blockchainem 1.0, který nám přinesl kryptoměny. Blockchain 1.0 řeší měny, výměnu měn, transakce mezi uživateli a všeobecně platební systém. O blockchainu 2.0 hovoříme s využitím chytrých kontraktů. V této verzi se s chytrými kontrakty nepočítá mimo finanční svět a tak se věnuje rozšířením možností finančního světa, jako jsou otázky důvěry a spravedlnosti mezi stranami při obchodu. Tedy automatické úschovny, některé jednoduché právní smlouvy. Dokonce se zde řešily půjčky v kryptoměnách. Blockchain 3.0 už sahá za hranice finančních aplikací. Jedná se o rozšíření blockchainu decentralizovanými aplikacemi do všech možných oblastí lidské činnosti, ať už je to zdravotnictví, veřejná správa, řízení duševního vlastnictví, Iot systémy a mnoho dalších. Jednoduše řečeno blockchain 3.0 přináší nástroje pro uchování a autorizaci informací bez centrální autority. Dnes se nacházíme v časech, kdy se nám začíná formovat Blockchain 4.0, který představuje uplatnění, a tedy vylepšení industriálních využití. Pro lepší náhled do problematiky je v další části náhled do jednotlivých vývojových etap [29].

## 4.1 Blockchain 1.0

O blockchainu 1.0 bylo při vysvětlování, jak blockchain funguje, už zmíněno celkem dost informací, ale zde je rychlé shrnutí. Bitcoin byl v roce 2009 představen jako open-source platforma řešící dvojité poplatky současných platebních systémů nahrazením centrální autority distribuovanou účetní knihou mezi všechny zúčastněné uživatele. Síť sama si potvrzuje transakce a určuje, zda jsou rozumné, či nikoliv. Další implementace této generace blockchainu vznikaly dvěma způsoby. První je, že na blockchainu Bitcoin

vznikla takzvaná vidlička (rozdělení systému), update řekněme, který není povinný pro celou síť, ale rozdělí ji na dvě, nová síť využívá infrastrukturu té staré, ale přináší něco jinak. Pro rozlišení má nový token jako platidlo. Do této skupiny patří kryptoměny jako Litecoin a ZCash. Litecoin vnikl v roce 2011, když začal být blockchain při těžbě příliš náročný pro běžného uživatele a bylo třeba k těžení speciální výpočetní techniky. Vidlička Litecoin díky odlehčení umožňovala těžbu na běžném zařízení. Druhou možností je, že vznikne zcela nový blockchain, se svými tokeny a vlastnostmi. Takto vznikl blockchain Ethereum s tokenem ETH, který posunul blockchain do druhé generace [29].

## 4.2 Blockchain 2.0

Ethereum, jako nový blockchain přinesl jako první chytré kontrakty. Zveřejnil white-paper, ve kterém představil světu nové možnosti využití blockchainu. Ethereum zajišťuje, že předem definované podmínky v kódu budou vykonány, aniž by do nich šlo zasahovat zvenku. Nedá se měnit a tedy, co bylo domluveno to platí, a Ethereum blockchain zajistí dozor třetí strany (právníci, banky, notáři). Díky vlastnostem blockchainu je Ethereum vhodné pro aplikace vyžadující, vysokou důvěru, bezpečnost a trvanlivost, jako jsou finanční transakce, databáze majetku (registr nemovitostí), volební systémy, internet věcí [29].

## 4.3 Blockchain 3.0

Jak už bylo zmíněno blockchain 3.0 se věnuje decentralizovaným aplikacím takzvaným DAP. Jedná se o aplikace, které jsou postaveny na blockchainu, a některé příklady jsou uvedeny níže.

### 4.3.1 Systém dodání potravin

Ukázkovou implementací je systém pro dodávání potravin, na kterém pracuje potravinový řetězec Walmart společně s IBM. Dnes se stále více řeší, odkud daná potravina pochází, zda se jedná o maso z volného chodu, zda dostal farmář, obdělávající pole dostatečně zaplaceno a co vše bylo do jídla přidáno. Pro takový typ informací zatím nemají dodavatelé žádnou veřejnou infrastrukturu, a tak koncovému zákazníkovi nezbývá nic jiného než věřit, že informace poskytnuté prodejcem jsou pravdivé. Walmart a IBM vytvářejí veřejně dostupnou službu, která umožní zákazníkům walmartu sledovat cestu potravin od farmáře do obchodu. V rámci přeprav může být monitorována teplota nebo u farmáře půda. To má hned několik výhod. Jednak zákazník ví více, co jí, a v případě zkažené potraviny se dá dohledat možná příčina a následně stáhnout z trhu jen například jedno auto, kde vypadla lednička, a ne celou objednávku, což ušetří firmám, jako je Walmart nemalé množství finančních zdrojů. [2].

### 4.3.2 Přeprava květin

Podobnou implementací je systém na přepravu květin z Keni do Nizozemska. Tento obchodní styk je velmi administrativně náročný, totiž do administrativy je zapojeno

několik stran (přístavy, města, státy). Komunikace mezi nimi probíhala e-mailem nebo fyzicky, což daný obchod neulehčovalo a někdy i zdrželo. IBM s Maersk postavilo nový systém na blockchainu, kde mají obchodníci nahrané certifikace a povolení a zaznamenávají se do něj jednotlivé kroky procesu. Například: dojde-li k zaplacení cla, může se naložit zásilka do kontejneru. Firma se tím může více soustředit na přepravu květin než na administrativu kolem této přepravy [3].

### 4.3.3 TimeSeries

Další firma zabývající se logistikou. Umožňuje nalézt kontejner, zjistit, kde se nachází a veškeré přidané informace k němu a s oprávněním se dají ke kontejneru přidávat data a dokumenty[30].

### 4.3.4 Auto mobilita

IoT a chytrá auta jdou ruku v ruce, tak není překvapivé, že si i do toho odvětví blockchain našel svoji cestu. V auto mobilitě se blockchain věnuje 4 odvětvím. Automatické platby za palivo, chytré parkování, automatické řízení dopravy a samozřejmě i autonomní auta. Pro názornost rozeberu příklad chytrého parkování. Řidič začne hledat místo k parkování, napojí se na blockchain, kde jsou napojena parkovací místa, která díky senzorům vědí, zda jsou volná či nikoliv a tato informace je uložena v blockchainu. Auto je navedeno na nejbližší volné místo. Řidič nemusí řešit poplatky za parkování, celý proces je vyřešen díky chytrým kontraktům automaticky přes peněženky. Řidič ušetří čas a rychleji najde místo na parkování téměř bez starostí. Se spojením se samořízenými auty rovnou může autu poskytnout informace o rozměrech parkovacího stání a okolní situaci pro hladké zaparkování [30].

### 4.3.5 Chytré domácnosti

IoT je základní stavební kámen chytrých domácností. Zapojení blockcahinu do chytrých domácností pomůže vyřešit dva problémy, které chytré domácnosti, řeší a to zabezpečení komunikace a ukládání dat, a umožní vynechání centrální autority, která nemá omezení, jak nakládat s daty, která jí jsou posílána. Jedním z prvních průkopníků zapojení blockchainu v této oblasti je australská telekomunikační a mediální firma Telstra. Ta zapojila blockchain do systémů chytrých dveří, ať už pomocí otisků prstů, rozpoznání hlasu nebo obličeje. Jakmile jsou do blockchainu identity uloženy, nejdou upravit, jen odpojit, a tím jsou zabezpečeny a systém se otevře jen oprávněné osobě [23].

### 4.3.6 Farmaceutika

Jde o podobný případ jako u dodavatelského řetězce. Stejně jako u potravin je u léčiv rozhodující, odkud pochází a jaký je jejich stav. Mediledger je firma řešící transparentnost v původu léčiv a v přístupnosti k jednotlivým lidem (doktoři, koncoví zákazníci).

Plus zajišťuje jednoduchý systém na placení léčiv a stejně jako u potravin pomáhá efektivně stahovat špatná léčiva [30].

### 4.3.7 Zemědělství

O potravinách už byla řečena v kapitole o distribuci, ale kombinace těchto dvou technologií se využívá i na farmách. Senzory se dají do polí a posílají data o úrodě. Firma, která se tímto zabývá je Pavo. Díky Pavu mohou jednotlivé farmy porovnávat svoje výsledky a sdílet know-how. Potravinové řetězce mají možnost si pak vybrat dodavatele a přes Pavo Marketplace i rovnou obchodovat. Další firma, která využívá blockchain, je Apical, ta se zabývá palmovým olejem a využívá tento protokol, aby dokázala, že půda, na které palmy pěstují nebyla původně lesním pralesem [14].

### 4.3.8 Vodní hospodářství

Ve vodním hospodářství jsou hned dvě firmy Libelium a Airalab, které spolu spolupracují a využívají Ethereum blockchain pro ukládání dat v reálném čase, která nasbíral ze vzorků vody dron na řece Volga. Dále firma Aquai s pomocí NetObjex na blockcainu provozuje aplikaci, která se snaží zabránit plýtvání vody [22] [24].

### 4.3.9 Měření radioaktivity

Firma Clinitraq využívá IoT blockchain pro měření dozimetrem v nemocnicích, některé systémy vyhodnocovaly data až 60 dní, kdežto v kombinaci s IoT a blockchainem je celé měření do 60s. Takto rychlé vyhodnocení pomáhá chránit pracovníky v prostředí, kde je radiace [25].

# 5 Ukázková aplikace

Tato část práce se věnuje návrhu, který ověří a ukáže použitelnost a funkčnost technologie blockchain pro IoT systémy. Ukázkovým systémem je kontrolní systém pracovní docházky. Pracovník přijde do práce, pípne si osobní kartou a při odchodu pípne znova a rovnou mu jsou za uplynulý čas zaslány příslušné finanční prostředky. Všechno je zcela automatizované, jako nosná databáze je použita technologie blockchain, nebo technologie z ní vycházející, vnitřní procesy jsou zpracovány chytrými kontrakty a ke čtení karet je použita RFID technologie. Praktická část je rozdělená na několik částí. První se zaobírá výběrem a porovnáním blockchainů jako nosné technologie pro databázi. Druhá se věnuje návrhu architektury systému od senzoru po chytrý kontrakt. Třetí závěrečná část se zabývá implementací části navrženého systému.

## 5.1 Výběr blockchainu

Při výběru blockchainu je nejprve důležité se zamyslet, co by měl systém splňovat. Tyto požadavky se podobají požadavkům na IoT systémy. Při návrhu tohoto systému se snažím o co nejvyšší rychlost a bezpečnost systému. Počítám s růstem firmy, síť by tedy měla být ideálně nekonečně škálovatelná, aniž by došlo k narušení jiných parametrů, a ideálně s co nejnižšími náklady. Ani tak nejde o jednorázové náklady spojené s pořízením, ale o ty dlouhodobé spojené s chodem sítě. Plus určitě potřebuji blockchain podporující chytré kontrakty. Původní myšlenka byla, že postavím systém na Ethereu, jelikož se jedná o nejznámější a nejlépe podporovaný blockchain pro tvorbu těchto systémů, ale při hlubším zabřednutí do problematiky se ukázal jako nevhodný, a to skoro ve všech kategoriích, až na bezpečnost. Uzavření bloku u Etherea trvá přibližně 15 vteřin, což by byla pro tento systém přijatelná rychlost pro autorizaci transakce, ale Ethereum blockchain, jelikož je populární, je používaný více, než zvládá (více než 15 transakcí za vteřinu). Tím se transakce hromadí a na jejich autorizaci, tedy přidání transakce do bloku, se musí čekat déle, v závislosti na zatížení sítě, tedy Ethereum blockchain není škálovatelný. Aby se transakce vyřídila rychle, musel by se zaplatit vyšší poplatek jako motivace pro těžaře při výběru transakce pro přidání do uzavíraného bloku a tím se cena za transakci momentálně pohybuje mezi 3-7 dolary. Cena, i když se může zdát velmi vysoká, nemusí být nejvíce rozhodující faktor, jelikož díky vlastnostem blockchainu se může firma stát součástí sítě a tím vytěžit tokeny, které zaplatí provoz. Toto je typické pro PoW blockchainy, tak jsem se podíval po PoS blockchainu. Neblio jako PoS blockchain chvilku vypadal ideálně, je méně známý, rychlejší, ale problém se škálovatelností má stále, což pro IoT sítě, když vezmu v potaz očekávaný nárůst, není ideální. S problémem škálovatelnosti se potýkají zatím všechny blockchainy už ze své podstaty, jelikož blok má svá specifika a rychlost uzavírání bloků také a každý blockchain s potenciálem svou kapacitu dříve či později naplní, protože přiláká uživatele a ti jej zahltí transakcemi. Ideální by byl systém s vlastnostmi blockchainu, jako decentralizace, bezpečnost, ale s lepší škálovatelností. Tedy aby přibývající počet transakcí, neovlivnil rychlost autorizace a ideálně ani cenu. Toto nabízí Tangle jako je IOTA. Jelikož se jedná o poměrně novou technologii, jak jsem zmínil v popisu IOTA technologie, tak není úplně decentralizovaná, ale to by se mělo v dohledné době také vyřešit. To samé platí o chytrých kontraktech. V aktuální stabilní verzi ještě nejsou podporovány, ale na

testovací síti se již s nimi zaobírají. Technologie Tangle vyšla z blockchainu a jedná se o novou technologii speciálně upravenou pro IoT systémy. Je bezpečná, transparentní a každé připojené zařízení se aktivně podílí v síti, tedy je dokonale škálovatelná, jelikož s přibývajícím počtem připojených roste i počet validátorů. Díky tomu, že každý připojený uzel se účastní sítě, není třeba těžařů a transakce v síti jsou bez poplatků. Tedy náklady na provoz sítě jsou spojeny jen s energií spotřebovanou uzly. Rozhodl jsem se tedy v návrhu systému využít technolgii Tangle, implementaci IOTA, i když se nejedná přímo o blockchain, ale o technologii pro tyto účely vhodnější.

## 5.2 Možnosti vývoje na IOTA Tangle

Vývoj na IOTA síti není momentálně zcela triviální záležitostí, jelikož samotný projekt je od roku 2016 neustále ve vývoji. Od té doby se strategie několikrát vyvinula na základě zpětné vazby v odvětví, což vedlo ke změně podporovaných knihoven, nedokonalé aktualizaci návodů a z toho pramenících obtíží. Na druhou stranu komunita kolem IOTA projektu neustále roste, vzniká stále víc knihoven a počet programovacích jazyků, které se dají pro vývoj použít. Vývojářská wiki projektu IOTA dokonce obsahuje záložku s tutoriály, které zatím nejsou pro vývoj moc užitečné, ale hezky ukazují, jak se na projektu pracuje a jakým směrem se chce projekt ubírat. Ale podle vývojářů by se měl vývoj již ustálit a knihovny, které vznikají teď, by měly být podporovány i v dalších verzí IOTA Tangle. V této kapitole rozeberu možnosti vývoje a podporované programovací jazyky a tím ukáži, co vše lze dnes na IOTA síti vytvářet.

Od dubna 2021 je k dispozici IOTA 1.5, která je funkční a připravená pro vývoj aplikací, ale není ještě plně decentralizovaná, stále počítá s koordinátory. Ale nabízí možnost začít vyvíjet aplikace na Tangle. IOTA 2.0 řeší problém s decentralizací a vyřazuje koordinátora. Jak jsem zmínil výše, mělo by již docházet ke stabilizaci vývoje s protokolem IOTA 1.5, tedy nástroje, knihovny a API fungující v IOTA 1.5 by měly být funkční i v IOTA 2.0. To znamená, že projekty vytvořené na dnešní kódové základně by měly být použitelné bez větších úprav i v dalších verzích.

### 5.2.1 IOTA 1.5

Úloha prtokolu IOTA 1.5 je jasná. Má umožnit vývojářům tvořit projekty na IOTA Tangle již teď, nemuset čekat na dotažení decentralizace a, až se vše dodělá, tak plynule přejít na protokol IOTA 2.0. Síť fungující na protokolu IOTA 1.5 je již rychlá, autorizace transakce trvá kolem 10 vteřin, je spolehlivá a dostatečně škálovatelná. IOTA 1.5 podporuje dvě sítě, hlavní Mainnet a vývojářskou pro testování aplikací Devnet. Přehled dění na hlavní síti můžete najít na odkazu [4] i s krásnou animací, jak se připojují transakce do Tangle. Do sítě mohou zasahovat 2 entity. Uzly, například peněženky, a klienti. Uzly jsou účastníci sítě a podílejí se na uchovávání transakcí Tangle. Mají 2 varianty plnou a lehkou. Plná varianta obsahuje celou databázi Tangle a měla by běžet 24 hodin 7 dní v týdnu, tedy jedná se o uzel běžící hlavně na serveru. Celá technologie je navržena pro připojitelnost IoT zařízení, takže požadavky na uzly dokáží splnit i mikrokontrolery, jako je například Raspberry Pi 4. Lehká varianta uzlu ukládá jen posledních pár transakcí a je vhodná pro počítače, mobilní telefony a podobné přístroje,

od kterých se neočekává trvalé připojení. Pro napojení do Tangle se ale musí napojit na takzvaný hostující uzel, který je plnou variantou. IOTA 1.5 nabízí dvě možnosti práce s uzly, Hornet (Sršeň) a Bee (Včela). Hornet je původní verze a podporuje pro vývoj programovací jazyk Go. Bee je novější varianta v programovacím jazyce RUST. Pro ulehčení vývoje aplikací nabízí IOTA dvě základní knihovny Client.rs a Wallet.rs obě knihovny jsou napsané v programovacím jazyce RUST, ale je možné s nimi pracovat v Pythnu a v Node.js. Knihovna Client.rs slouží k interakci se sítí Tangle,jako je například ukládání a čtení transakcí a jim podobné operace. Wallet.js je pro práci s peněženkami, a umožňuje tedy posílání zprávy uchovávající hodnotu (tokeny) sítí. Základní funkce těchto dvou knihoven jsou pro IoT aplikace, které většinou běží na mikrokontrolerech, upraveny do knihovny lib.c, která je napsána v programovacím jazyce C a bude také v této práci použita při implementaci. Stejná úprava těchto dvou základních knihoven je v podobě knihovny lib.js pro Typescript, kterou je možné využít ve webových prohlížečích, a lib.go pro programování v Golangu. IOTA vývojáři dále nabízí tři zajímavé knihovny. První knihovna Stronghold, česky pevnost, slouží pro zabezpečení digitálního tajemství jako jsou soukromé klíče. Využívá protokolu, který měl chránit seedy, ale dá se využít i pro tyto účely. Využívá vlastní komunikační vrstvu založenou na p2p principu. Druhá je knihovna Identity, česky identita, je navržena pro potvrzování identity lidí a organizací mezi všemi a vším. Funguje jako sjednocující vrstva důvěry. Třetí a zatím poslední knihovna je knihovna Stream. Tato knihovna slouží pro uspořádání toku dat do jednotné struktury, díky tomu ulehčuje lokalizaci dat z jednoho zařízení v rámci celého Tangle.

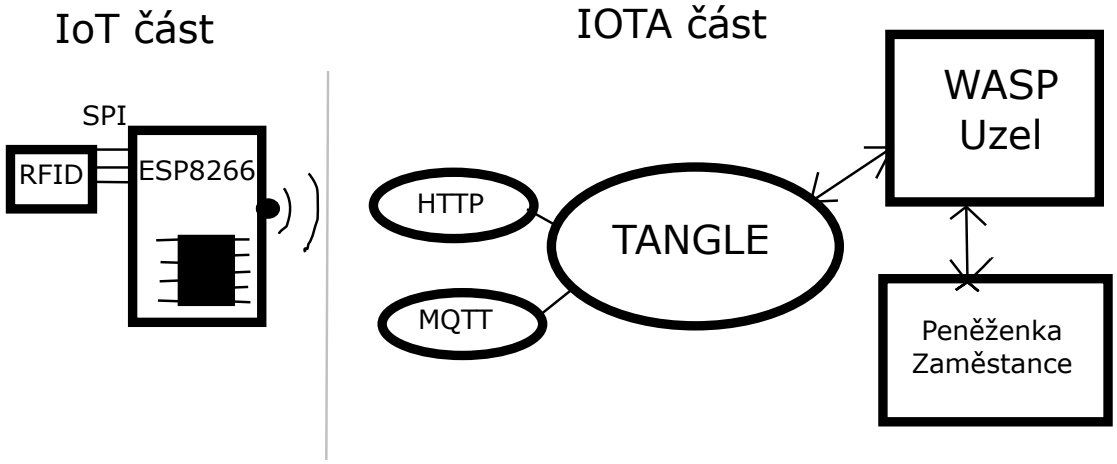
### 5.2.2 IOTA 2.0

IOTA 2.0 je protokol, který udává, jak by se měly uzly chovat v decentralizovaném Tanglu. Ještě není zcela hotov, momentálně se testuje a vylaďuje už skoro rok na testovací síti. Protokol IOTA 2.0 je zatím testován na testovací síti GOShimmer a mají hotových 5/11 cílů. IOTA 2.0 ponechává ukládání dat a funkce, které přinesla IOTA 1.5, plus navíc kromě decentralizace, která je jedním z nejdůležitějších vylepšení IOTA protokolu, přináší do IOTA také chytré kontrakty. Tedy umožňuje komukoliv vytvořit inteligentní smluvní blockchain a ukotvit jej do IOTA Tangle. Celé to funguje tak, že IOTA sama o sobě nevytváří bloky a chytré kontrakty, ale upevní na sebe libovolný blockchain, který chytré kontrakty obstará, v případě, že je transakcí v blockchainu moc a došlo by ke zdražení vyhotovení transakcí, jednoduše se přidá další blockchain, a tím odpadne přehlcení sítě a vše poběží zase rychle a za nízké ceny. Jelikož každý může vytvořit a přidat svůj vlastní blockchain a nastavit jeho pravidla, tak možností je opravdu mnoho, jelikož si můžete udělat blockchain na míru a nastavit si tam vlastní poplatky. Můžete dokonce nastavit přístupová práva k blockchainu jen pro vybrané uzly a tím mít svoji zabezpečenou síť bez vystavení veřejnosti. V jednom blockchainu může pracovat více typů virtuálních strojů. Zatím jsou dostupné dvě chytré smlouvy založené na RUST jazyce takzvaně Wasm a EVM (Ethereum virtual machine) v jazyce Solidity. Toto všechno dodává IOTA chytrým kontraktům větší komplexnost a možnosti využití než běžné chytré kontrakty. Pro funkčnost chytrých kontraktů v IOTA protokolu, přišla IOTA 2.0 s třetím typem uzlu pojmenovaným Wasp (Vosa). Wasp slouží jako validátorský uzel propůjčující výpočetní techniku do vyrobeného blockchainu. V

praxi to vypadá tak, že se jednotlivé uzly propojí a vytvoří virtuální stroj zajišťující chod blockchainu.

## 5.3 Návrh IoT systému s IOTA Tangle

V této části práce se nachází návrh systému pro evidenci docházky zaměstnanců s automatickou výplatou s použitím RFID technologie a IOTA databáze. Návrh je rozdělen do dvou částí: IoT část a IOTA část. Schéma celého návrhu je na obrázku 6. Jednotlivé části jsou popsány v následujících dvou kapitolách. V této části jsem se rozhodoval, jak celý koncept uchopit, jestli vyjít z toho, co je možné dnes na IOTA Tangle vytvořit a, nebo pojmout návrh více teoreticky a navrhnout to tak, jako že je IOTA 2.0 již plně funkční. Rozhodl jsem se pro více teoretickou variantu, jelikož celý systém i téma bakalářské práce se točí kolem chytrých kontraktů.




Obrázek 6: Schéma IoT systému s IOTA Tanglem

### 5.3.1 IoT část

Tato část je věnována sběru data a jejich předzpracování a následnému odeslání dat dál do sítě. Ke sběru dat slouží RFID senzor MFRC-522 RC522. RFID (radio frekvency identification) senzor je senzor, který na základě radiových frekvencí umí číst data z karet. Pro tuto aplikaci je to vhodná technologie, jelikož, dostane-li se karta do magnetického pole čtečky, je indukováno napětí na kartě, které pošle v případě správného oprávnění data z karty zpět na čtečku. Tedy stačí, když má každý zaměstnanec svoji kartu, kterou přiloží, a je to. V případě zabezpečení vstupu do budovy se dá zámek dveří zkombinovat s tímto systémem. RFID čtečka komunikuje pomocí SPI protokolu s mikrokontrolerem. Jako mikrokontroler pro zpracování dat a odeslání dat do sítě jsem hledal mikrokontroler s WIFI senzorem, nakonec jsem vybral hlavně kvůli jeho momentální dostupnosti mikrokontroler ESP8266 s vestavěným WIFI senzorem. Dalším rozhodujícím faktorem byl fakt, že knihovna IOTA lib.c podporuje tento mikrokontroler. Mikrokontroler je připojen do lokální sítě a pro napojení na IOTA Tangle má dvě možnosti: lokální síť je plným uzlem IOTA Tanglu a, nebo se pomocí API připojí

na plný uzel. Pro lehkost systému využiji druhou možnost, kterou dokáže obstarat i sám mikrokontroler, nebude k tomu potřeba server, ale pouze přes router pošle transakci. Pro provedení transakce mám opět dvě možnosti, buď HTTP (Hypertext Transfer Protocol) určený pro komunikaci s WWW serverem, nebo MQTT (Message Queuing Telemtry Transport), což je jednoduchý protokol pro výměnu zpráv mezi zařízeními často používaný v aplikacích internetu věcí. Pro návrh jsem se rozhodl využít HTTP protokol. Celá část systému funguje tak, že na kartě je nahráno ID plus volitelné další údaje. Když je karta do deseti cm od čtečky, čtečka přečte data a zaznamená zprávu o příchodu zaměstnance s časem příchodu a jeho ID. Zpráva je pomocí API a http protokolu uložena do Tangle. Co se týče softwareového hlediska, tak kód v mikrokontroleru je psán v programovacím jazyce C, jelikož je jednoduchý a vhodný pro mikrokontrolery ESP. Samotný program je psán v Visual Studio Code, jelikož umožňuje nainstalování rozšíření ESP-IDF, což je ID vhodné pro kompilaci kódů do ESP mikrokontrolerů.

### 5.3.2 IOTA část

Zde se jedná o zajímavější část této práce, v klasickém IoT systému by zde byla cloudová databáze, ale celá práce se věnuje tomu, zda se nedá nahradit jiným řešením, řešení jsem nalezl v IOTA Tangle. Již se nacházím v bodě, že transakce (informace) o vstupu zaměstnance je uložena do Tangle pomocí pevného uzlu typu Wasp. Pro uzel typu Wasp před uzlem typu Hornet nebo Bee jsem se rozhodl proto, že uzel typu Wasp je napsán v jazyce RUST, který je podporovaný v IOTA 2.0 napříč všemi uzly a knihovnami, to by platilo i pro uzel typu Bee, ale jen uzel typu Wasp podporuje chytré kontrakty, takže pro jednotnost a efektivitu se zdá jasnou volbou. Tento uzel zároveň zaštiťuje zaměstnavatele a z jeho peněženky jsou později vypláceny prostředky zaměstnanci. Tím, že zaměstnavatel provozuje vlastní plný uzel, se aktivně podílí v síti a pomáhá zachovávat decentralizaci a tím bezpečnost svých dat s minimálními náklady. Wasp uzel pošle data i do chytrého kontraktu. V tu chvíli je zavolán chytrý kontrakt poprvé. Zkontroluje, zda se jedná o příchod, či odchod. Jedná se o příchod, a tak nedělá nic dál. Chytrý kontrakt je také napsán v programovacím jazyce RUST. Ve chvíli, kdy je detekována další transakce, která je již odchod, chytrý kontrakt odečte počet odpracovaných hodin, vynásobí hodinovkou a převede prostředky z peněženky zaměstnavatele na peněženku daného zaměstnance, která je lehkou variantou uzlu, to znamená, nemusí běžet stále. Tyto údaje se pomocí knihovny Streem dávají do organizované struktury. Na první pohled nemusí vypadat, že se jedná o něco světoborného, ale jedná se o zcela automatizovaný proces, jehož velkou výhodou je, že data se dají dále využívat. Příkladem je konec roku, kdy je čas řešit daně. Struktura dat, do které jsou data ukládána, se zpřístupní chytrému kontraktu finančního úřadu a zcela automaticky jsou rázem vyřešeny daně, sociální i zdravotní, jelikož IOTA nabízí i ověřování identity. ¨

## 5.4 Implementace

Jelikož jsem se rozhodl pro návrh na systému, který ještě není zpřístupněn na stabilní verzi, musel jsem se rozhodnout, které části návrhu lze implementovat i na protokolu IOTA 1.5. Druhá část kolem IOTA Tangle počítá s přístupností verze protokolu IOTA

2.0, a tedy je momentálně neimplementovatelná. Kdežto první část IoT systému s uložením do Tangle je dostupná i v IOTA 1.5. Proto jsem se rozhodl v implementační části zaměřit na první část předchozího návrhu. Pro napojení mikrokontroleru do Tangle slouží IOTA knihovna lib.c, která poskytuje základní prvky z knihovny Client.rs a Wallet.rs, tedy umožňuje napojení mikrokontroleru na Tangle. Stejně, jak uvádím v předešlé kapitole, pro kompilaci souboru použiji ESP-IDF environment. Jelikož se jedná o novou technologii, tak se nedá najít moc návodů, jak postupovat a pro případné chyby neexistuje příliš velké komunita, která by je pomáhala řešit. Ale IOTA vývojáři poskytují na gitu potřebné knihovny i s jednoduchými návody použití pro práci s mikrokontrolerem ESP8266. Existují dva návody, jak postupovat, a ty jsem se rozhodl použít, liší se v tom, že jeden je pro HTTP komunikaci s uzlem a druhý komunikuje pomocí MQTT. Návod se dá rozdělit na 2 části, kód nahrávaný do mikrokontroleru, který dostane požadovaná data pomocí HTTP protokolu na lokální síť, a kód Bee uzlu v programovacím jazyce RUST, který data připojí na Tangle. První část, tedy ta, co se týče mikrokontroleru, pracuje bez větších obtíží, ale uzlová část, selže při práci s makefilem, jelikož základní knihovna od vývojářů IOTA byla pozměněna, ale již nebyly udělány změny v makefile umožňujícím propojení mikrokontroleru a uzlu, uzel s potřebnou konfigurací nejde spustit kvůli chybějící knihovně. Jelikož se jedná o velký program napsaný v jazyce RUST, nepodařilo se mi úspěšně změnit potřebné věci k rozchození programu. To samé jsem vyzkoušel pro MQTT komunikaci, ale základ kódu, který zajišťuje chod uzlu a který zabránil zprovoznění první možnosti, byl i v tomto případě osudový. Po důkladném pátrání jsem zjistil, že daný postup byl vývojáři zpřístupněn v roce 2019, zatímco protokol IOTA 1.5 byl spuštěn v dubnu 2021 a s ním se změnila většina knihoven. Po vyzkoušení práce s knihovnou lib.c používané v tomto návodu jsem zjistil, že i ta je zastaralá a nelze použít kvůli četným změnám úplně. Pátral jsem tedy po jiném řešení. Velká většina propojení jakýchkoliv mikrokontrolerů s Tangle je z let 2018 až 2020 a tedy již nepoužitelná. Ale pak jsem narazil na jedno řešení z července 2021 zveřejněné na oficiálních stránkách IOTA technologie. Toto řešení působilo vhodně. Nová knihovna lib.c po rozběhnutí IOTA 1.5, pouze nepodporovala mikrokontroler ESP 8266, ale podporovala ESP 32, což je výkonnější mikrokontroler ESP řady, který také obsahuje WIFI modul. Nároky na výkonnost zde byly nejspíš kvůli tomu, že tato metoda neposílala data na jiný uzel, ale zařízení se rovnou samo o sobě připojovalo do sítě právě pomocí knihovny lib.c. Rozhodl jsem se tedy pro změnu mikrokontroleru a pokusil se o implementaci. Bohužel, jakmile došel proces kompilace k buildu, tak makefile, který build zastřešuje, narazil na obdobný problém a to, že hledá knihovnu, která by měla být obsažena v lib.c, ale již kvůli změnám není. Tento problém se mi nepovedlo kvůli komplexnosti systému vyřešit a zatím jsem neobjevil způsob, jakým se pomocí mikrokontroleru řady ESP k Tangle připojit, i když sami vývojáři vyrábějí kódy pro jejich využití, ale vzhledem k robustnosti vývoje, nestačí aktualizovat všechny pomocné soubory a vytvoření vlastních takto komplexních souborů je zatím nad moje možnosti.

# 6 Závěr

Cílem této práce bylo seznámit s technologií blockchain a poukázat a prozkoumat potenciál propojení blockchainu s IoT. Vlastnosti blockchainu jako je bezpečnost a decentralizace by svoje užití v IoT určitě našly, jelikož bezpečnost je u IoT systémů často opomíjené téma i přes jeho důležitost. Decentralizace by zabránila výpadkům a nedostupnosti cloudových úložišť. Jako velkou nevýhodu ovšem vnímám škálovatelnost blockchainu a s tím při naplnění kapacity snížení rychlosti a zvýšení ceny. Blockchain jako takový se ukázal použitelný jen v některých IoT systémech. Při pátrání jsem ovšem objevil technologii Tangle, která řeší právě problém škálovatelnosti, a tedy i rychlosti a ceny v IoT systémech. Jedná se o technologii vycházející z blockchainu stavěnou pro IoT systémy, která dle mého názoru představuje budoucnost ukládání dat a práce s nimi v IoT systémech, jelikož poskytuje větší důvěru a bezpečnost než cloudová řešení a je skoro dokonale škálovatelná, tedy může být řešením nabývajícího počtu IoT zařízení připojených v síti, která by do budoucna mohla přetížit síť a tím ji zpomalit. Momentálně je komunikace IoT systémů s Tangle stále pomocí internetových protokolů, takže přetížení sítě je stále hrozbou, ale v kombinaci s dalším zmíněným blockchainem a to Heliem, které staví infrastrukturu LoRaWan pro internet věcí, by se dal vytvořit velký IoT systém včetně komunikační i úložné vrstvy, který by byl propojen bez internetu, a tedy by jej absolutně nezatěžoval. IOTA sama o sobě je bez poplatků, takže jediné náklady na tuto síť by byly spojeny s drobným poplatkem pro provozovatele Helium sítě, kde by ovšem každý účastník mohl být součástí, a tedy být i nazpět odměňován za zprostředkování sítě, a s cenou jednotlivých chytrých kontraktů připojených na IOTA Tangle, tedy náklady spojené s propůjčením výpočetní techniky cizích strojů. Díky zdokonalování zpracování dat mají data převážně generovaná IoT systémy stále větší cenu a je škoda, aby na těchto datech, která produkuje každý z nás, benefitovali jen provozovatelé cloudů. V práci jsem měl za úkol daný systém implementovat a, i když se mi to nepodařilo, tak práci hodnotím úspěšně, jelikož jsem se dostal k technologiím, které jsem ani nevěděl, že existují, ale perfektně zapadají do mých představ ohledně vývoje infrastruktury systémů internetu věcí.

# Reference

[1] *A comprehensive survery of blockchain: From theory to IoT applications and beyond.*

[2] *Walmart case study.* [online]. Available: https://www.hyperledger.org/resources/publications/walmart-case-study, Accessed: 12.2.2022.

[3] *TradeLens blockchain-enabled digital shipping platform continues expansion with addition of major ocean carriers Hapag-Lloyd and Ocean Network Express.* [online]. Available: https://www.maersk.com/news/articles/2019/07/02/ hapag-lloyd-and-ocean-network-express-join-tradelens, Accessed: 12.4.2022.

[4] [online]. Available: https://explorer.iota.org/mainnet/visualizer/, Accessed: 17.5.2022.

[5] *Proof of Stake.* [online]. Available: https://wiki.p2pfoundation.net/Proof_of_Stake, Accessed: 19.2.2022.

[6] *Co je to Gateway?* [online]. Available: https://it-slovnik.cz/pojem/gateway, Accessed: 22.2.2022.

[7] *Data Transfer.* [online]. Available: https://wiki.iota.org/learn/about-iota/data-transfer, Accessed: 22.4.2022.

[8] *Energy Efficiency.* [online]. Available: https://wiki.iota.org/learn/about-iota/energy-efficiency, Accessed: 22.4.2022.

[9] *helium.* [online]. Available: https://docs.helium.com/, Accessed: 22.4.2022.

[10] *An Introduction to IOTA.* [online]. Available: https://wiki.iota.org/learn/about-iota/an-introduction-to-iota, Accessed: 22.4.2022.

[11] *IOTA Value Transactions.* [online]. Available: https://wiki.iota.org/learn/about-iota/value-transfer, Accessed: 22.4.2022.

[12] *INTRODUCTION TO SMART CONTRACTS.* [online]. Available: https://ethereum.org/en/developers/docs/smart-contracts/, Accessed: 23.2.2022.

[13] *Solidity.* [online]. Available: https://soliditylang.org/, Accessed: 23.2.2022.

[14] *Palm Oil SUSTAIN – A Traceability Solution With Blockchain.* [online]. Available: https://www.apicalgroup.com/articles/palm-oil-sustain-a-traceability-solution-with-blockchain/, Accessed: 23.4.2022.

[15] *Technology Overview, About us,..* [online]. Available: https://nebl.io, Accessed: 24.2.2022.

[16] *What is Neblio?* [online]. Available: https://simpleswap.io/what-is/neblio, Accessed: 24.2.2022.

[17] *IoT Chain.* [online]. Available: https://iotchain.io/, Accessed: 25.4.2022.

[18] *Merkle Tree*. Available: https://en.wikipedia.org/wiki/Merkle$_t ree$, [*online*].*Accessed* : 17.2.2022.

[19] ANTONOPOULOS, A. M. *Mastering Ethereum*. O'Reilly UK Ltd., 2018.

[20] D. J. YAGA, P. M. MELL, N. R., AND SCARFONE, K. *Blockchain technology overview*. NIST, Gaithersburg, MD, USA, rep. NISTIR-8202, 2018.

[21] DIMITRIOS SERPANOS, M. W. *Internet-of-Things (IoT) Systems - Architectures, Algorithms, Methodologies*. Springer International Publishing AG, 2018.

[22] ENKERLIN, M. *Aquai The Smart Water Company*. [online]. Available: https://www.netobjex.com/casestudy/aquai/, Accessed: 23.4.2022.

[23] FOYE, B. *Telstra quietly switches on internet of things network*. [online]. Available: https://www.crn.com.au/news/telstra-quietly-switches-on-internet-of-things-network-473757, Accessed: 26.4.2022.

[24] GERONI, D. *Blockchain With IoT – Top Blockchain IoT Use Cases*. [online]. Available: https://101blockchains.com/blockchain-iot-use-cases/, Accessed: 23.4.2022.

[25] KRISHNAREDDY, D. D. *Clinitraq. Smart Radiation Dosimeter Technology*. [online]. Available: https://www.netobjex.com/casestudy/clinitraq/, Accessed: 23.4.2022.

[26] MARUŠIN, M. *Virtual Wallet Compatible with Cryptocurrency*. Bachelor's thesis, Brno, University of Technology, Faculty of Information Tech-nology, 2018.

[27] NAKAMOTO, S. *Bitcoin: A Peer-to-Peer Electronic Cash System*. [online]. Available: https://bitcoin.org/bitcoin.pdf, Accessed: 17.2.2022.

[28] TAR, A. *Proof-of-Work, Explained*. [online]. Available: https://cointelegraph.com/explained/proof-of-work-explained, Accessed: 19.2.2022.

[29] WU, MINGLI, E. A. A comprehensive survery of blockchain: From theory to iot applications and beyond. *IEEE Internet of Things Journal* (, 6.5: 8114-8154).

[30] YAFIMAVA, D. *9 Real-life Blockchain and IoT Use Cases*. [online]. Available: https://openledger.info/insights/blockchain-iot-use-cases/, Accessed: 12.4.2022.

# Seznam obrázků