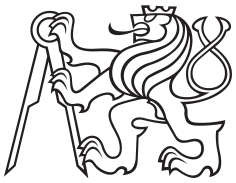
Diplomová práce



České
vysoké
učení technické
v Praze

F3

Fakulta elektrotechnická
Katedra radioelektroniky

Nové metody zabezpečení komunikace v IoT

Bc. David Juřík

Vedoucí práce: doc. Ing. Stanislav Vítek, Ph.D
Leden 2024

ZADÁNÍ DIPLOMOVÉ PRÁCE

I. OSOBNÍ A STUDIJNÍ ÚDAJE

Příjmení: **Juřík** Jméno: **David** Osobní číslo: **466013**

Fakulta/ústav: **Fakulta elektrotechnická**

Zadávající katedra/ústav: **Katedra radioelektroniky**

Studijní program: **Elektronika a komunikace**

Specializace: **Technologie internetu věcí**

II. ÚDAJE K DIPLOMOVÉ PRÁCI

Název diplomové práce:

Nové metody zabezpečení komunikace v IoT

Název diplomové práce anglicky:

New Methods to Secure IoT Communication

Pokyny pro vypracování:

1. Proveďte rešerši možností zabezpečení komunikace v IoT, včetně LPWAN sítí.
2. Na základě rešerše identifikujte IoT aplikaci vhodnou pro demonstraci principů zabezpečení a navrhněte infrastrukturu pro implementaci aplikace.
3. Navrženou infrastrukturu implementujte s využitím vhodného hardware, založeného např. na procesorech STM32.
4. Navrhněte a implementujte vhodný způsob testování infrastruktury. Diskutujte výsledky.

Seznam doporučené literatury:

[1] HASSAN, Wan Haslina, et al. Current research on Internet of Things (IoT) security: A survey. Computer networks, 2019, 148: 283-294.
[2] ALFANDI, Omar, et al. A survey on boosting IoT security and privacy through blockchain. Cluster Computing, 2021, 24.1: 37-55
[3] CHVYKOVA, Viktoria, Decentralized Authentication of IoT Devices Based on Blockchain Technology, Master thesis, CTU In Prague, 2022

Jméno a pracoviště vedoucí(ho) diplomové práce:

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

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

Datum zadání diplomové práce: **20.09.2023** Termín odevzdání diplomové práce: **09.01.2024**

Platnost zadání diplomové práce: **16.02.2025**

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

III. PŘEVZETÍ ZADÁNÍ

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

. | Podpis studenta

Datum převzetí zadání

Poděkování

Děkuji vedoucímu diplomové práce panu doc. Ing. Stanislavu Vítkovi, Ph.D za jeho pomoc a věcné připomínky při řešení problematiky spojené s diplomovou prací.

Prohlášení

Prohlašuji, že jsem předloženou práci vypracoval samostatně, a že jsem uvedl veškerou použitou literaturu.

V Praze, 1. ledna 2024

I declare that this work is all my own work and I have cited all sources I have used in the bibliography.

Prague, January 1, 2024

Abstrakt

Diplomová práce se zaměřuje na výzkum a vývoj nových metod pro zabezpečení komunikace v sítích IoT. Hlavní důraz je kladen na Distributed Ledger Technologies (DLT), které pro svůj ledger používají strukturu Directed Acyclic Graph (DAG). IOTA Tangle je poté vybrán jako nejslibnější technologie a je poskytnut detailní popis funkčních principů. Nakonec je vybrána komerčně dostupná vývojová deska s procesorem STM32U5, která demonstruje připojení zprávy do IOTA Tangle.

Klíčová slova: IoT, Internet věcí, ESP32, IOTA Tangle, blockchain, decentralizovaná síť, bezpečnost IoT, DLT, struktura s Orientovaným Acyklickým Grafem

Vedoucí práce: doc. Ing. Stanislav Vítek, Ph.D

Abstract

Diploma thesis concentrates on research and development of new methods to secure communication in IoT networks. Main focus is placed on Distributed Ledger Technologies (DLTs) which use Directed Acyclic Graph (DAG) structure for their ledger. IOTA Tangle is then selected as the most promising technology and an in-depth description of working principles is provided. At the end, commercially available development board with STM32U5 processor is chosen to demonstrate attaching a message to the IOTA Tangle.

Keywords: IoT, Internet of things,ESP32 ,IOTA Tangle, blockchain, decentralized network, security of IoT, DLT, Directed Acyclic Graph structure

Title translation: New Methods to Secure IoT Communication

Obsah

Obrázky

Kapitola 1
Úvod

IoT, neboli Internet of Things, je koncept, který pochází již z 90. let minulého století. V této době označení IoT nexistovalo a jako první jej použil Kevin Ashton (spoluzakladatel Auto-ID Centra na MIT) ve své řeči v roce 1999, když popisoval systém mnoha zařízení a senzorů připojených do Internetu [9]. V této době však nebyly vyvinuty efektivní komunikační protokoly ani dostatečně výkonné čipy aby se mohla myšlenka IoT dále rozvíjet.

Velká změna v této oblasti přišla s příchodem vyspělých technologií, díky kterým bylo možné levně pořídit výkonné a nízkoenergetické čipy, které v sobě integrovaly rádivou část (RF). To otevřelo dveře k velkým možnostem v oblasti automatizace, sběru dat a vzdáleného řízení. S tímto rozvojem přicházejí i výzvy ohledně zabezpečení komunikace v IoT. Zabezpečení se stalo stěžejním tématem, protože stále více zařízení a systémů je propojeno do tohoto rozsáhlého ekosystému, a tím se zvyšuje zranitelnost vůči různým hrozbám a kybernetickým útokům. Toto téma je aktuálně nejen relevantní, ale i nezbytné pro zajištění úspěchu a udržitelnosti IoT a jeho širokého uplatnění v průmyslu, energetice, zdravotnictví a mnoha dalších oblastech. Nové metody zabezpečení komunikace v IoT jsou klíčem k ochraně osobních údajů, kritické infrastruktury a vytvoření důvěryhodného prostředí pro budoucí digitální inovace.

Tato diplomová práce se zaměří na nové metody zabezpečení komunikace v IoT a na přínos inovací do této oblasti. Bude zkoumat, jak lze chránit přenos dat mezi různými IoT zařízeními a jak nové technologie a postupy mohou přispět k zajištění integrity, dostupnosti a důvěrnosti komunikace v tomto prostředí. V druhé části práce bude vytvořen IoT systém na základě provedeného průzkumu s využitím komerčně dostupného hardware.

Kapitola 2

Zabezpečení komunikace v IoT včetně LPWAN sítí

2.1 Co je IoT

Internet of Things (IoT) popisuje propojení mnoha fyzických zařízení do sítě (ne nutně do internetu), což umožňuje těmto zařízením mezi sebou komunikovat [10]. Sběr a výměna dat je prováděna jak pomocí bezdrátových technologií tak pomocí kabelových sběrnic.
Klíčové prvky Internetu věcí zahrnují:

- Fyzická zařízení
  - IoT může zahrnovat různá fyzická zařízení, jako jsou senzory, čidla, průmyslové stroje, automobily, domácí spotřebiče a další objekty, které jsou vybaveny schopností komunikace a sběru dat.
- Internetové připojení
  - Zařízení v IoT jsou nejčastěji propojena s internetem prostřednictvím různých komunikačních technologií, jako jsou Wi-Fi, mobilní sítě, Bluetooth, LoRaWAN, Sigfox a další.
- Sběr a výměna dat
  - Zařízení IoT shromažďují různé typy dat (teplota, vlhkosti, poloha, atd.). Tato data jsou poté odesílána k dalšímu zpracování.
- Analýza dat
  - Data z IoT zařízení jsou analyzována a mohou sloužit ke spuštění akcí, jako je automatická regulace teploty, detekce problémů, bezpečnostní alarmy a další.

IoT představuje zajímavý koncept v oblasti informačních technologií a má široké uplatnění v reálném světě. Vzhledem k tomu, že stále více zařízení a objektů je propojeno s internetem, předpokládá se rostoucí trend i v dalších letech.

2.2 Co je LPWAN

LPWAN je zkratka pro "Low Power Wide Area Network", což představuje síť s širokým dosahem a nízkou spotřebou energie. Jedná se o bezdrátovou komunikační technologii, která byla navržena tak, aby umožnila komunikaci s nízkou energetickou náročností a širokým dosahem [11]. Tyto sítě většinou obsahují větší množství senzorů a koncových zařízení, proto je tento pojem často spojován s IoT.
LPWAN sítě lze charakterizovat následovně:

- Nízká spotřeba energie
  - LPWAN technologie jsou navrženy tak, aby minimalizovaly spotřebu energie, což umožňuje jejich dlouhou výdrž na baterky.
- Dlouhý dosah
  - LPWAN technologie mají schopnost pokrýt velké geografické oblasti, což je vhodné pro připojení zařízení na velké vzdálenosti.
- Sběr a výměna dat
  - Zařízení IoT shromažďují různé typy dat (teplota, vlhkosti, poloha, atd.). Tato data jsou poté odesílána k dalšímu zpracování.
- Nízká rychlost datového přenosu a velikost přenášených dat
  - LPWAN sítě mají obvykle nízkou rychlost datového přenosu a zpravidla přenášení ne více jak 30 bajtů. To je obvykle dostatečné pro mnoho IoT aplikací.

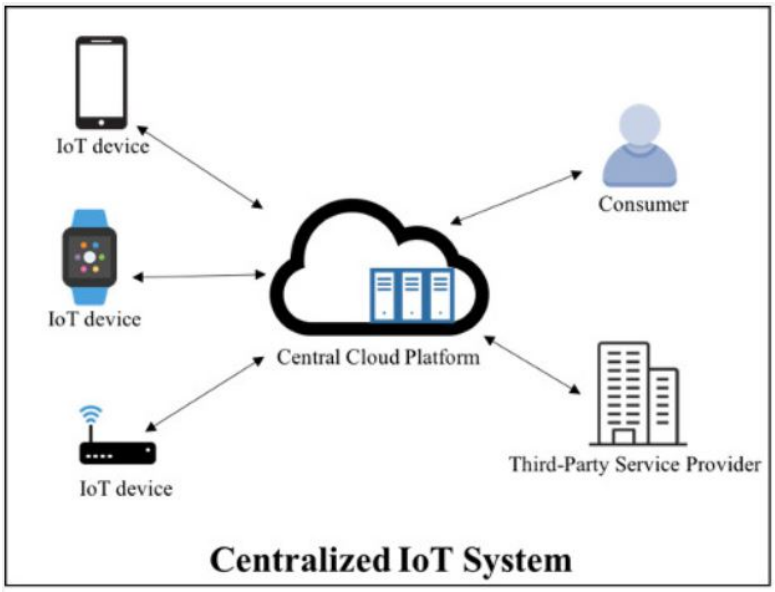
Existují různé LPWAN technologie a standardy, jako je LoRaWAN (Long Range Wide Area Network), Sigfox, NB-IoT (Narrowband IoT) a další. Každý z těchto standardů má své vlastní charakteristiky a výhody, a je možné mezi nimi vybírat na základě potřeb a požadavků pro konkrétní IoT nasazení.

2.3 Centralizované zabezpečení IoT systému

U centralizovaného zabezpečení informačních systémů a dat je kontrola a správa zabezpečení prováděna z centrálního systému. Tento centrální bod je obvykle zodpovědný za monitorování, řízení přístupu, detekci hrozeb a další bezpečnostní funkce pro celou síť. Hlavní výhodou centrálního zabezpečnostní je možnost jednotné správy a kontroly všech zabezpečnostních prvků v organizaci. To zahrnuje správu uživatelských oprávnění, aktualizace software, monitorování hrozeb a další aspekty zabezpečení. Nevýhodou centralizovaného zabezpečení může být nutnost investovat do centrálního hardware a software. Dále s sebou nese riziko selhání centrálního systému (single point of failure), které může ohrozit celou síť. V neposlední řadě uživatel musí

důvěřovat centrále, že nedojde k odcizení nebo manipulaci s uživatelskými daty.

Další text se již bude věnovat pouze decentralizovanému přístupu při návrhu sítí, které by svojí architekturou mělo vyřešit výše zmíněné problémy centralizovaného IoT. Tato práce se zabývá především novými možnostmi zabezpečení IoT sítí, které vznikají právě v decentralizované topologii sítě.



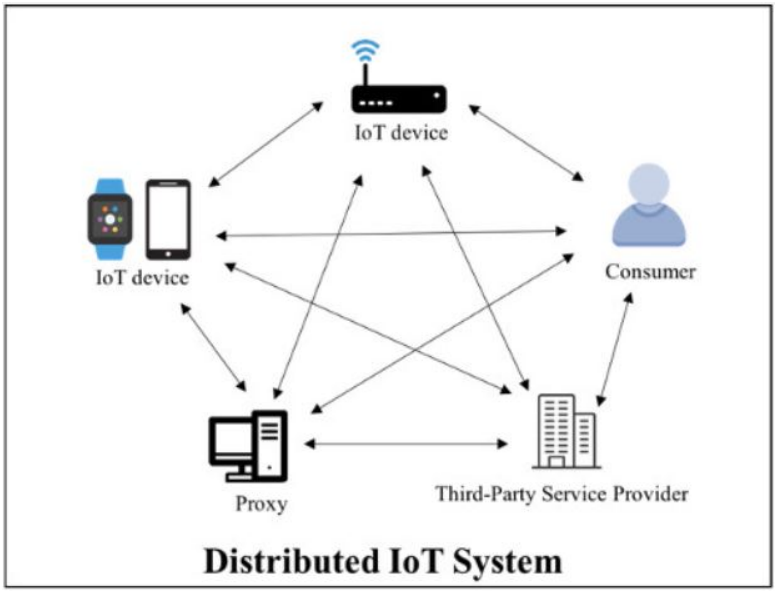
Obrázek 2.1: Centralizovaný IOT systém [8].

2.4 Decentralizované zabezpečení IoT systému

Decentralizované IoT je přístup k architektuře, který klade důraz na rozložení dat a kontroly v IoT systémech mimo centrální body nebo servery. V této topologii jsou funkce zpracování dat a řízení rozptýleny na okraji sítě a blízko samotných zařízení IoT narozdíl od centralizovaného systému, kde jsou data shromažďována a zpracovávána na centrálním serveru.
Hlavní rysy decentralizovaného IoT zahrnují:

- Lokální zpracování dat
  - Data jsou zpracovávána na okraji sítě nebo přímo na zařízeních IoT, což umožňuje rychlejší a efektivnější zpracování.
- Snížená latence
  - Díky možnosti zpracovávání dat lokálně se latence (zpoždění) při komunikaci a rozhodování snižuje, což je důležité pro reálný čas a rychlou reakci na události.

- Snížení zátěže sítě
  - Díky distribuovanému zpracování dat může dojít k menšímu množství dat, která musí být přenášena přes síť, což šetří šířku pásma.
- Větší bezpečnost dat
  - Data jsou distribuována po celé síti, nejčastěji pomocí DLT (distributed ledger technology), což zvýší bezpečnost dat a sníží riziko kompromitace centrálního úložiště.
- Odolnost proti výpadkům centrály (single point of failure)
  - Decentralizované IoT nemá žádné centrální úložiště, při výpadku jednoho nebo více zařízení není nijak ovlivněna funkčnost sítě.



Obrázek 2.2: Distribuovaný(decentralizovaný) IOT systém [8].

Decentralizované IoT může být vhodné pro aplikace, které vyžadují rychlé a efektivní zpracování dat a to zejména tam, kde je nutné minimalizovat latenci a maximalizovat odolnost systému. Tento přístup je účelný pro průmyslovou automatizaci, chytrá města, autonomní vozidla a další aplikace, kde je důležité mít distribuovaný a odolný systém IoT.

2.5 DLT (distributed ledger technology)

Distributed Ledger Technology (DLT) je technologie, která umožňuje decentralizované a distribuované ukládání a výměnu dat přes síť uzlů. Základní myšlenkou DLT je vytvořit odolný a transparentní záznam transakcí nebo dat, který je sdílen a ověřován několika účastníky v síti. Každý uzel má kopii celého (nebo části) ledgeru a změny v podobě nových transakcí nebo dat jsou dohodnuty prostřednictvím konsensu [13].

Konsensus je klíčový mechanizmus, který zajišťuje dohodu mezi jednotlivými uzly o tom, jaké zprávy a transakce jsou platné. V decentralizované síti nahrazuje centrální autoritu, kterou využívají centralizované systémy.

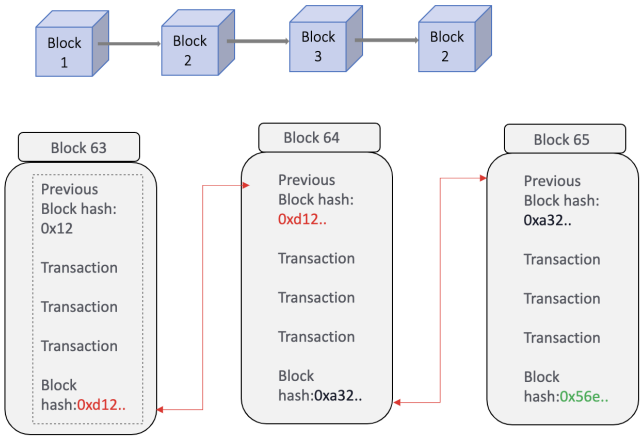
Nejznámějším typem DLT je blockchain, v posledních letech však došlo k rozvoji jiné formy distribuovaného ledgeru, jako jsou například grafy s orientovanou acyklickou strukturou (DAG).

2.5.1 Blockchain

Blockchain je specifický typ DLT. Jedná se o decentralizovaný systém, který slouží k záznamu a ověřování transakcí nebo dat bez potřeby centrální autority. Základním konceptem blockchainu je vytvoření řetězce bloků, kde každý blok obsahuje seznam transakcí a odkaz na předchozí blok.
Zde jsou klíčové prvky blockchainu:

- Bloky
  - Transakce jsou seskupeny do bloků, které jsou následně propojeny. Každý blok obsahuje unikátní identifikátor (hash) a odkaz na předchozí blok.
- Decentralizace
  - Blockchain funguje na základě decentralizované sítě uzlů - není ovládán jedinou entitou. Každé zařízení v síti má kopii celého blockchainu.
- Konsensus
  - Pro ověření a zápis nových bloků do blockchainu je potřeba dosáhnout konsensu mezi uzly sítě. Různé blockchainové sítě používají různé algoritmy konsensu, jako Proof of Work, Proof of Stake nebo jiné.
- Neměnnost
  - Jakmile je blok přidán do blockchainu, je nemožné změnit obsah tohoto bloku. To zajišťuje, že transakce uložené na blockchainu jsou neměnné.

- Transparentnost
  - Většina blockchainů je transparentní, což znamená, že každý uzel v síti může vidět historii transakcí.
- Kryptografie
  - K zajištění bezpečnosti a autentičnosti transakcí se používá kryptografie (elliptic curve cryptography, SHA256, veřejné a privátní klíče atd.).



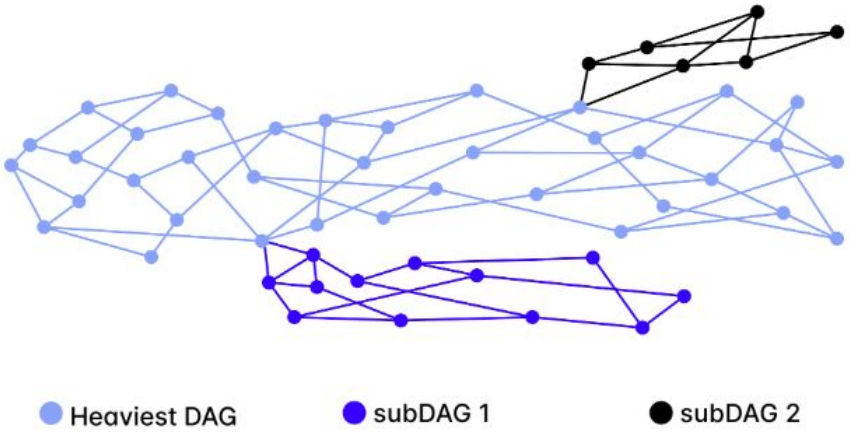
Obrázek 2.3: Struktura blockchain ledgeru [13].

Blockchain má mnoho aplikací, přičemž nejznámější je v oblasti kryptoměn (Bitcoin, Ethereum atd.). Nicméně, může být používán i v jiných odvětvích, jako jsou dodavatelské řetězce, zdravotnictví, a mnoho dalších, kde záznam a bezpečné ověřování transakcí jsou klíčové. Z pohledu architektury je blockchain nevyhovující pro použití v IoT sítích. Jedním z hlavních důvodů je, že s rostoucím počtem zařízení v síti roste i doba pro potvzení jednotlivých transakcí a dat. Dále kvůli použití silné kryptografie je zapotřebí, aby koncová zařízení měla dostatečně kvalitní hardware, což navyšuje náklady celého IoT systému. V neposlední řadě jde také o poplatky spojené s ověřením transakcí.

2.5.2 DAG (Directed Acyclyc Graph)

Distributed Ledger Technology (DLT) se strukturou Directed Acyclic Graph (DAG) je typ decentralizované technologie ledgeru, který používá orientovaný acyklický graf jako základní architekturu pro ukládání a ověřování dat a transakcí. Namísto tradičního blockchainu, kde bloky jsou lineárně propojeny, jsou bloky v DAG vzájemně propojené v acyklickém uspořádání [14].
Vlastnosti DAG:

- Neměnnost a bezpečnost
  - Stejně jako u běžných blockchainů, i DLT s DAG nabízí neměnnost dat. Jakmile jsou data zaznamenána na uzlu, je obtížné je změnit. K tomu přispívá také použití kryptografie pro ověření a zabezpečení transakcí.
- Transparentnost:
  - Každý uzel v síti má přístup k celé historii transakcí, což zajišťuje transparentnost. Uživatelé mohou sledovat původ a průběh transakcí a dat.
- Rozšiřitelnost (Scalability)
  - Struktura DAG je snadno rozšiřitelná o další koncová zařízení a s rostoucím počtem uzlů může narůstat rychlost s jakou jsou zprávy do ledgeru přidávány. U klasických blockchainů je rychlost konstatní bez ohledu na počet uživatelů.
- Nízké nebo žádné poplatky
  - Některé implementace DLT s DAG, nabízejí možnost provádět transakce bez poplatků nebo s velmi nízkými poplatky. To může být výhodné v situacích, kde jsou nízké transakční náklady klíčové.
- Odpadnutí potřeby těžařů
  - Oproti některým blockchainům, které vyžadují těžaře pro potvrzení transakcí, některé implementace DLT s DAG umožňují každému uzlu přispívat k ověřování transakcí.



Obrázek 2.4: Struktura DAG ledgeru.

Příkladem DLT s DAG strukturou je například IOTA, která využívá Tangle jako svůj decentralizovaný ledger. Tangle je specifický typ DAG, který umožňuje uzlům potvrzovat transakce, aniž by bylo nutné vytvářet bloky a spoléhat se na těžaře.

2.6 Konsensus

Jak již bylo zmíněno, konsensus zajišťuje dohodu mezi uzly distribuovaného systému, je tedy stěžejním mechanizmem celého DLT. Dohodou v tomto kontextu je myšleno, jaké transakce či zprávy jsou platné (platnost nemůže ověřit centrální autorita, která v distribuovaných systémech není). Jako každý elektronický systém i sítě DLT se mohou stát cílem hackerů. Především z pohledu kryptoměn ale i IoT je důležité, aby útočník nemohl pozměnit transakci nebo zprávu IoT. Konsensus zajišťuje bezpečnost, neměnnost a důveryhodnost celého DLT.

2.6.1 Konsensus v blockchainových technoligiích

V klasických blockchainových DLT (Bitcoin, Ethereum) je konsensu dosaženo pomocí řešení matematické úlohy. Má-li být přidán nový blok, obsahující stovky až tisíce transakcí, do blockchainu, je nutné aby jeden z těžařů (miners) vyřešil kryptografickou úlohu a úhádnul takzvané nonce (number once). Princip tohoto mechanizmu spočívá v tom, že tato úloha je obtížně řešitelná a nejlepším postupem jak uhádnout nonce je postupným generováním čísel a hashováním celeho bloku dat. Těžař který nonce úhádne připojí daný blok do blockchainu a získá odměnu v podobě kryptoměny. Bezpečnost spočívá v matematické náročnosti úlohy - aby byl vydán blok s upravenými transakcemi nebo zprávami, musel by útočník vlastnit více než 50% výpočetního výkonu všech těžařů na síti, což je velice nepravděpodobné.

2.6.2 Konsensus v technologiích s DAG

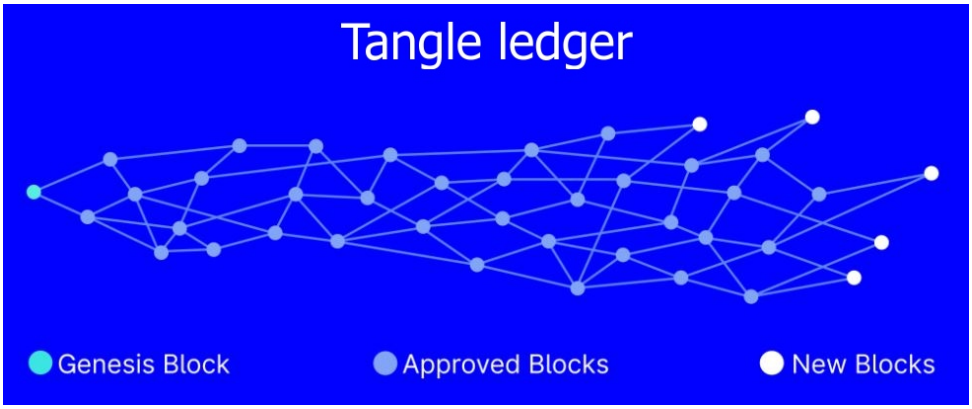
Z důvodu, že se jedná o poměrně novou technologii, konsesus ve strukturách DAG není nijak standardizovaný. Hlavní myšlenkou je uplné nebo částečné odstranění těžařů a minimalizace poplatků spojených s využitím sítě. Konsensu je většinou dosaženo pomocí kumulativní váhy transakcí. Dále je využito struktury DAG a není nutné aby byly transakce uzavřeny do bloků – každá zpráva je provázána se zprávami předchozími. Propustrnost takovéhoto systému může být vice než 1000 TPS (transaction per second) na rozdíl od blockainových technologií, kde je počet potvrzených transakcí za sekundu nízký (Bitcoin 7 TPS, Ethereum 27 TPS).

Kapitola 3
IOTA

IOTA je open-source decentralizovaný ledger a stejnojmenná kryptoměna. Využívá strukturu DAG pro svůj ledger zvaný Tangle k ukládání transakcí a datových zpráv. Hlavní výhodou IOTA je, že ke svému fungování nevyužívá těžaře (miners) k ověřování transakcí. Díky tomuto konceptu je možné provádět platby a ukládat data bez poplatků, což umožňuje takzvané mikroplatby. Z pohledu návrhu a nulových poplatků je také vhodným kandidátem pro decentralizované IoT.

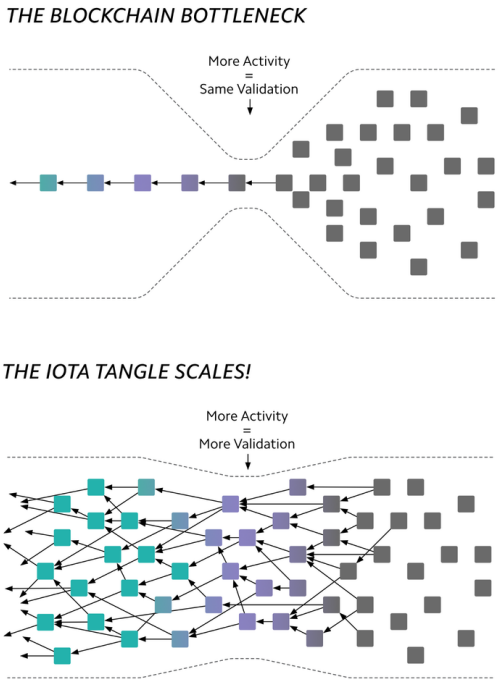
3.1 Tangle ledger

IOTA Tangle je distribuovaný ledger, který obsahuje údaje o všech transakcích a datových zprávách. V okamžiku, kdy je zpráva přidána do ledgeru, je velice obtížné až nemožné původní obsah pozměnit protože obsah zprávy je provázán se zprávami předchozími skrz hash. Tangle využívá struktury orientovaného acyklického grafu jak je znázorněno na následujícím obrázku.



Obrázek 3.1: Struktura Tangle ledgeru [22].

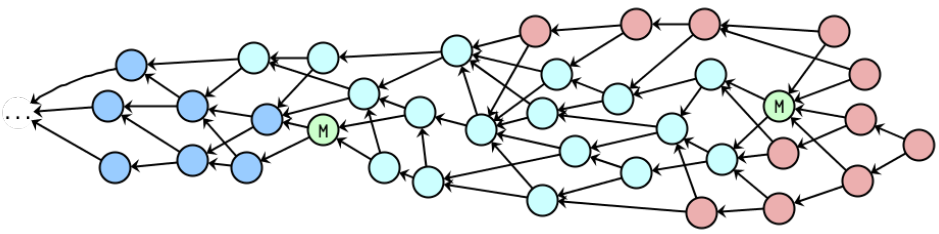
Největší výhodou této struktury je, že s rostoucím počtem zpráv, které jsou do Tangelu přidávány roste i rychlost s jakou jsou potvrzeny. To je hlavní výhoda oproti klasickému decentralizovému blockchainu, kde je rychlost potvrzování konstantní.



Obrázek 3.2: Srovnání propustrnosti - blockchain ledger oproti DAG ledger [15].

V souvislosti s Tangle hovoříme o třech typech zpráv z pohledu stavu, ve kterém se nacházejí:

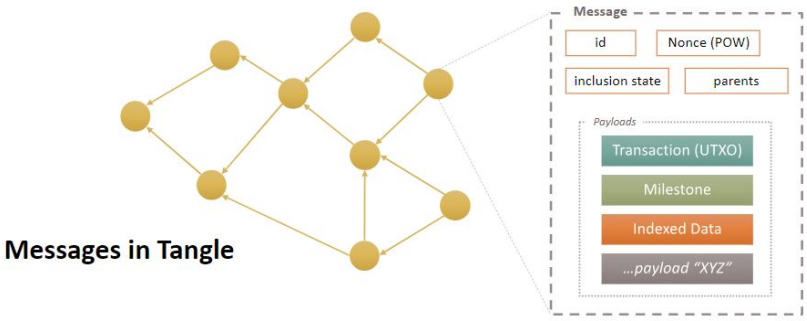
- Confirmed
  - Potvzené transakce\zprávy na obrázku znázorněny modrou barvou.
- Unconfirmed
  - Nepotvrzené transakce\zprávy na obrázku znázorněny tyrkysovou barvou.
- Tip
  - Nově přidané transakce\zprávy na obrázku znázorněny červenou barvou.



Obrázek 3.3: Stavy zpráv v Tangle.

3.2 IOTA zpráva

Pokud chce uživatel vytvořit novou transakci nebo zprávu, musí vybrat 2-8 předchozích nepotvrzených transakcí\zpráv a jejich hash přímo referencovat (direct reference) ve své zprávě, vykonat malý proof-of-work a tím vyřešit kryptografickou úlohu (podstatně jednodušší než např. u Bitcoinu). Tím však není zpráva potvrzena, tento postup pouze brání spamování sítě a odstraňuje nutnost těžařů (miners). Výběr náhodných zpráv pro referenci zajišťuje Tip Selection Algorithm. V průběhu času, kdy jsou do Tangle přidávány další zprávy\transakce, dochází k nepřímé referenci (indirect reference) původních zpráv.



Obrázek 3.4: Vrcholy grafu jsou jednotlivé transakce\zprávy, hrany představují reference mezi jednotlivými zprávami

Struktura IOTA zprávy

Každá zpráva, kterou chce uživatel připojit do Tangle musí splňovat určité náležitosti, v opačném případě je sítí odmítnuta. V okamžiku, kdy je zpráva ověřena, že splňuje strukturu daného protokolu (Chrysalis\Stardust) je pomocí gossip algoritmu přeposlána do všech koncových zařízení, aby byl Tangle ledger konzistentní.

- ID zprávy
  - Unikátní číslo, které je vygenerováno z bajtů zprávy prostřednictvím hashovacího algoritmu. Pomocí tohoto unikátního identifikátoru lze zprávu dohledat v Tangle.
- ID sítě
  - Jedna z veřejných IOTA sítí (Mainnet, Shimmer, Testnet, Devnet) popřípadě privátní síť.

- ID referencovaných zpráv
  - Každá zpráva musí referencovat 2-8 předchozích zpráv. Tím dojde k vytvoření klasické struktury DAG, kterou IOTA využívá. Zprávy jsou náhodně vybrány pomocí tip selection algoritmu.
- Délka zprávy
  - Maximální délka zprávy nesmí přesáhnout 32Kbi. V případě, že uživatel potřebuje odeslat zprávu delší, může využít prokolu L2Sec. Funkce a využití tohoto protokolu bude dále uvedena v textu.
- Druh zprávy (Devnet - Chrysalis)
  - Transaction payload
    - Definuje transakci mezi uživateli. Transakce musí obsahovat digitální podpis pomocí privátního klíče, který vlastní uživatel digitální peněženky.
  - Milestone payload
    - Bezpečnostní zpráva. Musí obsahovat digitální podpis koordinátora.
  - Indexation payload
    - Jedná se o libovolný textový řetězec, což je z pohledu IOT nejzajímavější druh zprávy. Dají se tak přenášet řídící zprávy, data ze senzorů atd. Hlavní výhodou takto přenesených dat je jejich neměnnost v Tangelu.
  - Nonce (number once)
    - Nonce je výsledkem proof-of-work (PoW) a zabraňuje spamování sítě. Každý klient, který chce umístit zprávu do tangelu, musí vyřešit jednoduchou kryptografickou úlohu a výsledek (nonce) uvést do zprávy.
    - IOTA představuje zajímavý koncept, při kterém nízkoenergetická zařízení nemusí odvádět PoW lokálně, ale jiné zařízení vykoná PoW místo samotného klienta. Z pohledu IoT je to dobře promyšlená funkce, která dovoluje bateriově poháněným zařízením odesílat zprávy do Tangle aniž by musely plýtvat energii na PoW.

3.3 IOTA konsensus

Potvrzovací proces je založený na kumulativní váze, která je spojená s proof-of-work. Čím více jsou transakce nepřímo referencovány, tím více je transakce považována za potvrzenou a bezpečnou. Dále jsou do Tangle přidávány speciální zprávy – Milestony. Ty mají vysokou váhu bezpečnosti a jsou periodicky připojovány pomocí koordinátora (coordinator). Jakákoliv transakce, která přímo či nepřímo referencuje Milestone je považována za potvrzenou. Koordinátor je speciální komponent, který pomáhá chránit síť před případnými útoky. Jedná se o jediný centralizovaný prvek v decentralizované IOTA síti, který bude odstraněn ve verzi protokolu 2.0 pomocí konsensu OTV (On Tangle Voting). Po této aktualizaci bude IOTA kompletně decentralizovaná.

3.4 IOTA sítě

IOTA má aktuálně 4 hlavní sítě, ke kterým se lze připojit pomocí klienta. Ten může v současnosti využívat jeden ze 2 podporovaných protokolů – Chrysalis a Stardust. Doporučeným klientem pro přímý přístup do IOTA sítě je software Hornet.

- Mainnet
  - Hlavní síť, která aktuálně běží na protokolu Stardust. Na této síti má IOTA peněžní hodnotu a je možné posílat IOTA tokeny mezi uživateli. Dále lze obchodovat na platformách jako jsou kryptoměnové burzy nebo kryptoměnové směnárny.
- Shimmer
  - Síť běžící na protokolu Stardust. Jejím hlavním cílem je prostor pro testování nových funkcí a aktualizací před tím, než jsou využity v Mainnetu.
- Testnet
  - Síť běžící na protokolu Stardust. Je využita k testování a interakci s chytrými kontrakty (smart contracts).
- Devnet
  - Síť běžící na protokolu Chrysalis. Využívá se k testování transakcí a zpráv pro IoT zařízení.

3.5 Zabezpečení komunikace v Tangle

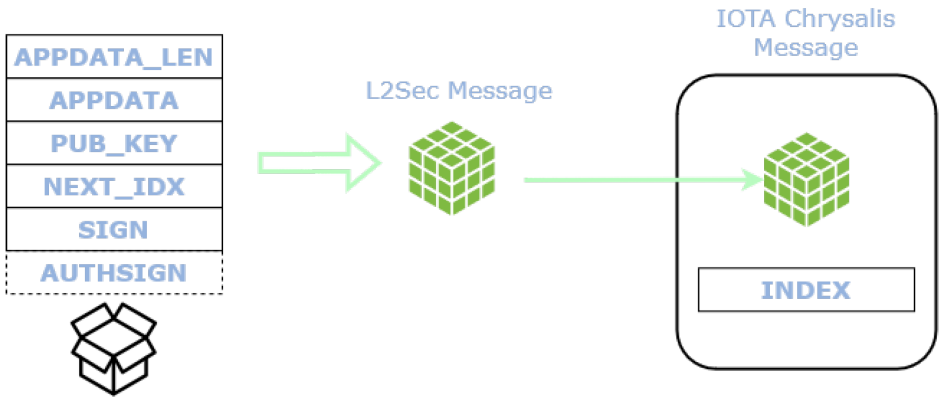
Indexation zprávy, které jsou z pohledu IoT stěžejní nejsou v defaultní verzi Tangle nijak kryptograficky chráněné – se znalostí message ID může kdokoliv zprávu dohledat a do jejího obsahu nahlédnout. Tento problém řeší vrstva L2, která se stará o šifrování dat zpráv v Tangle. V současné době existují 2 protokoly, kterými mohou uživatelé svá data zašifrovat – Streams a L2Sec.

3.5.1 Streams protokol

Streams protokol dovoluje strukturovat, šifrovat a připojit datovou zprávu do Tangle ledger, který garantuje integritu a neměnnost uložených dat. Uživatel (publisher), který zprávu vytvořil, může přidělit nebo zakázat přístup ostatním uživatelům (subscribers). Streams představuje kompletní řešení pro zabezpečenou komunikaci. Aktuální verze je implementována v jazyce Rust a pro správnou funkci vyžaduje mikrokontrolér s operačním systémem. Z pohledu IoT je to nevyhovující protokol, protože nároky na chod takového systému jsou z hlediska výkonnosti hardware a odběru elektrické energie příliš vysoké.

3.5.2 L2Sec protokol

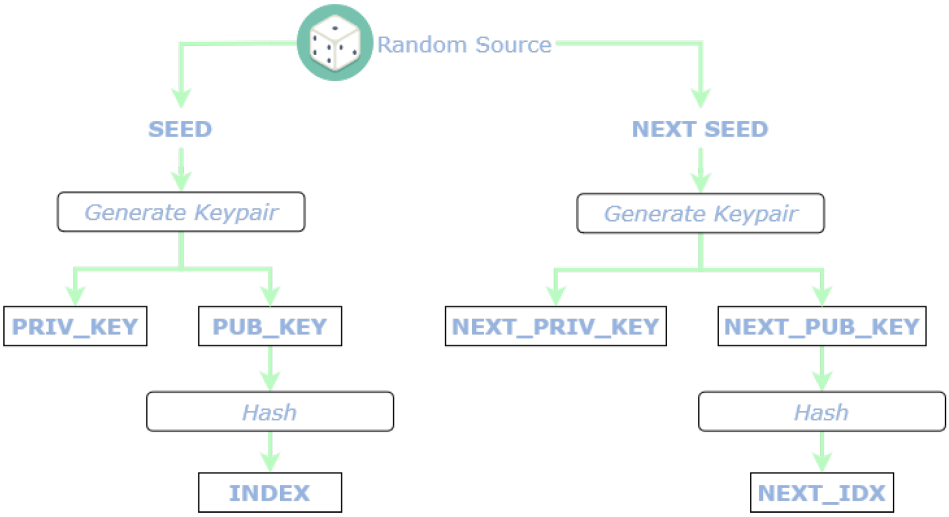
Problém protokolu Streams a jeho využití ve sféře IoT elegantně řeší protokol L2Sec. Jedná se o lehký (možnost provádě kryptografické operace na levném hardware) open-source kryptografický protokol implementovaný v jazyce C navržený pro nízkoenergetické systémy. S výhodou jej lze uplatnit v síti Devnet (Chrysalis) k šifrování uživatelských dat, jak jeznázorněno na následujícím obrázku.



Obrázek 3.5: Zapouzdření zprávy pomocí L2sec protokolu [16].

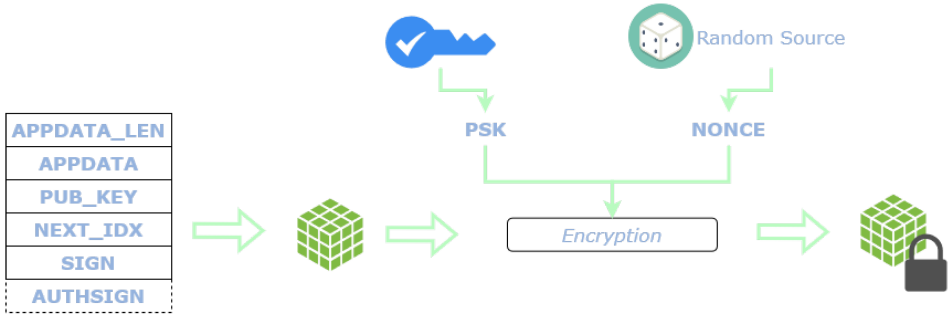
Data jsou zapouzdřena do L2Sec message a v případě, že je payload delší, než je maximální povolená délka zprávy, je zpráva rozdělena do 2 a více částí, které jsou zřetězeny pomocí položky NEXT_IDX, což je ID další zprávy v

pořadí, kterou je možné dohledat v Tangle ledgeru. L2Sec protokol vygeneruje privátní a veřejný klíč z náhodného čísla (random seed). Tento pár klíčů, který slouží pouze pro zřetězení zpráv, je vygenerován na základě eliptické křivky Edwards25519. Z veřejného klíče je následně odvozen NEXT_IDX. Celý proces je znázorněn na následujícím obrázku.



Obrázek 3.6: Způsob generování páru klíčů pro odvození ID zprávy [16].

Zpráva je následně zašifrována pomocí symetrického předem sdíleného klíče (PSK) s využitím inicializačního vektoru (nonce). Celý proces šifrování probíhá za pomoci XSalsa20 šifry. Poté jsou zprávy umístěny v do Tangle ledgeru. Dále je nutné podotknout, že ze zprávy nikdy nelze odvodit ID zprávy předchozí. Celkový payload může být tedy koncovým zařízením zrekonstruována pouze ze znalosti první zprávy.



Obrázek 3.7: Proces šifrování zprávy [16].

3.6 Odolnost IOTA sítě proti kvantovým počítačům

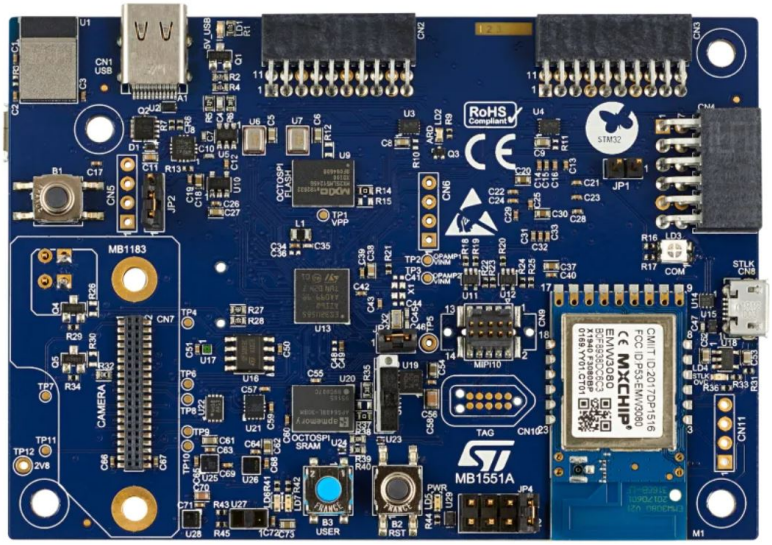
IOTA Tangle v současné době používá algoritmy kryptografie, které by měly být odolné vůči kvantovým počítačům. Jedná se zejména o kvantově odolné podpisy. Většina kryptografických funkcí, které jsou odolné vůči kvantovým útokům, je založena na matematických problémech, které by kvantové počítače měly velmi obtížné řešit.

V případě IOTA Tangle jsou používány podpisy Winternitz One-Time Signature Scheme (W-OTS), které jsou známé svou kvantovou odolností v rámci Groverova algoritmu. Groverův algoritmus by mohl efektivněji prolomit některé běžné kryptografické funkce, ale podpisy W-OTS jsou navrženy tak, aby byly odolné i vůči tomuto typu kvantových útoků.

Kapitola 4

Implementace infrastruktury pomocí B-U585I-IOT02A

V praktické části práce bude využita vývojová deska od společnosti STMicroelectronics. Ta je založena na procesorech z rodiny STM32U5, která využívá architekturu Arm Cortex-M33. Fyzické rozměry B-U585I-IOT02A jsou 10cm na délku a 7cm na šířku - na této ploše se nachází hlavní procesor, WiFi modul, BLE modul a další senzory a konektory. Hlavní výhodou zvoleného MCU je nízký odběr elektrické energie a dostupná cena, což jsou hlavní předpoklady pro využití desky jako koncové zařízení IOT.



Obrázek 4.1: Vývojová deska od společnosti STMicroelectronics.

4.1 Technické parametry desky B-U585I-IOT02A

- Nízkoenergetický STM32U585AII6Q mikrokontrolér založený na Arm® Cortex®-M33 jádře s Arm® TrustZone®, 2Mb Flash paměti a 786Kb SRAM.
- 512-Mbit Quad-SPI Flash paměť, 64-Mbit Octo-SPI PSRAM, 256-Kbit I2C EEPROM.
- 802.11 b/g/n Wi-Fi® modul značky MXCHIP.
- Bluetooth® Low Energy od STMicroelectronics.
- Authentikace a zabezpečení periferií a IoT zařízení od STMicroelectronics.
- 3D akcelerometer a 3D gyroscope.
- 3-axis magnetometer.
- MEMS sensory od STMicroelectronics.
- Senzor teploty a vlhkosti.
- STSAFE-A110 bezpečností hardwarový element.
- Podpora široké nabídky IDEs: Embedded Workbench®, MDK-ARM a STM32CubeIDE.

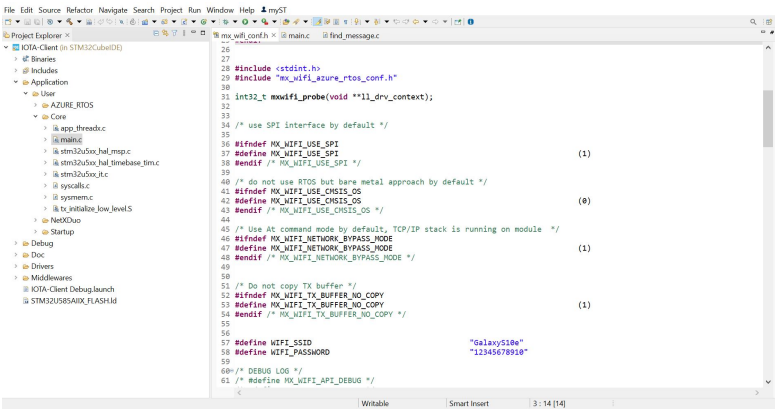
4.2 X-CUBE-IOTA1 software balíček

Dalším důležitým komponentem při vytváření IOT zařizení je předpřipravený software X-CUBE-IOTA1. Ten je speciálně vytvořený pro výše popisovanou vývojovou desku, ale s drobnými modifikacemi by mohl být použit i pro jiný STM32 procesor. X-CUBE-IOTA1 umožňuje odeslat uživatelská data v síti Devnet (Chrysalis) v indexation payloadu do IOTA Tangle. V následujícím textu bude do detailů vysvětlen způsob použití s praktickým příkladem.
Hlavní komponenty middlewaru:

- STSAFE-A110 bezpečnostní hardwarový prvek pro správu kryptografických funkcí.
- Wi-Fi management.
- Šifrování, hashování, authentikace zpráv, digitální podpisy (sodium/mbedCrypto).
- Azure RTOS ThreadX a NetXDuo.
- IOTA Client API pro interakci s Tangle.

4.3 Software pro kompilaci STM32CubeIDE

Pro kompilaci programu bude využit software STM32CubeIDE. Jediná modifikace zdrojových kódů bude provedena v souboru mx_wifi_conf.h, kde uživatel zadá SSID a heslo WiFi sítě, přes kterou bude koncové zařízení připojeno k Devnetu.



Obrázek 4.2: Software STM32CubeIDE pro kompilaci a nahrání programu.

Po úspěšné kompilaci programu je zapotřebí nahrát binární soubor s programem do desky B-U585I-IOT02A. Dále je nutné připojit se k zařízení pomocí USART protokolu, například prostřednictvím programu TeraTerm.

4.4 Funkce programu

V okamžiku připojení má uživatel na výběr z menu ze dvou základních funkcí. Odeslání zprávy do Tangle nebo odeslání zprývy do Tangelu pomocí L2Sec protokolu. Z teoretického rozboru, který proběhl v minulé kapitole je zřejmé, že první možnost připojí zprávu do Tangelu bez jakéhokoliv šifrování. Kdokoliv se znalostí ID bude schopen obsah zprávy získat. V druhém případě budou data zašifrována pomocí symetrického PSK.

Obrázek 4.3: Menu pro výběr fuknce k odeslání zprávy.

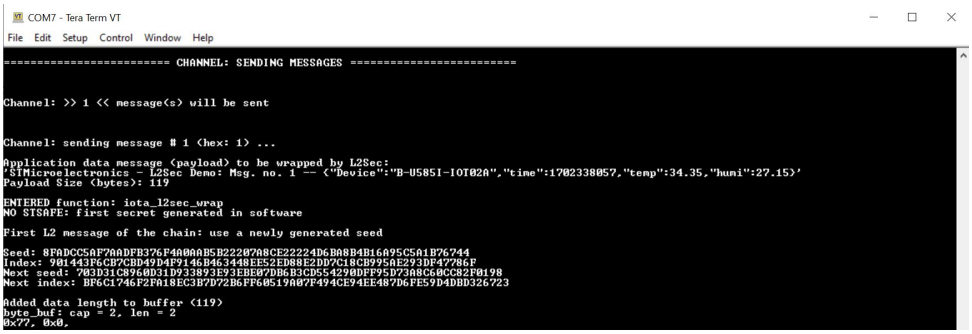
4.4.1 Odeslání nezabezpečené zprávy

Pomocí řídících příkazů je zpráva odeslána do sítě Devnet. Vygenerované ID bude uschováno pro následné ověření, že zpráva byla úspěšně přidána do Tangle. Jeho hodnota je zobrazena na obrázku níže.

Obrázek 4.4: Odeslání nezabezpečené zprávy do Tangle.

4.4.2 Odeslání zabezpečené zprávy

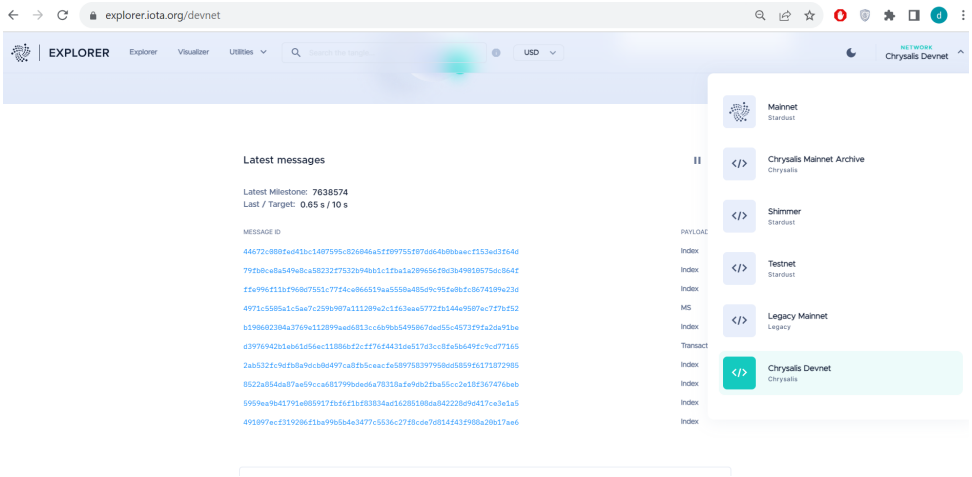
Zašifrovaná zpráva byla odeslána do sítě Devnet. V souboru l2sec_example.c lze dohledat PSK, kterým byl daný payload zašifrován. Vygenerované ID bude uschováno pro následné ověření, že zpráva byla úspěšně přidána do Tangle. K dešifrování bude využit stejný PSK, neboť se jedná o symetrickou šifru.



Obrázek 4.5: Odeslání zabezpečené zprávy do Tangle.

4.5 Kontrola zpráv v Tangle

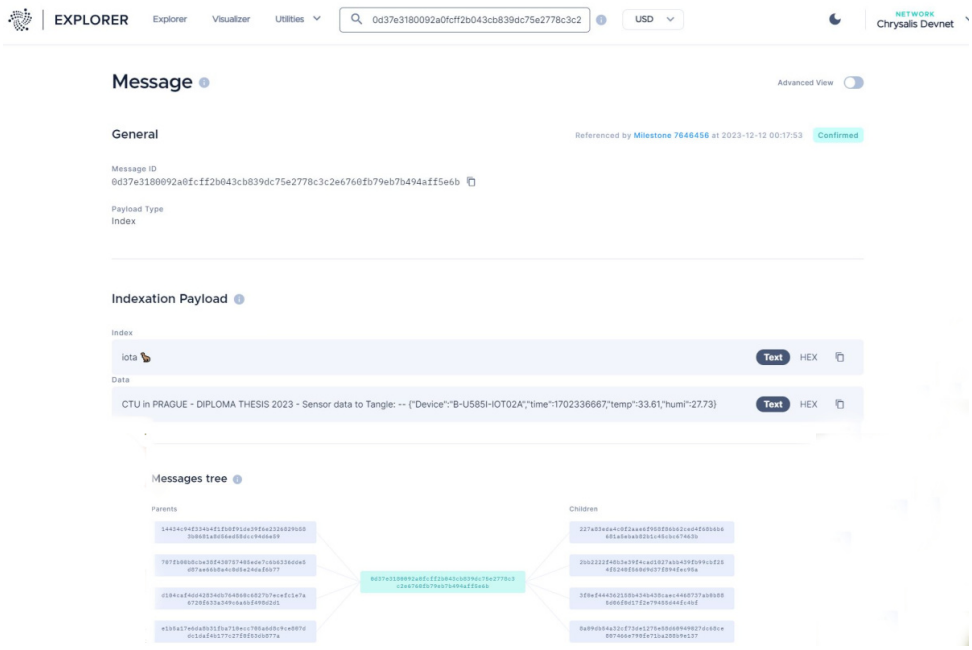
Na URL adrese `https://explorer.iota.org/` je možné dohledat zprávy Tangle v sítích IOTA. Pro testování byla zvolena síť Devnet. Dále můžeme pozorovat v prostřední části obrázku nově přidané zprávy (a jejich ID) do Tangle – nejvíce zpráv je typu indexation, avšak transaction a milestone jsou také přítomny. Pomocí vyhledávače jsme schopni dohledat zprávu pomocí



Obrázek 4.6: Odeslání zabezpečené zprávy do Tangle.

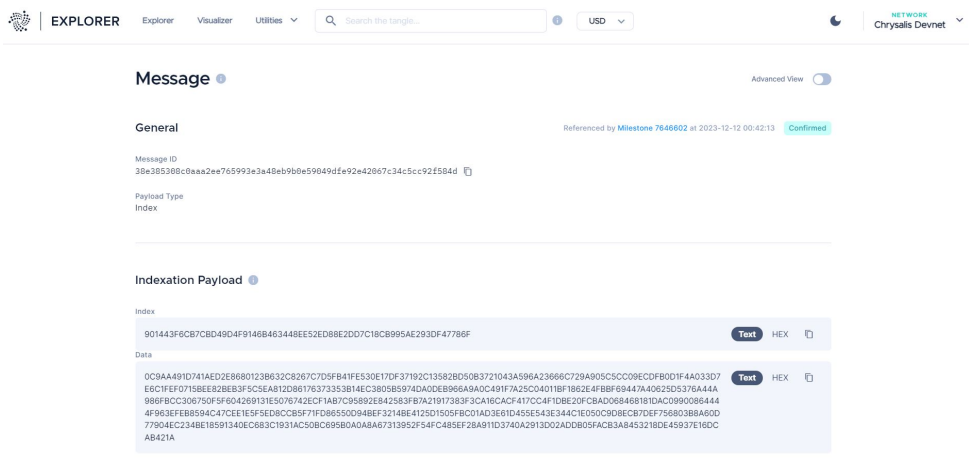
message ID. Jak již bylo zmíněno, 1. odeslaná zpráva není nijak zašifrovaná. Na obrázku níže můžeme pozorovat následující:

- Operujeme v síti Devnet (Chrysalis).
- Obsah zprávy (jedná se o textový řetězec doplněný o údaje ze senzorů a časový timestamp).
  - “CTU in PRAGUE - DIPLOMA THESIS 2023 - Sensor data to Tangle: – "Device":"B-U585I-IOT02A","time":1702336667,"temp":33.61,"humi":27.73”.
- Payload type:
  - Indexation.
- Zpráva je potvrzená a byla referencována Milestonem číslo 7646456.
- Message tree:
  - Odeslaná zpráva referencovala 4 jiné zprávy a je referencována 4 jinými zprávami.



Obrázek 4.7: Rozbor odeslané zprávy v IOTA exploreru.

I v druhém testování jsme schopni v Tangle zprávu snadno dohledat a její obsah zobrazit s tím rozdílem, že payload je zašifrovaný. Struktura zprávy je stejná jako v předchozím nezašifrovaném případě.



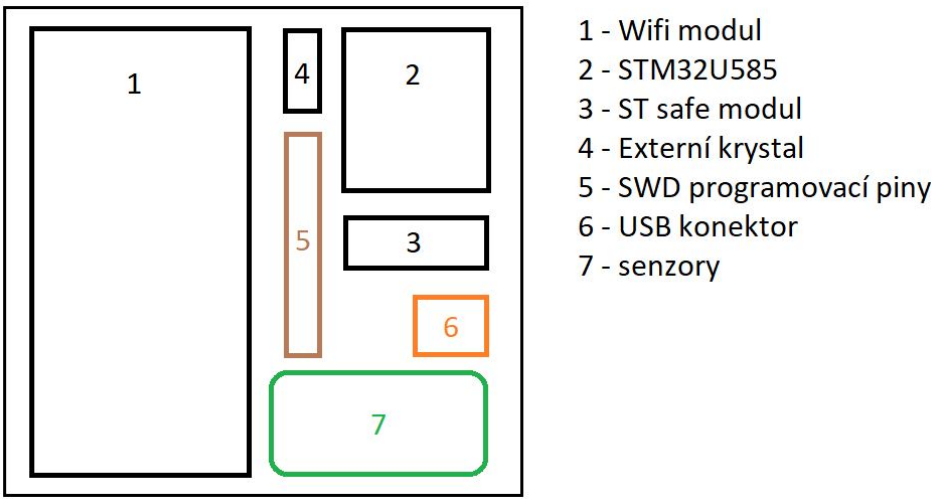
Obrázek 4.8: Rozbor odeslané zprávy v IOTA exploreru.

Kapitola 5

Implementace IoT zařízení

V předchozí kapitole byl představen ukázkový program, který uvedl funkce a možnosti, které vývojová deska B-U585I-IOT02A a software umožňují. Tato kapitola se zaměří na tvorbu software pro koncové zařízení, využitelné v běžných podmínkách v terénu v IoT sítích. Program nebude kontrolován z osobního počítače a bude implementován úsporný režim daného procesoru tak, aby koncové zařízení mohlo fungovat na bateriový akumulátor.

Dále je nutné zdůraznit, že vývojová deska nabízí další moduly a senzory, které ve výsledné aplikaci nebudou potřeba a zbytečně tak zvětšují fyzické rozměry koncového zařízení. Uvážíme-li pouze komponenty, které jsou aplikací využívány, jsme schopni rozměry zredukovat, jak je naznačeno na následujícím obrázku.



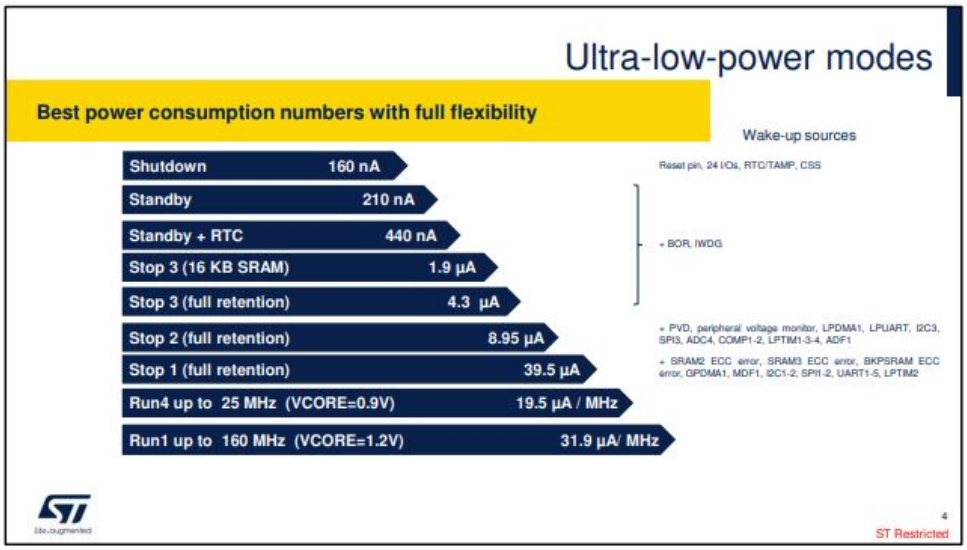
Obrázek 5.1: Blokové schéma komponentů využitých v koncovém zařízení.

Takto navržený modul by měl rozměry čtverce o hraně 3.5cm. Z druhé strany plošného spoje je dostatek místa pro knoflíkovou baterii pro napájení modulu.

5.1 Teoretický rozbor funkcionalit procesoru

5.1.1 Low-power módy

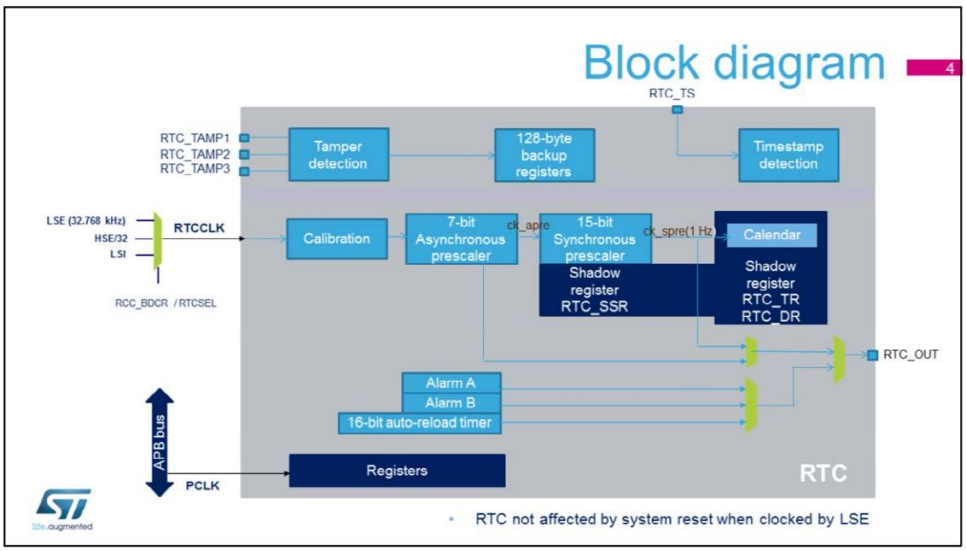
Procesory z rodiny STM32 nabízí několik energeticky úsporných módů, do kterých může být procesor uveden během neaktivity, která v běžných sítích IoT převyšuje před dobou, kdy je procesor aktivní – v našem případě při sběru a odeslání dat. Obecně lze snížit frekvenci procesoru, což vede ke značným energetickým úsporám. Dále je možné úplně zastavit jádro MCU a ponechat celý obsah paměti flash nebo jen část vybraných registrů. Každý mód lze nastavit pomocí vnitřních řídících registů. V okamžiku provedení instrukce zápisu přechází MCU do daného low-power módu přičemž se snižuje i spotřeba elektrické energie. Jedním ze způsobů jak low-power mód opustit je vnitřní nebo vnější interrupt v podobě náběžné hrany na pinu procesoru, přetečení časovače nebo další vnitřní události. V případě procesoru STM32U5 má uživatel na výběr z celkem 9 low-power módů.



Obrázek 5.2: 9 low-power módů procesoru STM32U5 [21].

5.1.2 RTC (Real Time Clock)

V sítích IoT je běžné, že se koncové zařízení periodicky probouzí, vyčte data ze senzorů, ta odešle a přejde zpět do pow-power módu. Díky hodinám reálného času (RTC) může být využito jednoho z čítáčů, který zajistí probuzení procesoru po uplynutí definované doby. Tato vnitřní periferie zajišťuje přesný čas a časovou základnu pro časovače (timers) procesoru - lze nastavit datum, čas a rok. Zdrojem pro časovou základnu může být vnitřní oscilátor, tvořený RC článkem nebo externí krystal s kmitočtem 32.768kHz, který bývá zpravidla přesnější, ale energeticky náročnější. Tato periférie je funkční ve všech low-power módech s možností vygenerování interruptu pro probuzení procesoru z režimu spánku. Ty mohou být spuštěny přetečením časovače nebo shodou časové timestamp.



Obrázek 5.3: Blokové schéma RTC periferie [23].

5.2 Deska X-NUCLEO-LPM01A

Dalším komponentem, který bude využit je vývojová deska od STMicroelectronics s označením X-NUCLEO-LPM01A pro přesné měření odebíraného proudu procesoru v rozmezí od 100nA do 50mA. Může pracovat v samostatném módu, kdy je odebíraný proud zobrazován na displeji nebo lze využít software STM32CubeMonitor-Power, který poskytuje grafické uživatelské prostředí a více funkcionalit.

Před použitím je nutné nahrát do desky nejnovější firmware z důvodu kompatibility se software. Přesný postup a soubory ke stažení jsou k dohledání na webových stránkách výrobce.

Obrázek 5.4: Vývojová deska X-NUCLEO-LPM01A pro měření odběru proudu.

5.3 Zdrojový kód programu

Program pro STM32U5 je implementovaný v jazyce C a skládá se z velkého množství podpůrných zdrojových souborů, které mohou být zařazeny do následujících skupin.

- Core Drivers
  - Ovladače pro konkrétní MCU včetně souboru main.c zajišťující nejzákladnější konfigurace procesoru jako je nastavení NVIC (tabulky interruptů), stack pointer, prvotní spuštění hodin atd.
- Board Drivers
  - Ovladače pro konkrétní desku, v našem případě B-U585I-IOT02A. Jedná se především o soubory pro práci se základními komponentami umístěnými na desce - tlačítka, LED diody, displeje a senzory atd.
- RTOS NetXDuo
  - Operační systém reálného času s duálním IPv4 a IPv6 TCP/IP stack speciálně navržený pro embedded systémy.
- STSAFE
  - Knihovny pro komponent STSAFE-A110, který zajišťuje kryptografické operace a prostor pro uložení privátních a veřejných klíčů. S procesorem komunikuje pomocí I2C protokolu a je vybaven anti-tamper funkcionalitami pro vysoký stupeň ochrany jak z pohledu softwarového útoku, tak i fyzického.
- WiFi
  - Ovladače pro komunikaci prostředníctvím WiFi modulu. Ten je s procesorem propojený pomocí protokolu SPI.
- IOTA
  - Fuknce pro vytvoření kompatibilní zprávy pro IOTA Tangle.
- Sodium
  - Knihovna pro kryptografické operace v případě, že uživatel nechce využít STSAFE.

V této části budou představeny hlavní bloky zdrojového kódu programu. Jednotlivé funkce příkazů jsou popsány přímo ve zdrojovém kódu.

```
int main(void)
{

  /* reset periferií, initializace flash a nastavení časové základny systick */
  HAL_Init();

  /* Konfigurace hlavních hodin pro procesor */
  SystemClock_Config();

  /* Nastavení spínaného zdroje SMPS */
  SystemPower_Config();

  /* Nastavení LED diod */
  BSP_LED_Init(LED_RED);
  BSP_LED_Init(LED_GREEN);

  /* Nastavení vstupně-výstupních pinů pro LED diody a tlačítka */
  MX_GPIO_Init();

  /* Initializace cache paměti */
  MX_ICACHE_Init();

  /* Initializace SPI periférie pro připojení WiFi modulu  */
  MX_SPI2_Init();

  /* Initializace UART periférie pro sériovou komunikaci s STM32U5  */
  MX_USART1_UART_Init();

  /* Initializace generátoru náhodných čísel pro random seed při provádění kryptografických operací  */
  MX_RNG_Init();

  /* Initializace periférie reálného času  */
  MX_RTC_Init();
  /* USER CODE BEGIN 2 */

  /* volání funkce pro vytvoření vláken aplikace */
  MX_ThreadX_Init();

  while (1)
  {

  }
  /* USER CODE END 3 */
}
```

Obrázek 5.5: Obsah hlavní funkce main.c.

Jak je patrné z výše uvedeného obrázku, smyčka while() je prázdná. V okamžiku, kdy je zavolána funkce MX_ThreadX_Init() jsou vytvořena vlákna aplikace - časování a správu událostí zajišťuje RTOS scheduler. Program je pro přehlednost členěn do více vláken s konkrétní úlohou a s různou prioritou přístupu k MCU.

Na následujícím obrázku je znázorněn blok kódu, který odešle data do IOTA Tangle, nastaví zdroje pro probuzení MCU, následně spustí časovač a přejde do módu standby. V tom okamžiku je procesor STM32 uspán a jediná RTC periferie a SRAM2 jsou aktivní. Jako jedna z možností probuzení je zde i náběžná hrana na pinu PC13. Tento pin je přes odpor a kondenzátor připojen k tlačítku umístěném na vývojové desce. Po zmáčknutí je pin připojen na VCC, na pinu se objeví náběžná hrana a procesor je probuzen. Pokud se u zařízení nacházíme fyzicky, můžeme data do Tangle odeslat zmáčknutím tohoto tlačítka.

```
static void iota_client_run(void)
{
  /* Clear all related wakeup flags*/
  send_data_message();

  /* Povolení zdroje probuzení - PC13 */
  HAL_PWR_EnableWakeUpPin(PWR_WAKEUP_PIN2_HIGH_1);

  /* Povolení zdroje probuzení - RTC */
  HAL_PWR_EnableWakeUpPin(PWR_WAKEUP_PIN7_HIGH_3);

  /* Nastavení registru s wakeup flags*/
  __HAL_PWR_CLEAR_FLAG(PWR_WAKEUP_FLAG2);

  /*Deaktivace vnitřního časovače RTC periferie*/
  HAL_RTCEx_DeactivateWakeUpTimer(&hrtc);
  __HAL_RTC_WAKEUPTIMER_CLEAR_FLAG(&hrtc, RTC_FLAG_WUTF);

  /*Aktivace vnitřního časovače RTC periferie a jeho spuštění*/
  if (HAL_RTCEx_SetWakeUpTimer_IT(&hrtc, 0x1B58, RTC_WAKEUPCLOCK_RTCCLK_DIV16, 0) != HAL_OK)
    {
      Error_Handler();
    }

  /*Přechod do režimu spánku*/
  HAL_PWR_EnterSTANDBYMode();
}
```

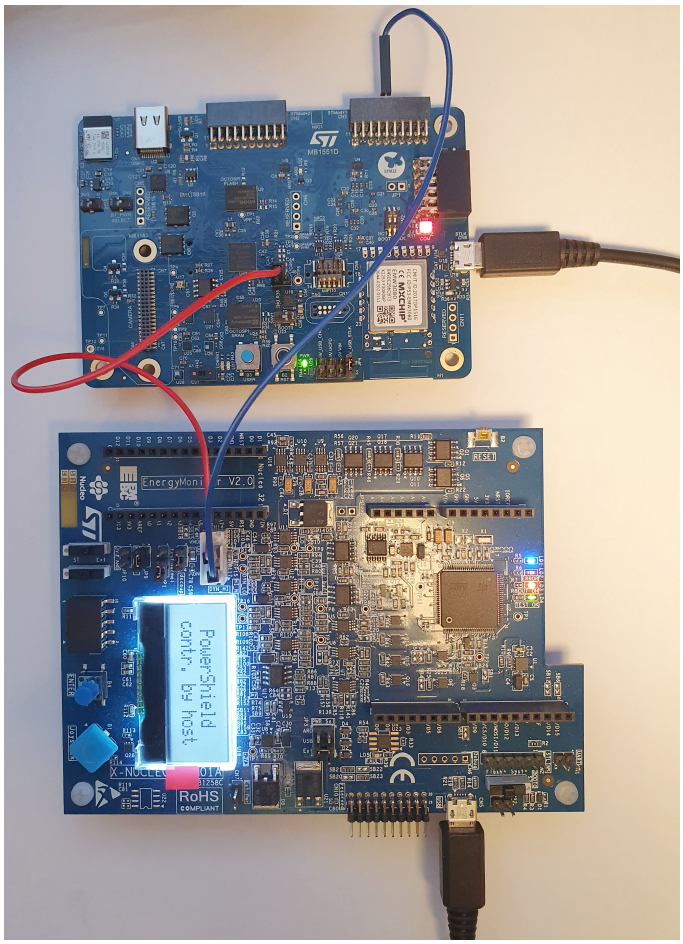
Obrázek 5.6: Obsah funkce pro odeslání zprávy do Tangle a přechodu do low-power módu.

Probuzení z režimu standby procesor vnímá jako restart MCU. Po každém probuzení projde programová smyčka přes main() funkci. Zda došlo k opuštění low-power módu nebo restartu se dá otestovat přečtením flagu v příslušném registru, který je snadno dohledetelný například v reference manuálu procesoru STM32U5.

5.4 Implementace koncového zařízení a měření odběru elektrického proudu

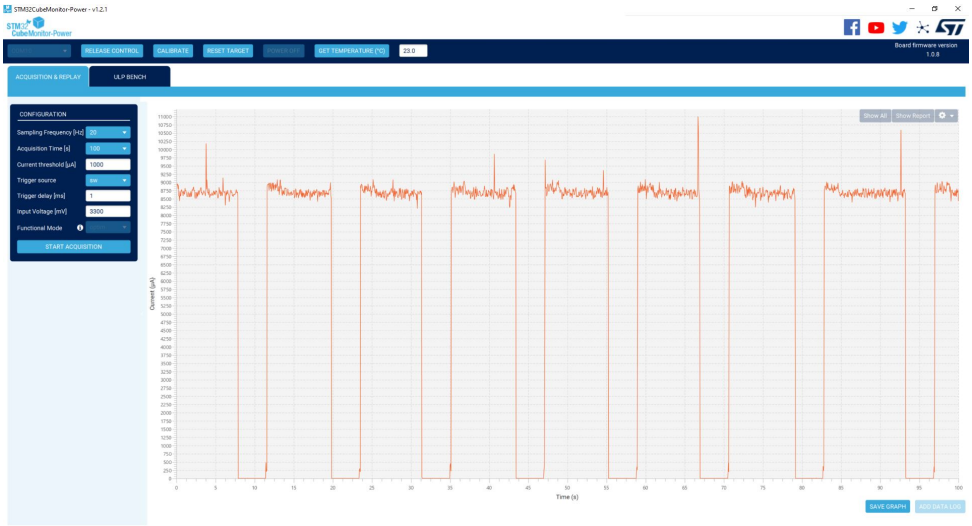
Pro IoT aplikaci bude nejvhodnější Standby + RTC který má odběr 440 nA. V tomto módu je procesor zcela zastaven, veškeré ostatní periférie procesoru vypnuty, pouze 8 Kb v paměti SRAM2 je během nečinnosti zachováno. Důležitým komponentem uvnitř procesoru, který je při tomto módu v činnosti je RTC (Real Time Clock) a pro časovou základnu bude využit externí oscilátor.

Každá vývojová deska má svůj uživatelský manuál, který je snadno dohledatelný na stránkách výrobce. Tam jsou popsány jednotlivé konektory, vývody a odhalené piny. Na desce B-U585I-IOT02A bude odpojena svorka JP3, přes kterou je možné změřit prodouvý odběr procesoru. Na druhé desce X-NUCLEO-LPM01A využijeme konektor CN14. Spuštěním programu STM32CubeMonitor-Power a připojením k COM portu získáme kontrolu nad funkcemi desky.



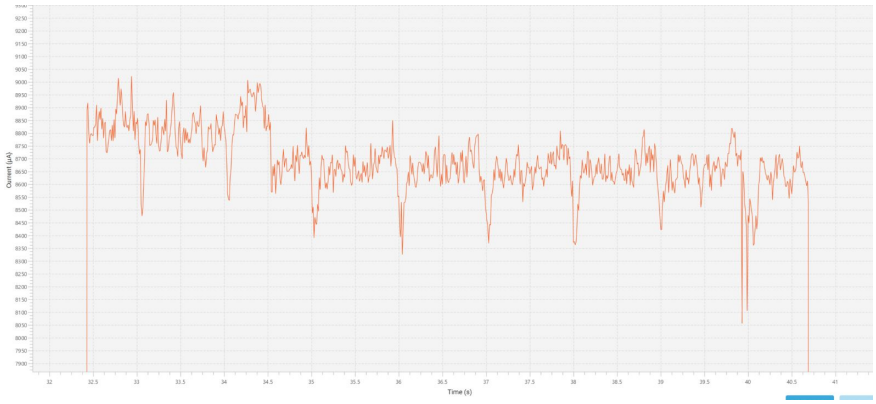
Obrázek 5.7: Propojení STM32 vývojových desek v režimu kalkulace odebíraného proudu.

Pro testovací účely bude vnitřní čítač periferie RTC nastaven na 3.5s, procesor bude uspán jen na chvíli. Na následujícím obrázku je zobrazen průběh testování.

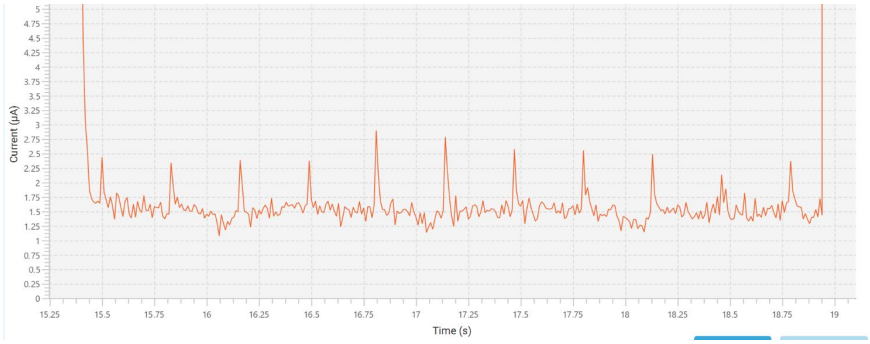


Obrázek 5.8: Testování funkčnosti časovače procesoru.

Je patrné, že v okamžiku probuzení procesoru spotřeba několikanásobně vystoupá. Celý proces připojení na WiFi, vyčtení dat a následné odeslání trvá 8.25s. Poté procesor přechází do standby módu a odběr proudu razantně klesne. Spotřeby v aktivním a neaktivním módu jsou řádově v jiných jednotkách. Přiblížením na jednotlivé průběhy můžeme spočítat průměrné hodnoty.



Obrázek 5.9: Průměrná hodnota odebíraného proudu v aktivním módu je 8.65mA.



Obrázek 5.10: Průměrná hodnota odebíraného proudu v módu spánku je 1.75uA.

Z průběhu, kdy je procesor ve standby módu lze pozorovat, že spotřeba je vyšší než 440nA jak uvádí datasheet daného procesoru. Využitím přesnějších externích hodin a zachováním většího počtu registrů bude odběr v low-power módu asi 1.75μA, což je stále zanedbatelná spotřeba.

5.5 Výpočet výdrže baterie

V tomto okamžiku bylo ověřeno, že vnitřní čítač periferie RTC funguje bez problému a můžeme přenastavit dobu buzení na hodnotu 6 hodin. Procesor se 4x za den probudí, odešle data a přejde do režimu spánku. Dalším důležitým krokem je výpočet výdrže baterie, abychom měli představu jak dlouho bude dané zařízení fungovat bez nutnosti servisu. K výpočtu využijeme klasickou komerčně dostupnou knoflíkovou baterii s kapacitou 260mAh. Pro výpočet výdrže je nutné využít průměrnou hodnotu z odběrů proudu jak v aktivním tak v neaktivním módu normovanou na jeden den.

$$C = 1.75 \cdot 10^{-3} mAh \tag{5.1}$$

$$i_{nonact} = 1.75 \cdot 10^{-3} mA \tag{5.2}$$

$$i_{act} = 8.65 mA \tag{5.3}$$

$$t_{day} = 86400 s \tag{5.4}$$

$$t_{act} = 8.25 s \tag{5.5}$$

$$t_{nonact} = (t_{day} - 4t_{act}) s \tag{5.6}$$

$$\bar{i} = \frac{t_{nonact}}{t_{day}} + \frac{4t_{act}}{t_{day}} = \frac{(86400 - 33)}{86400} \cdot 1.75 \cdot 10^{-3} mA + \frac{(33)}{86400} \cdot 8.65 mA = 0.00505 mA \tag{5.7}$$

Úlohu lze vyřešit pomocí jednoduchého vzorce:

$$t_{batterylife} = \frac{batterycapacity}{currentdraw} = \frac{C}{\bar{i}} = \frac{260 mAh}{0.00505 mA} = 51485 h \approx 5.9 years \tag{5.8}$$

Výpočtem rovnice (5.8) se dozvídáme, že naše koncové zařízení by mělo být funkční skoro 6 let. Jedná se o jednoduché IoT zařízení a v běžných aplikacích je nutný nejen uplink ale i downlink řídících příkazů nebo energeticky náročnější měření - u takové aplikace by mohl být odběr proudu několikrát vyšší, ale přesto by zařízení mohlo fungovat v řádech let.

5.6 Snížení spotřeby

Koncové zařízení je zcela funkční a obstálo by i nasazení v reálné aplikaci. V tuto chvíli by bylo možné spotřebu snížit použitím interního oscilátoru, úplným vypnutím SRAM2 paměti a také nastavením vstupně-výstupních pinů do analogového módu, kdy mají vysokou impedaci a odebírají minimální proud. Velký odběr elektrické energie má WiFi modul, který zajišťuje odeslání zprávy do IOTA Tangle.

V aplikaci s kritickou životností baterie by bylo možné data ze senzorů odeslat pomocí nízkoenergetické bezdrátové technologie. LoraWAN nebo Sigfox jsou vhodnými adepty pro tento účel - data by byla odeslána na gateway příslušné technologie, ta by zpracovala dané požadavky a odeslala data do Tangle. V tomto případě je gateway napájená ze sítě a není třeba řešit její spotřebu.

Kapitola 6

Závěr a diskuze

V diplomové práci byl proveden teoretický rozbor nových technologií pro zabezpečení komunikace v IoT. Byly představeny staré blokchainové technologie, které sloužily jako základ pro možnosti vylepšení současných a dřívějších technologií. Jako nejslibnější koncept se zdají být DAG struktury, které využívají orientované acyklické grafy pro svůj ledger. Následně byla vybrána IOTA Tangle jako nejpoužívanější DAG ledger současné doby a byly detailně popsány její funkční principy. Hlavní důraz byl kladen na vnitřní strukturu, strukturu zprávy a možnosti zabezpečení. Z hlediska bezpečné komunice, byl představen protokol L2Sec, který se stará o kryptografické zabezpečení zprávy, kterou uživatel hodlá umístit do Tangle. Tento protokol je s výhodou využit v IoT platformách, neboť je implementován v jazyce C a je možné ho aplikovat v levném hardware. Tímto byla uzavřena teoretická část, která byla pro čtenáře nezbytným předpokladem pro pochopení implementace infrastruktury v části praktické.

Praktická část práce představuje vhodný a komerčně dostupný hardware a software od firmy STMicroelectronics pro implementaci IoT zařízení, které je schopné odeslat zprávy do IOTA Tangle. Nejdříve je čtenáři představen ukázkový program implementovaný jazyce C se všemi jeho funkcemi a ovládacími prvky. Ten je vhodný pro pochopení funkčních principů a ověření, že daná vývojová deska a program fungují. Následně je implementovaný vlastní program, který by bylo možné aplikovat ve skutečné IoT aplikaci. Do programu byly přidány další nezbytné funkcionality jako RTC a low-power mód a byl spočten předpokládaný odběr elektrické energie modulu.

Diplomová práce splnila všechny body doporučené osnovy a je dobrým základem pro čtenáře, který by chtěl pochopit jak teoretické principy fungování IOTA Tangle, tak jeho praktickou implementaci.

Příloha A

Literatura

[1] HASSAN, Wan Haslina, et al. Current research on Internet of Things (IoT) security: A survey. Computer networks, 2019, 148: 283-294.

[2] ALFANDI, Omar, et al. A survey on boosting IoT security and privacy through blockchain. Cluster Computing, 2021, 24.1: 37-55

[3] CHVYKOVA, Viktoria, Decentralized Authentication of IoT Devices Based on Blockchain Technology, Master thesis, CTU In Prague, 2022

[4] Noviello, Carmine, *Mastering STM32 [PDF]*, Listopad 2016, Itálie, Leanpub

[5] *HAL User Manual*, `https://www.st.com/resource/en/user_manual/um2659-description-of-stm32l5-hal-and-lowlayer-drivers-stmicroelectronics.pdf`, [Online, navštíveno 27. 12. 2023]

[6] *STM32U585 datasheet*, `https://www.st.com/resource/en/datasheet/stm32u585ai.pdf`, [Online, navštíveno 27. 12. 2023]

[7] *STM32 IOTA Details*, `https://www.st.com/en/evaluation-tools/b-u585i-iot02a.html`, [Online, navštíveno 27. 12. 2023]

[8] *Centralilized end decentralized system*, `https://blockchain.ieee.org/technicalbriefs/january-2019/enabling-distributed-and-trusted-iot-systems-with-blockchain-technology`, [Online, navštíveno 27. 12. 2023]

[9] *Internet of Things*, `https://www.britannica.com/science/Internet-of-Things`, [Online, navštíveno 27. 12. 2023]

[10] *IoT Definition*, `https://www.oracle.com/internet-of-things/what-is-iot/`, [Online, navštíveno 27. 12. 2023]

[11] *LoRaWAN*, `https://lora-alliance.org/wp-content/uploads/2020/11/lorawan_security_whitepaper.pdf`, [Online, navštíveno 27. 12. 2023]

[12] *IOTA payloads*, https://wiki.iota.org/iota.rs/explanations/messages_payloads_and_transactions/, [Online, navštíveno 27. 12. 2023]

[13] *DLT, Blockchain structure* , https://training.corda.net/blockchain-basics/distributed-ledger-technology/, [Online, navštíveno 27. 12. 2023]

[14] *DAG Structure*, https://arxiv.org/pdf/1905.10925.pdf, [Online, navštíveno 27. 12. 2023]

[15] *Blockchain vs Tangle*, https://en.wikipedia.org/wiki/File:Blockchain_vs_tangle_bottleneck.png, [Online, navštíveno 27. 12. 2023]

[16] *L2Sec protocol*, https://www.mdpi.com/1424-8220/22/4/1384, [Online, navštíveno 27. 12. 2023]

[17] *STM32 IOTA user manual*, https://www.st.com/resource/en/user_manual/um2606-getting-started-with-the-iota-distributed-ledger-technology-software-pdf, [Online, navštíveno 27. 12. 2023]

[18] *IOTA overview*, https://wiki.iota.org/iota.rs/overview/, [Online, navštíveno 27. 12. 2023]

[19] *X-NUCLEO-LPM01A user manual*, https://www.st.com/resource/en/user_manual/um2243-stm32-nucleo-expansion-board-for-power-consumption-measurement-stmicr pdf, [Online, navštíveno 27. 12. 2023]

[20] *Tangle Explorer*, https://explorer.iota.org/devnet, [Online, navštíveno 27. 12. 2023]

[21] *STM32 power management*, https://www.st.com/content/ccc/resource/training/technical/product_training/group1/95/38/81/9b/cb/0d/43/89/STM32U5-System-Power-management_PWRMNGMNT/files/STM32U5-System-Power-management_PWRMNGMNT.pdf/_jcr_content/translations/en.STM32U5-System-Power-management_PWRMNGMNT.pdf, [Online, navštíveno 27. 12. 2023]

[22] *Tangle structure*, https://wiki.iota.org/learn/protocols/iota2.0/core-concepts/data-structures/, [Online, navštíveno 27. 12. 2023]

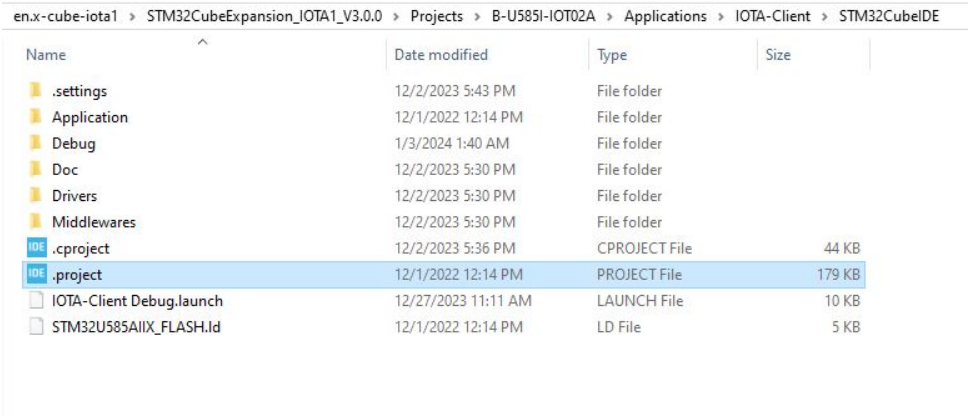
[23] *RTC Timers*, https://www.st.com/resource/en/product_training/stm32l4_wdg_timers_rtc.pdf, [Online, navštíveno 27. 12. 2023]

[24] *IOTA PoW*, https://medium.com/bytes-io/iota-proof-of-work-remote-vs-local-explained-1cbd89392a79, [Online, navštíveno 27. 12. 2023]

Příloha B

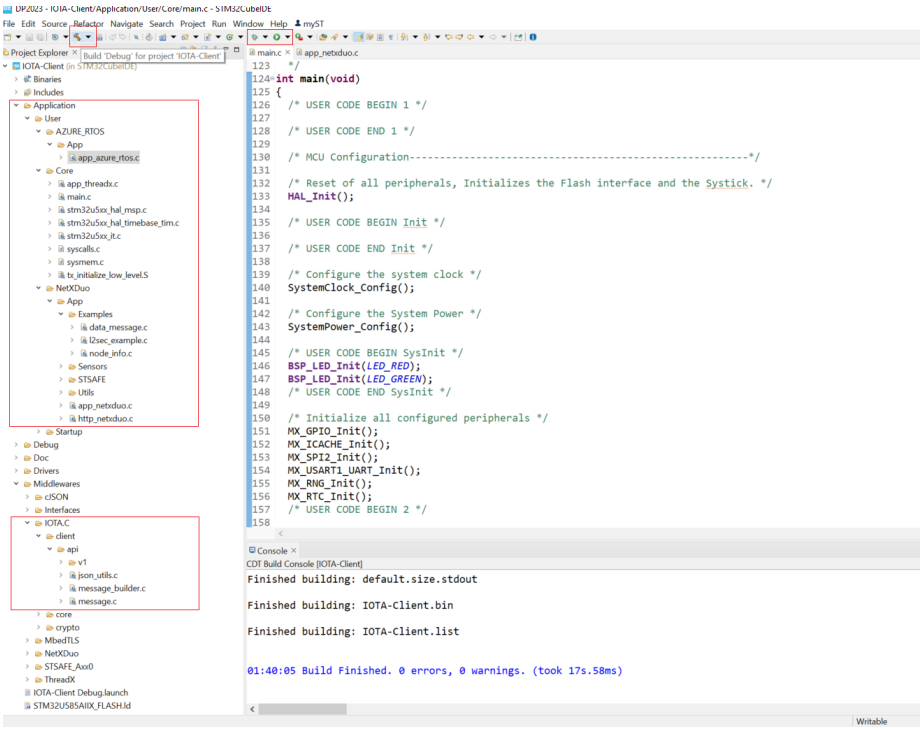
Zdrojový kód

Zdrojový kód pro desku B-U585I-IOT02A je ve formě projektu pro vývojové prostředí STM32CubeIDE ve verzi 1.14.0 a byl otestován na operačním systému Windows 10. Po rozzipování přílohy je nutné se přes složky proklikat až k samotnému projektu, jak je naznačeno na následujícím obrázku. Dvojtým kliknutím na ikonu .project se automaticky spustí vývojové prostředí STM32CubeIDE.



Obrázek B.1: Cesta k projektu v systému Windows 10.

Projekt se skládá z velkého množství podpůrných souborů a middleware. Uživatel má například na výběr, zda využije externí komponent STSafe pro kryptografické operace nebo se přikloní k opensource knihovně Sodium, která nabízí stejné funkce, ale dané operace mohou být pro procesor časově náročnější. Dále je možné v kompilátoru nastavit optimalizaci kódu z pohledu velikosti, debuggování nebo rychlosti. Všechny možnosti a nastavení je možné dohledat v uživatelském manuálu pro STM32CubeIDE. Na následujícím obrázku můžeme vidět strukturu projektu.



Obrázek B.2: Struktura projektu ve vývojovém prostředí STM32CubeIDE.

Červenými obdelníky jsou zdůrazněny důležitité ovládací prvky a soubory se zdrojovým kódem. Ve vrchní liště je umístěna ikona kladívka, které slouží ke kompilaci programu, ikonka brouka pro debuggování kódu pomocí SWD interface a ikonka zelené šipečky pro nahrání programu do MCU.
Důležitými složkami se soubory jsou následující:

- AZURE_RTOS
  - Funkce operačního systému reálného času.
- Core
  - Soubor main.c s funkcí main(), MCU support pacakge, nastavení časové základny a nastavení interruptů.
- NetXDuo
  - Ukázkový program pro poslání zpráv do IOTA Tangle, v souboru app_nextduo.c se nachází funkce static void iota_client_run(void) ve které dochází k odeslání zprávy do IOTA Tangle, nastavení zdrojů pro probuzení MCU, zapnutí časovače a přechodu do standby módu.
- IOTA.C
  - Funkce pro tvorbu zprávy podle náležitostí protokolu Chrysalis v síti IOTA Devnet.