



VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ

BRNO UNIVERSITY OF TECHNOLOGY

FAKULTA INFORMAČNÍCH TECHNOLOGIÍ

FACULTY OF INFORMATION TECHNOLOGY

ÚSTAV POČÍTAČOVÉ GRAFIKY A MULTIMÉDIÍ

DEPARTMENT OF COMPUTER GRAPHICS AND MULTIMEDIA

NÁZEV PRÁCE

THESIS TITLE

DIPLOMOVÁ PRÁCE

MASTER'S THESIS

AUTOR PRÁCE

AUTHOR

Bc. JURAJ HOLUB

VEDOUCÍ PRÁCE

SUPERVISOR

Ing. IVAN HOMOLIAK, Ph.D.

BRNO 2021

Abstrakt

Do tohoto odstavce bude zapsán výtah (abstrakt) práce v českém (slovenském) jazyce.

Abstract

Do tohoto odstavce bude zapsán výtah (abstrakt) práce v anglickém jazyce.

Klíčové slová

Sem budou zapsána jednotlivá klíčová slova v českém (slovenském) jazyce, oddělená čárkami.

Keywords

Sem budou zapsána jednotlivá klíčová slova v anglickém jazyce, oddělená čárkami.

Citácia

HOLUB, Juraj. *Název práce*. Brno, 2021. Diplomová práce. Vysoké učení technické v Brně, Fakulta informačních technologií. Vedoucí práce Ing. Ivan Homoliak, Ph.D.

Název práce

Prehlásenie

Prohlašuji, že jsem tuto bakalářskou práci vypracoval samostatně pod vedením pana X... Další informace mi poskytli... Uvedl jsem všechny literární prameny, publikace a další zdroje, ze kterých jsem čerpal.

.....

Juraj Holub

10. septembra 2021

Podakovanie

V této sekci je možno uvést poděkování vedoucímu práce a těm, kteří poskytli odbornou pomoc (externí zadavatel, konzultant apod.).

Obsah

1	Úvod	2
2	Blockchain	3
2.1	Distribovaná účtovná kniha	3
2.1.1	Vlastnosti blockchainu	3
2.1.2	Aplikačné využitie	4
2.2	Moderná kryptografia	4
2.2.1	Hash	5
2.2.2	Digitálny podpis	5
2.3	Peer-to-peer sieť	6
2.3.1	Referenčný model	6
2.3.2	Využitie v blockchaine	6
2.4	Datová štruktúra blockchain	7
2.4.1	Transakcia	8
2.4.2	Hlavička bloku	8
2.4.3	Obsah bloku	8
2.4.4	Binárny hashovací strom	8
	Literatúra	10
	A Jak pracovat s touto šablonou	11
	B Psaní anglického textu	16
	C Checklist	20
	D L^AT_EXpro začátečníky	24
	E Příklady bibliografických citací	27

Kapitola 1

Úvod

TODO

Kapitola 2

Blockchain

2.1 Distribuovaná účtovná kniha

Účtovná kniha (anglicky *ledger*) sa v histórii ľudstva dlhodobo používa na záznam rôznych položiek, najčastejšie peňazí a majetku. Príchod digitalizácie a globalizácie rozšíril tento známy koncept o nové požiadavky. *Distribuovaná účtovná kniha* (anglicky *distributed ledger*) je všeobecne technológia, ktorá poskytuje databázu zdieľanú naprieč viacerými inštitúciami, krajinami a to typicky verejne. Najtypickejším odvetvím využitia distribuovanej účtovnej knihy je bankovníctvo. Banka poskytuje centralizovanú autoritu, ktorá zabezpečuje bezpečnú manipuláciu s peniazmi klientov. [10]

V roku 2008 bola publikovaná práca [8], ktorá navrhla *decentralizovanú* distribuovanú účtovnú knihu. Práca navrhla koncept elektronického platobného systému, ktorého bezpečnosť je založená na kryptografickom dôkaze namiesto dôvere v centralizovanú autoritu. **Blockchain** je decentralizovaná účtovná kniha založená na *peer-to-peer* sieti a asymetrickej kryptografii s digitálnym podpisom (pozri 2.2).

2.1.1 Vlastnosti blockchainu

Blockchain je datová štruktúra, ktorá má nasledujúce vlastnosti:

- **Decentralizácia:** Blockchain je peer-to-peer sieť, ktorá nepotrebuje centralizovanú dôveryhodnú autoritu.
- **Auditovateľnosť:** Blockchain v sebe nesie celú históriu zmien jeho obsahu a teda každú zmenu stavu dát uložených v blockchaine je možné sledovať.
- **Nemennosť:** Pri správnom použití a dostatočne veľkej sieti nie je možné zmeniť históriu alebo dátový obsah blockchainu.
- **Anonymita:** Užívatelia pracujúci s blockchainom používajú na identifikáciu modernú kryptografiu (asymetrické kľúče, hashovanie a digitálny podpis). Takýto kryptografický identifikátor neodhaľuje skutočnú identitu užívateľa.

Nemennosť a auditovateľnosť blockchainu sú zabezpečené pomocou samotnej datovej štruktúry, ktorá využíva modernú kryptografiu (viď sekcia 2.4) a taktiež pomocou samotnej decentralizovanej siete (viď sekcia 2.3). [1]

2.1.2 Aplikačné využitie

Blockchain bol navrhnutý a po prvýkrát implementovaný s účelom poskytnúť peňažnú menu nezávislú od centralizovaného bankovníctva. Tento prvý, a najznámejší, blockchain je Bitcoin [8]. Avšak vlastnosti blockchainovej technológie nachádzajú uplatnenie vo veľkom množstve odvetví. Nasledujúci zoznam vymenúva niekoľko aplikácií, ktoré blockchain môže riešiť [6]:

- **Elektronická peňaženka:** Elektronické peňaženky pre obchod s nejakou formou peňazí (typicky v podobe tokenov). Takéto tokeny sú typicky vlastnené pomocou privátneho kľúča, ktorý má uschovaný majiteľ. Majiteľ môže vlastníctvo tokenov presúvať na iné subjekty v danej sieti.
- **Zmenárne:** V dnešnej dobe existuje veľké množstvo kryptomien. S toho dôvodu sa prirodzene zvyšuje dopyt po zmenárni medzi jednotlivými kryptomenami. Klasická zmenáreň je riešená tradične centralizovanou autoritou. Avšak blockchain je vhodnou technológiou aj pre decentralizovanú zmenáreň.
- **Súborové systémy:** V dnešnej dobe už existujú decentralizované súborové systémy založené na peer-to-peer sieťach. Implementácia takéhoto decentralizovaného súborového systému ako blockchain by nám umožnila nepopierateľne a trasovateľne verzovať zmeny v obsahu.
- **Správa identít:** Správa identít je typicky centrálna autorita, ktorá prideliť pre konkrétne entity určité zdroje na ktoré majú právo. Ide o schému podobnú banke. Blockchain by v tomto prípade opäť umožnil náhradu tejto centralizovanej autority za decentralizovanú sieť.
- **Volby:** Elektronické voľby sú ďalším vhodným príkladom, kde sa dá efektívne využiť blockchain. Voliace entity predstavujú decentralizovanú sieť a vlastnosti blockchainu zase poskytujú transparentnosť a verejnú overiteľnosť.
- **Reputačné systémy:** Reputačné systémy slúžia na meranie úrovne dôvery v určité entity. Typickým príkladom je reputácia rôznych predajcov na základe hlasovania zákazníkov. Transparentnosť a nemennosť blockchainovej histórie by znížila možnosť manipulácie s reputáciou v prospech nejakej entity.
- **Aukcie:** Elektronická aukcia je služba veľmi podobná elektronickej peňaženke alebo zmenárni s podobnými bezpečnostnými požiadavkami. Tieto vlastnosti by opäť dokázala pokryť technológia blockchain.

2.2 Moderná kryptografia

Pre pochopenie technológie blockchain je potrebná základná znalosť modernej kryptografie. V tejto sekcii je popísaný kryptografický hash (pozri 2.2.1) a digitálny podpis (pozri 2.2.2). Obe tieto kryptografické primitívy sú základom na ktorom stojí nemennosť, auditovateľnosť a anonymita blockchainu.

2.2.1 Hash

Hashovacia funkcia je taká funkcia h , ktorá má ako parameter x reťazec bitov ľubovoľnej dĺžky a vracia reťazec y s konštantnou dĺžkou. Reťazec y voláme hash. Hashovacia funkcia vracia pre konkrétny vstup vždy rovnaký hash.

$$h(x) = y$$

Kryptografická hashovacia funkcia, alebo tiež jednocestná funkcia (anglicky *one way function*), je taká hashovacia funkcia pre ktorú platia nasledujúce tri vlastnosti:

1. Pre daný hash x je výpočetne nezládnuté nájsť správu takú, že $h(x) = y$. Anglicky voláme túto vlastnosť *first preimage resistant*.
2. Pre danú správu je výpočetne nezládnuté nájsť inú správu s rovnakým hashom. Anglicky voláme túto vlastnosť *second preimage resistant*.
3. Pre ľubovoľnú správu je výpočetne nezládnuté nájsť inú správu s rovnakým hashom. Anglicky voláme túto vlastnosť *collision resistant*.

Hashovacie funkcie majú v oblasti počítačovej bezpečnosti dôležité využitie:

- Bezpečné ukladanie hesiel: Digitálna služba neukladá v databáze heslo, ale len jeho hash. Pri ukradnutí databázy nedochádza k odhaleniu hesiel užívateľov.
- Integrita dát: Hashovacia funkcia môže byť použitá na ochranu integrity ľubovoľných dát. Ak spočítate hash veľkého súboru a bezpečne ho uložíte tak ste schopný detekovať, že niekto tento súbor zmenil.
- Digitálny podpis: Hashovacia funkcia je kryptografické primitívum potrebné pre vytvorenie digitálneho podpisu.

Existuje množstvo hashovacích funkcií. Medzi veľmi známe a používané patrí napríklad MD5 (128 bitový výstup), SHA256 (256 bitový výstup), SHA512 (512 bitový výstup). [7, 12]

2.2.2 Digitálny podpis

Moderná kryptografia používa pre zaistenie dôvernosti šifrovanie pomocou tajného kľúča. Pre zašifrovanie a dešifrovanie tajnej správy je potrebná znalosť tajného kľúča. Tento spôsob šifrovania zaisťuje dôvernosť avšak nezaistuje nepopierateľnosť pretože obe komunikujúce strany poznajú tajný kľúč a teda nie je možné právne dokázať kto správu napísal. Na zaistenie nepopierateľnosti sa používa asymetrické šifrovanie, ktoré používa dvojicu kľúčov:

- **Privátny kľúč** je tajný a pozná ho len odosielateľ správy. Odosielateľ používa tento kľúč na zašifrovanie správy.
- **Verejný kľúč** je dostupný komukoľvek. Ktokoľvek s týmto kľúčom dokáže dešifrovať správu.

Tieto dva kľúče tvoria dvojicu prepojenú matematickým spôsobom. Zo znalosti verejného kľúča je výpočetne nezládnuté zistiť privátny kľúč. Zašifrovaná správa nie je dôverná pretože ktokoľvek môže použiť verejný kľúč na jej dešifrovanie. Avšak zašifrovaná správa je nepopierateľne napísaná vlastníkom privátneho kľúča. Tento koncept je základom digitálneho podpisu. Pre väčšiu efektivitu sa nešifruje celá správa ale len jej hash (viď Sekcia 2.2.1). Najznámejšie algoritmy na digitálny podpis sú RSA, DSA, ECDSA. [7]

2.3 Peer-to-peer sieť

Technológia blockchain je postavená na peer-to-peer sieťach. Peer-to-peer sieť sa podieľa na decentralizovanosti, nemennosti a auditovateľnosti blockchainu.

Peer-to-peer sieť je dynamický súbor nezávislých uzlov (anglicky *peers*), ktoré sú prepojené do grafu. Každý uzol obsahuje zdroje, ktoré zdieľa všetkým ostatným uzlom v sieti. [4, 11] Dôvod existencie peer-to-peer sietí je teda decentralizovaný spôsob zdieľania zdrojov ako sú súbory, fyzické zariadenia, výpočetný výkon alebo aj elektronické finančné zdroje. Dnes existuje množstvo peer-to-peer sietí. Veľmi známe sú napríklad Gnutella, Kazaa alebo BitTorrent. [2]

2.3.1 Referenčný model

Najbežnejšie technické riešenie peer-to-peer siete je navrstvenie siete (anglicky *overlay network*) na už existujúcu sieť, ktorou je typicky Internet. Takúto sieť potom môžeme definovať ako päťicu (P, R, I, F_P, F_R) , kde:

- P je množina uzlov
- R je množinu zdrojov
- I je priestor identifikátorov
- $F_P : P \rightarrow I$ je funkcia, ktorá mapuje uzoly na identifikátory
- $F_R : R \rightarrow I$ je funkcia, ktorá mapuje zdroje na identifikátory

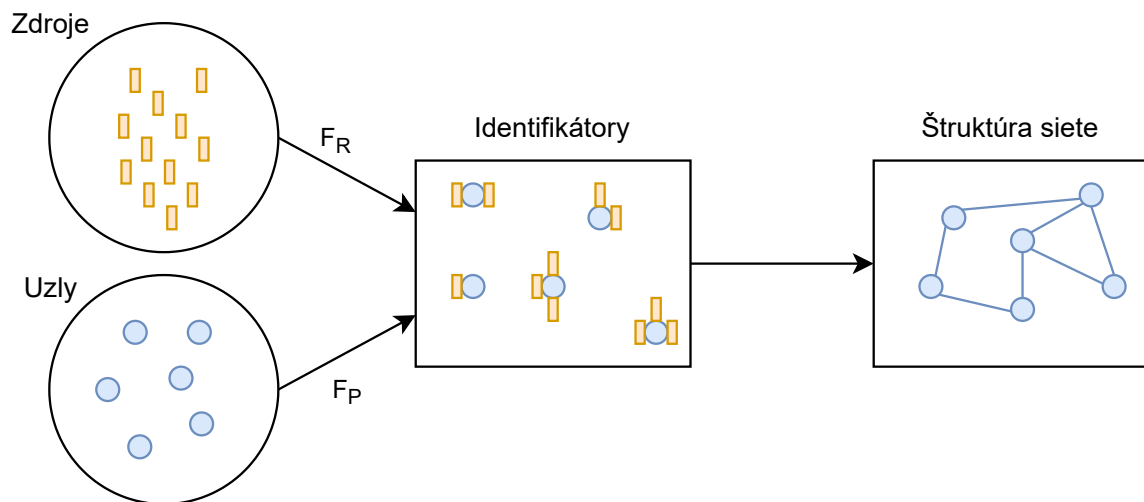
Obrázok 2.1 ukazuje princíp fungovania takto definovanej siete. Tvorba siete s týmto modelom je potom závislá od šiestich návrhových aspektov:

1. Voľba priestoru identifikátorov.
2. Mapovanie zdrojov a uzlov na identifikátory.
3. Správa priestoru identifikátorov v réžii uzlov siete.
4. Tvorba grafu (štruktúra siete).
5. Stratégia smerovania (anglicky *routing*).
6. Stratégia údržby.

Konkrétne riešenie pre popisovaných šesť aspektov je závislé od požiadaviek na efektivitu, škálovateľnosť, samoorganizovateľnosť, odolnosť voči chybám a kooperáciu. [2]

2.3.2 Využitie v blockchaine

Elektronické financie sú typicky reprezentované pomocou elektronických mincí. Takáto minca je reprezentovaná pomocou nejakej sekvencie bitov. Avšak narozdiel od fyzických mincí, elektronické mince umožňujú jednoduchú falzifikáciu. Útočník skopíruje bitový reťazec danej mince a zaplatí ním viacnásobne rôzne produkty. Tento útok sa volá zdvojnásobenia výdavkov (anglicky *double-spending attack*). Proti tomuto útoku existuje tradičné zabezpečenie pomocou centrálnej autority. Banka je centrálna autorita, ktorá schvaľuje



Obr. 2.1: Referenčný model peer-to-peer siete. [2]

všetky manipulácie s elektronickými mincami a teda neumožní použiť mincu takýmto podvodným spôsobom. Avšak toto riešenie nie je možné použiť v decentralizovanej sieti, kde centrálna autorita neexistuje. V prípade decentralizovanej siete je možné zabrániť tomuto útoku pomocou použitia dátovej štruktúry blockchain. [5]

Kryptomena Bitcoin ako prvá navrhla použitie peer-to-peer siete v spojení s blockchain technológiou pre zabránenie double-spending útoku. V takejto sieti je jediný zdroj na zdieľanie a to je dátová štruktúra blockchain v ktorej sú uložené všetky informácie o elektronických financiách. Zjednodušene môžeme povedať, že majorita uzlov siete zdieľa rovnaký zdroj (rovnakú kópiu blockchainu). Ak chce niektorý uzol vykonať finančnú transakciu tak zašle správu s navrhovanou zmenou blockchainu do siete. Uzly v tejto sieti nie je potrebné identifikovať pretože správy posielané v tejto sieti nie sú smerované na žiadne konkrétne miesto. Keď uzol prijme správu s nejakou modifikáciou tak si overí či ide o validnú požiadavku na finančnú transakciu. Štruktúra blockchainu používa modernú kryptografiu na overenie validnosti transakcie (pozri sekciu 2.2). Blockchain, ktorý vlastní väčšina siete je ten, ktorý sa považuje za pravdu. Útočník by musel teda vlastniť aspoň 51 % uzlov v sieti aby mohol vykonať double-spending útok. Ak je daná sieť dostatočne veľká tak by toho útočník nemal byť schopný dosiahnuť. [8]

2.4 Dátová štruktúra blockchain

Blockchain je dátová štruktúra podobná zoznamu (anglicky *linked list*). Blockchain organizuje dáta do podmnožín, ktoré sa volajú bloky. Blok je podobný uzlu v zozname. Každý blok obsahuje referenciu na ďalší blok. Rozdiel medzi zoznamom a blockchainom je v tom, že referencia blockchainu je zabezpečená proti manipulácii (anglicky *tamper-evident*) pomocou modernej kryptografie. Bežný zoznam používa referenciu pomocou ukazovateľov (anglicky *pointers*), ktoré môže ktokoľvek a kedykoľvek pozmeniť bez toho aby pozmenil dátový obsah. Naopak, blockchain vôbec neumožňuje meniť už pridané bloky. Jediná povolená operácia je prídanie ďalšieho bloku na koniec blockchainu. [1]

Každý blok obsahuje dáta, ktoré sú typicky vo forme transakcií. Kryptograficky bezpečný blockchain by mohol fungovať aj tak, že v každom bloku bude uložená práve jedna

transakcia. Z dôvodu optimalizácie je ale v jednom bloku uložené množstvo transakcií. Vďaka tejto optimalizácii nemusí celá sieť vytvárať konsenzus po každej transakcii. Samotné transakcie v rámci jedného bloku sú ukladané v ďalšej dátovej štruktúre, ktorá taktiež používa kryptografické hashovanie (viď sekcia 2.4.4). [9]

2.4.1 Transakcia

Transakcia je základný prvok blockchainu. Ide o elementárnu dátovú jednotku, ktorá obsahuje dáta uložené v blockchaine. Bitcoin, prvý blockchain, použil transakciu na manipuláciu s elektronickými financiami. Takáto transakcia sa skladá z troch častí:

- **Množina vstupov:** Každý vstup má uložený hash predošlej transakcie s ktorej vychádza. Ďalej definuje, ktoré výstupy s predošlej transakcie si nárokuje. Nakoniec obsahuje digitálny podpis, ktorý autorizuje tvorcu transakcie.
- **Množina výstupov:** Každý výstup má hodnotu, ktorá je uchovávaná v blockchaine (typicky minca nejakej kryptomeny). Suma hodnôt všetkých výstupov transakcie musí byť menšia alebo rovná sume všetkých vstupov transakcie. Ak je menšia, tak tento rozdiel je použitý ako odmena pre toho, kto publikoval tento blok blockchainu.
- **Hlavička:** Obsahuje hash transakcie, ktorý je používaný ako unikátny identifikátor pomocou ktorého sa na transakciu odkazujeme.

2.4.2 Hlavička bloku

2.4.3 Obsah bloku

transakcie

2.4.4 Binárny hashovací strom

Binárny hashovací strom alebo tiež Merkle strom (anglicky *Merkle tree*) je datová štruktúra podobná binárnemu stromu, ktorá slúži na efektívne a rýchle vypočítanie hashu veľkého množstva dát. Blockchain používa tento strom na časovo efektívny výpočet hashu všetkých transakcií. Takto vypočítaný hash je uložený v hlavičke bloku.

Merkle strom je vyvážený binárny strom, kde listové uzly obsahujú jednotlivé transakcie uložené v danom bloku blockchainu. Každý nelistový uzol stromu obsahuje hash vypočítaný z jeho potomkov. Koreňový uzol teda obsahuje hash celého stromu a teda aj všetkých transakcií. Pridanie, odobranie, zmena obsahu, alebo zmena poradia transakcií bude teda viesť k zmene koreňového hashu. Konštrukcia stromu, inak povedané výpočet hashu všetkých transakcií, prebieha nasledovne:

1. Všetky transakcie sú uložené do listovej úrovne stromu. Ak je počet transakcií nepárny tak, je posledná vložená dvakrát.
2. Nad každým listovým uzlom je vypočítaný hash.
3. Každý nelistový uzol skonkatenuje hash ľavého a pravého syna, vypočíta nad nimi hash a uloží si ho.

Konštrukcia takéhoto stromu pre n transakcií má časovú zložitosť $O(\log(n))$. Takýto spôsob výpočtu hashu je teda veľmi efektívny pre veľké množstvo transakcií (blok v blockchaine bežne obsahuje stovky transakcií). [3]

Merkle strom umožňuje efektívne šetriť pamäťové nároky blockchainu. Do blockchainu sú neustále pridávané nové bloky, ktoré obsahujú aj rovnaké staré transakcie. Ak už sú transakcie zaznamenané v dostatočne veľkom množstve blokov tak sú z hľadiska bezpečnosti nemenné. V nových blokoch ich už preto nie je potrebné ukladať. Nový blok si preto uloží len hashe starých vetiev stromu, ale ich obsah už nepotrebuje. Takto je zachovaná integrita hashu všetkých transakcií. [8]

Literatúra

- [1] *Horizen Academy - Blockchain as a data structure* [<https://academy.horizen.io/technology/expert/blockchain-as-a-data-structure/>]. Accessed: 2021-06-03.
- [2] ABERER, K., ALIMA, L., GHODSI, A., GIRDZIJAUSKAS, S., HARIDI, S. et al. The Essence of P2P: A Reference Architecture for Overlay Networks. In:. Január 2005, s. 11– 20. DOI: 10.1109/P2P.2005.38. ISBN 0-7695-2376-5.
- [3] BOSAMIA, M. a PATEL, D. Current Trends and Future Implementation Possibilities of the Merkel Tree. *INTERNATIONAL JOURNAL OF COMPUTER SCIENCES AND ENGINEERING*. August 2018, zv. 6, s. 294–301. DOI: 10.26438/ijcse/v6i8.294301.
- [4] BUFORD, J., YU, H. a LUA, E. P2P Networking and Applications. *P2P Networking and Applications*. Január 2009. DOI: 10.1016/B978-0-12-374214-8.X0001-3.
- [5] HOEPFMAN, J.-H. Distributed Double Spending Prevention. Marec 2008.
- [6] HOMOLIAK, I., VENUGOPALAN, S., HUM, Q., REIJSBERGEN, D., SCHUMI, R. et al. The Security Reference Architecture for Blockchains: Towards a Standardized Model for Studying Vulnerabilities, Threats, and Defenses. Október 2019.
- [7] MENEZES, A. J. *Handbook of Applied Cryptography*. Taylor & Francis Inc, 1996. ISBN 0849385237ID.
- [8] NAKAMOTO, S. Bitcoin: A Peer-to-Peer Electronic Cash System. *Cryptography Mailing list at https://metzdowd.com*. Marec 2009.
- [9] NARAYANAN, A., BONNEAU, J., FELTEN, E., MILLER, A. a GOLDFEDER, S. *Bitcoin and Cryptocurrency Technologies: A Comprehensive Introduction*. Princeton University Press, 2016. ISBN 9780691171692.
- [10] ROBLEH ALI, R. B. et al. *Distributed Ledger Technology: beyond block chain*. London, 1 Victoria Street, 2016.
- [11] SCHOLLMEIER, R. A Definition of Peer-to-Peer Networking for the Classification of Peer-to-Peer Architectures and Applications. In:. September 2001, s. 101 – 102. DOI: 10.1109/P2P.2001.990434. ISBN 0-7695-1503-7.
- [12] SMART, N. *Cryptography: An Introduction*. McGraw-Hill, 2003.

Príloha A

Jak pracovat s touto šablonou

V této příloze je uveden popis jednotlivých částí šablony, po kterém následuje stručný návod, jak s touto šablonou pracovat. Pokud po jejím přečtení k šabloně budete mít nějaké dotazy, připomínky apod., neváhejte a napište na e-mail `sablona@fit.vutbr.cz`.

Popis částí šablony

Po rozbalení šablony naleznete následující soubory a adresáře:

bib-styles Styly literatury (viz níže).

obrazky-figures Adresář pro Vaše obrázky. Nyní obsahuje `placeholder.pdf` (tzv. TODO obrázek, který lze použít jako pomůcku při tvorbě technické zprávy), který se s prací neodevzdává. Název adresáře je vhodné zkrátit, aby byl jen ve zvoleném jazyce.

template-fig Obrázky šablony (znak VUT).

fitthesis.cls Šablona (definice vzhledu).

Makefile Makefile pro překlad, počítání normostran, sbalení apod. (viz níže).

projekt-01-kapitoly-chapters.tex Soubor pro Váš text (obsah nahradte).

projekt-20-literatura-bibliography.bib Seznam literatury (viz níže).

projekt-30-prilohy-appendices.tex Soubor pro přílohy (obsah nahradte).

projekt.tex Hlavní soubor práce – definice formálních částí.

Styl literatury v šabloně je od Ing. Radka Pyšného [?], jehož práce byla vylepšena prof. Adamem Heroutem, dr. Jaroslavem Dytrychem a panem Karlem Hanákem tak, aby odpovídala normě a podporovala všechny často využívané typy citací. Jeho dokumentaci naleznete v příloze [E](#).

Makefile kromě překladu do PDF nabízí i další funkce:

- přejmenování souborů (viz níže),
- počítání normostran,
- spuštění vlny pro doplnění nezlomitelných mezer,
- sbalení výsledku pro odeslání vedoucímu ke kontrole (zkontrolujte, zda sbalí všechny Vámi přidané soubory, a případně doplňte).

Nezapomeňte, že vlna neřeší všechny nezlomitelné mezery. Vždy je třeba manuální kontrola, zda na konci řádku nezůstalo něco nevhodného – viz Internetová jazyková příručka¹.

Pozor na číslování stránek! Pokud má obsah 2 strany a na 2. jsou jen „Přílohy“ a „Seznam příloh“ (ale žádná příloha tam není), z nějakého důvodu se posune číslování stránek o 1 (obsah „nesedí“). Stejný efekt má, když je na 2. či 3. stránce obsahu jen „Literatura“ a je možné, že tohoto problému lze dosáhnout i jinak. Řešení je několik (od úpravy obsahu, přes nastavení počítadla až po sofistikovanější metody). **Před odevzdáním proto vždy přezkontrolujte číslování stran!**

Doporučený postup práce se šablonou

1. **Zkontrolujte, zda máte aktuální verzi šablony.** Máte-li šablonu z předchozího roku, na stránkách fakulty již může být novější verze šablony s aktualizovanými informacemi, opravenými chybami apod.
2. **Zvolte si jazyk,** ve kterém budete psát svoji technickou zprávu (česky, slovensky nebo anglicky) a svoji volbu konzultujte s vedoucím práce (nebyla-li dohodnuta předem). Pokud Vámi zvoleným jazykem technické zprávy není čeština, nastavte příslušný parametr šablony v souboru `projekt.tex` (např.: `documentclass[english]{fitthesis}`) a přeložte prohlášení a poděkování do angličtiny či slovenštiny.
3. **Přejmenujte soubory.** Po rozbalení je v šabloně soubor `projekt.tex`. Pokud jej přeložíte, vznikne PDF s technickou zprávou pojmenované `projekt.pdf`. Když vedoucímu více studentů pošle `projekt.pdf` ke kontrole, musí je pracně přejmenovávat. Proto je vždy vhodné tento soubor přejmenovat tak, aby obsahoval Váš login a (případně zkrácené) téma práce. Vyhněte se však použití mezer, diakritiky a speciálních znaků. Vhodný název může být např.: „`xlogin00-Cisteni-a-extrakce-textu.tex`“. K přejmenování můžete využít i přiložený Makefile:

```
make rename NAME=xlogin00-Cisteni-a-extrakce-textu
```
4. Vyplňte požadované položky v souboru, který byl původně pojmenován `projekt.tex`, tedy typ, rok (odevzdání), název práce, svoje jméno, ústav (dle zadání), tituly a jméno vedoucího, abstrakt, klíčová slova a další formální náležitosti.
5. Nahraďte obsah souborů s kapitolami práce, literaturou a přílohami obsahem svojí technické zprávy. Jednotlivé přílohy či kapitoly práce může být výhodné uložit do samostatných souborů – rozhodnete-li se pro toto řešení, je doporučeno zachovat konvenci pro názvy souborů, přičemž za číslem bude následovat název kapitoly.

¹Internetová jazyková příručka <http://prirucka.ujc.cas.cz/?id=880>

6. Nepotřebujete-li přílohy, zakomentujte příslušnou část v `projekt.tex` a příslušný soubor vyprázdněte či smažte. Nesnažte se prosím vymyslet nějakou neúčelnou přílohu jen proto, aby daný soubor bylo čím naplnit. Vhodnou přílohou může být obsah přiloženého paměťového média.
7. Smažte soubory s kapitolami a přílohami pro jazyk, který jste nevyužili (s nebo bez `-en`).
8. Zadání, které si stáhnete v PDF z IS FIT (odkaz „Zadání pro vložení do práce“ či „Thesis assignment“), uložte do souboru `zadani.pdf` a povolte jeho vložení do práce parametrem šablony v `projekt.tex` (`documentclass[zadani]{fitthesis}`).
9. Nechcete-li odkazy tisknout barevně (bez konzultace s vedoucím příliš nedoporučuji), budete pro tisk vytvářet druhé PDF s tím, že nastavíte parametr šablony pro tisk: (`documentclass[zadani,print]{fitthesis}`). Budete-li tisknout barevně, místo `print` použijte parametr `cprint`. Barevné logo se nesmí tisknout černobíle!
10. Vzor desek, do kterých bude práce vyvázána, si vygenerujte v informačním systému fakulty u zadání. Pro disertační práci lze zapnout parametrem v šabloně `cover` (více naleznete v souboru `fitthesis.cls`).
11. Nezapomeňte, že zdrojové soubory i (obě verze) PDF musíte odevzdat na CD či jiném médiu přiloženém k technické zprávě.

Obsah práce se generuje standardním příkazem `\tableofcontents` (zahrnut v šabloně). Přílohy jsou v něm uvedeny úmyslně.

Pokyny pro oboustranný tisk

- **Oboustranný tisk je doporučeno konzultovat s vedoucím práce.**
- Je-li práce tištěna oboustranně a její tloušťka je menší než tloušťka desek, nevypadá to dobře.
- Zapíná se parametrem šablony: `\documentclass[twoside]{fitthesis}`
- Po vytištění oboustranného listu zkontrolujte, zda je při prosvícení sazební obrazec na obou stranách na stejné pozici. Méně kvalitní tiskárny s duplexní jednotkou mají často posun o 1–3 mm. Toto může být u některých tiskáren řešitelné tak, že vytisknete nejprve liché stránky, pak je dáte do stejného zásobníku a vytisknete sudé.
- Za titulním listem, obsahem, literaturou, úvodním listem příloh, seznamem příloh a případnými dalšími seznamy je třeba nechat volnou stránku, aby následující část začínala na liché stránce (`\cleardoublepage`).
- Konečný výsledek je nutné pečlivě překontrolovat.

Styl odstavců

Odstavce se zarovnávají do bloku a pro jejich formátování existuje více metod. U papírové literatury je častá metoda s použitím odstavcové zarážky, kdy se u jednotlivých odstavců textu odsazuje první řádek odstavce asi o jeden až dva čtverčíky, tedy přibližně o dvě šířky

velkého písmene M základního textu (vždy o stejnou, předem zvolenou hodnotu). Poslední řádek předchozího odstavce a první řádek následujícího odstavce se v takovém případě neoddělují svislou mezerou. Proklad mezi těmito řádky je stejný jako proklad mezi řádky uvnitř odstavce [?].

Další metodou je odsazení odstavců, které je časté u elektronické sazby textů. První řádek odstavce se při této metodě neodsazuje a mezi odstavce se vkládá vertikální mezera o velikosti 1/2 řádku. Obě metody lze v kvalifikační práci použít, nicméně často je vhodnější druhá z uvedených metod. Metody není vhodné kombinovat.

Jeden z výše uvedených způsobů je v šabloně nastaven jako výchozí, druhý můžete zvolit parametrem šablony „odsaz“.

Užitečné nástroje

Následující seznam není výčtem všech využitelných nástrojů. Máte-li vyzkoušený osvědčený nástroj, neváhejte jej využít. Pokud však nevíte, který nástroj si zvolit, můžete zvážit některý z následujících:

MikTeX L^AT_EX pro Windows – distribuce s jednoduchou instalací a vynikající automatizací stahování balíčků. MikTeX obsahuje i vlastní editor, ale spíše doporučuji TeXstudio.

TeXstudio Přenositelné GUI pro L^AT_EX s otevřeným zdrojovým kódem (opensource). Ctrl+klik umožňuje přepínat mezi zdrojovým textem a PDF. Má integrovanou kontrolu pravopisu², zvýraznění syntaxe apod. Pro jeho využití je nejprve potřeba nainstalovat MikTeX, případně jinou L^AT_EXovou distribuci.

WinEdt Ve Windows je dobrá kombinace WinEdt + MiKTeX. WinEdt je GUI pro Windows, pro jehož využití je nejprve potřeba nainstalovat **MikTeX** či **TeX Live**.

Kile Editor pro desktopové prostředí KDE (Linux). Umožňuje živé zobrazení náhledu. Pro jeho využití je potřeba mít nainstalovaný **TeX Live** a Okular.

JabRef Pěkný a jednoduchý program v Javě pro správu souborů s bibliografií (literaturou). Není potřeba se nic učit – poskytuje jednoduché okno a formulář pro editaci položek.

InkScape Přenositelný opensource editor vektorové grafiky (SVG i PDF). Vynikající nástroj pro tvorbu obrázků do odborného textu. Jeho ovládnutí je obtížnější, ale výsledky stojí za to.

GIT Vynikající pro týmovou spolupráci na projektech, ale může výrazně pomoci i jednomu autorovi. Umožňuje jednoduché verzování, zálohování a přenášení mezi více počítači.

Overleaf Online nástroj pro L^AT_EX. Přímě zobrazuje náhled a umožňuje jednoduchou spolupráci (vedoucí může průběžně sledovat psaní práce), vyhledávání ve zdrojovém textu či ve vygenerovaném PDF, kontrolu pravopisu apod. Zdarma jej však lze využít pouze s určitými omezeními (někomu stačí na disertaci, jiný na ně může narazit i při psaní bakalářské práce) a pro dlouhé texty je pomalejší. FIT VUT v Brně má pro studenty i zaměstnance licenci, kterou si lze aktivovat na <https://www.overleaf.com/edu/but>.

²Českou kontrolu pravopisu lze doinstalovat z <https://extensions.openoffice.org/de/project/czech-dictionary-pack-ceske-slovniky-cs-cz>

Pozn.: Overleaf nepoužívá Makefile v šabloně – aby překlad fungoval, je v menu nutné zvolit `projekt.tex` jako hlavní dokument.

Príloha B

Psaní anglického textu

Tato příloha je převzata ze stránek doc. Černockého [?].

Spousta lidí píše zprávy k projektům anglicky (a to je dobře!), ale dělá v nich spoustu zbytečných chyb (a to je špatně). Nejsem angličtinář, ale tento jazyk už nějakých pár let používám k psaní, čtení i komunikaci – tato příloha obsahuje pár důležitých věcí. Pokud chcete napsat práci nebo článek opravdu 100 % dobře, nezbude Vám než si najmout rodilého mluvčího (a to by měl by být trochu technicky zdatný a aspoň trochu rozumět tomu, co píšete, ať to neskončí ještě hůř ...).

Obecně

- Předtím, než budete sami něco psát, si přečtěte pár anglických technických článků a zkuste si zapamatovat a získat „obecný pocit“, jak se to píše.
- Používejte vždy korektor pravopisu – zabudovaný ve Wordu, nebo v OpenOffice, pokud děláte na Linuxu, tak ISPELL a další (většina editorů pro L^AT_EX má již kontrolu pravopisu integrovanou).
- Používejte korektor gramatiky. Nevím, jestli je nějaký dostupný na Linuxu, ale ten ve Wordu celkem slušně funguje a pokud Vám něco zelené podtrhne, je tam většinou opravdu chyba. Můžete do něj nakopírovat i zdrojový text pro L^AT_EX, opravit, a pak uložit opět jako čistý text. Pokud používáte vim, je tam zabudovaný také a zvládne jak překlepy, tak základní gramatiku. V dokumentu `diplomka.tex` na první řádek napište:

```
% vim:spelllang=en_us:spell
```

(případně `en_gb` pro OED angličtinu) *Poznámka editora:* Existuje i velmi dobrý online nástroj Grammarly¹, který je v základní verzi zdarma.

- Online slovníky jsou dobré, ale nepoužívejte je slepě. Většinou dají více variant a ne každá je správně.

¹<https://www.grammarly.com/>

- Na vyhledávání a zjištění, co bude asi správné, můžete použít Google. Např.: nevíte, jak se řekne „výhoda tohoto přístupu“. Slovník na seznam.cz dá asi 10 variant. Napište je postupně do vyhledávání na googlu:

```
"advantage of this approach" 1100000 hits
"privilege of this approach" 6 hits
"facility of this approach" 16 hits
```

Neříkám, že je to 100 % správně, ale je to určité vodítko. Toto se dá použít i na dohledání správných spojek (třeba „among two cases“ nebo „between two cases“?)

SVOMPT a shoda

Struktura anglické věty je SVOPMT: SUBJECT VERB OBJECT MANNER PLACE TIME a přes to nejede vlak! Není volná jako v češtině. Jinak to je maximálně v nějaké divadelní hře, kde je potřeba něco zdůraznit. Hlavně podmět tam musí vždy být, na to se často zapomíná, protože v CZ/SK může být zamlčený nebo nevyjádřený. SVOMPT platí i ve vedlejších větách!

```
BAD: We have shown that is faster than the other function.
GOOD: We have shown that it is faster than the other function.
```

Shoda podmětu s přísudkem – zní to šíleně, ale dělá se v tom spousta chyb.

```
he has
the users have
people were
```

Členy

Členy v angličtině jsou noční můra a téměř nikdo z nás je nedává dobře. Základní pravidlo je, že když je něco určitého, musí předtím být „the“. Členy musí být určité u těchto spojení:

```
the first, the second, ...
the last
the most (třetí stupeň přídavných jmen a příslovčí) ...
the whole
the following
the figure, the table.
the left, the right - on the left pannel, from the left to the right ...
```

Naopak člen NESMÍ být, pokud používáte přesné označení obrázku, kapitoly atd.

```
in Figure 3.2
in Chapter 7
in Table 6.4
```

Pozor na „a“ vs. „an“, řídí se to podle výslovnosti a ne podle toho, jak je slovo napsané, takže:

```
an HMM
an XML
a universal model
a user
```

Slovesa

Pozor na trpné tvary sloves – u pravidelných je to většinou bez problémů, u nepravidelných často špatně, typicky

```
packet was sent (ne send)
approach was chosen (ne choosed)
```

... většinou to opraví korektor pravopisu, ale někdy ne.

Pozor na časy, občas je v nich pěkný nepořádek. Pokud něco nějak obecně je, přítomný čas. Pokud jste něco udělali, minulý. Pokud to dalo nějaký výsledek a ten výsledek teď existuje a třeba ho nějak diskutujete, přítomný. Nepoužívejte příliš složité časy jako je předpřítomný a vůbec ne předminulý pokud nevíte přesně, co děláte.

```
JFA is a technique that works for everyone in speaker recognition.
We implemented it according to Kenny's recipe in \cite{Kenny}.
12000 segments from NIST SRE 2006 were processed. When compared
with a GMM baseline, the results are completely bad.
```

Délka vět a struktura

- Pište kratší věty a souvětí, pokud máte něco na 5 řádků, většinou se to nedá číst.
- Strukturujte věty pomocí čárek (více než v češtině!), hlavně po úvodu věty, po kterém začíná vlastní věta. Někdy se dává čárka i před „and“ (na rozdíl od češtiny).

```
In this chapter, we will investigate ...
The first technique did not work, the second did not work as well,
and the third one also did not work.
```

Specifika technického textu

Píšete technický text, proto nepoužívejte zkratky

```
he's
gonna
Petr's working on ...
```

a podobně. Jediné, které je tolerované, je „doesn't“, ale neuděláte chybu, když napíšete „does not“.

V technických textech se spíš používá trpný rod než činný:

BAD: In this chapter, I describe used programming languages.

GOOD: In this chapter, used programming languages are described.

Pokud už činný použijete, dává se v technických textech spíše „we“, i když na práci děláte sami. „I“, „my“ atd. se používají pouze tam, kde jde o to zdůraznit, že jde o Vaši osobu, tedy třeba v závěru nebo v popisu „original claims“ v disertaci.

Časté chyby ve slovech

- Pozor na jeho/její, není to it's, ale its.
- Obrázek není picture, ale figure.
- Spojka „než“ je „than“, ne „then“ – bigger than this, smaller than this ... hrozně častá chyba! „Then“ je pak, potom.

Príloha C

Checklist

Tento checklist byl převzat ze šablony pro kvalifikační práce, která je k dispozici na blogu prof. Herouta [?], který s laskavým dovolením využil nápadu dr. Szökeho¹.

Velká bezpečnost letecké dopravy stojí z části na tom, že lidé kolem letadel mají **checklisty** na úplně každý, třeba rutinní a dobře zažitý, postup. Jako pilot strpí to, že bude trochu za blbce a opravdu tužičkou do seznamu úkonů odškrtná dokonale zvládnuté akce, vytiskněte si a odškrtejte před odevzdáním diplomky i vy tento checklist a vyhněte se tak častým chybám, které by mohly mít až fatální následky na výsledné hodnocení Vaší práce.

Struktura

- ☐ Už ze samotných názvů a struktury kapitol je patrné, že bylo splněno zadání.
- ☐ V textu se nevyskytuje kapitola, která by měla méně než čtyři strany (kromě úvodu a závěru). Pokud ano, radil(a) jsem se o tom s vedoucím a ten to schválil.

Obrázky a grafy

- ☐ Všechny obrázky a tabulky byly zkontrolovány a jsou poblíž místa, odkud jsou z textu odkazovány, takže nebude problém je najít.
- ☐ Všechny obrázky a tabulky mají takový popisek, že celý obrázek dává smysl sám o sobě, bez čtení dalšího textu. Vůbec nevadí, když má popisek několik řádků.
- ☐ Pokud je obrázek převzatý, tak je to v popisku zmíněno: „Převzato z [X].“
- ☐ Písmenka ve všech obrázcích používají font podobné velikosti, jako je okolní text (ani výrazně větší, ani výrazně menší).
- ☐ Grafy a schémata jsou vektorově (tj. v PDF).
- ☐ Snímky obrazovky nepoužívají ztrátovou kompresi (jsou v PNG).
- ☐ Všechny obrázky jsou odkázány z textu.
- ☐ Grafy mají popsání osy (název osy, jednotky, hodnoty) a podle potřeby mřížku.

¹<http://blog.igor.szoke.cz/2017/04/predstartovni-priprava-letu-neni.html>

Rovnice

- ☐ Identifikátory a jejich indexy v rovnicích jsou jednopísmenné (kromě nečastých zvláštních případů jako t_{\max}).
- ☐ Rovnice jsou číslovány.
- ☐ Za (nebo vzácně před) rovnicí jsou vysvětleny všechny proměnné a funkce, které zatím vysvětleny nebyly.

Citace

- ☐ **Všechny použité zdroje jsou citovány.**
- ☐ Adresy URL odkazující na služby, projekty, zdroje, github apod. jsou odkazovány pomocí `\footnote{\url{...}}`.
- ☐ Všechny citace používají správné typy.
- ☐ Citace mají autora, název, vydavatele (název konference), rok vydání. Když některá nemá, je to dobře zdůvodněný zvláštní případ a vedoucí to odsouhlasil.
- ☐ Je-li ve zdrojových textech programu něco převzaté, je to tam řádně citováno v souladu s licencí.
- ☐ Je-li podstatná část zdrojových textů programu převzatá, je toto zmíněno v textu práce a je citován zdroj.

Typografie

- ☐ Žádný řádek nepřetéká přes pravý okraj.
- ☐ Na konci řádku nikde není jednopísmenná předložka (spraví to nedělitelná mezera `~`).
- ☐ Číslo obrázku, tabulky, rovnice, citace není nikde první na novém řádku (spraví to nedělitelná mezera `~`).
- ☐ Před číselným odkazem na poznámku pod čarou nikde není mezera (to jest vždy takto², nikoliv takto ³).

Jazyk

- ☐ Použil jsem kontrolu pravopisu a v textu nikde nejsou překlipy.
- ☐ Nechal jsem si text přečíst od (alespoň) jednoho dalšího člověka, který umí dobře česky / anglicky / slovensky.
- ☐ V práci psané česky nebo slovensky abstrakt zkontroloval někdo, kdo umí opravdu dobře anglicky.
- ☐ V textu se nikde nepoužívá druhá mluvnická osoba (vy/ty).

²příklad poznámky pod čarou

³jiný příklad poznámky pod čarou

- ☐ Když se v textu vyskytuje první mluvnická osoba (já, my), vždy se popisuje subjektivní záležitost (*rozhodl jsem se, navrhl jsem, zaměřil jsem se na, zjistil jsem* apod.).
- ☐ V textu se nikde nepoužívají hovorové výrazy.
- ☐ V českém či slovenském textu se zbytečně nepoužívají anglické výrazy, které mají ustálené české překlady. Např. slovo *defaultní* se nahradí např. slovem *implicitní* nebo *výchozí*.

Výsledek na datovém médiu, tj. software

- ☐ Mám připravené nepřepisovatelné datové médium
 - CD-R,
 - DVD-R,
 - DVD+R ve formátu ISO9660 (s rozšířením RockRidge a/nebo Joliet) nebo UDF,
 - paměťová karta SD (Secure Digital) ve formátu FAT32 nebo exFAT s nastavenou ochranou proti přepisu.
- ☐ Pokud je výsledek online (služba, aplikace, ...), URL je viditelně v úvodu a závěru, aby bylo jasné, kde výsledek hledat.
- ☐ Na médiu nechybí povinné:
 - zdrojové kódy (např. Matlab, C/C++, Python, ...)
 - knihovny potřebné pro překlad,
 - přeložené řešení,
 - PDF s technickou zprávou (je-li pro tisk 2. verze, tak obě),
 - zdrojový kód zprávy (L^AT_EX),

a případně volitelně po dohodě s vedoucím práce

- relevantní (např. testovací) data,
 - demonstrační video,
 - PDF plakátku,
 - ...
- ☐ Zdrojové kódy jsou refaktorovány, komentovány a označeny hlavičkou s autorstvím, takže se v nich snadno vyzná i někdo další, než sám autor.
- ☐ Jakákoliv převzatá část zdrojového kódu je řádně citována – tedy označena úvodním a v případě převzetí více řádků i ukončovacím komentářem. Komentář obsahuje vše, co vyžaduje licence uvedená na webu (vždy je nutné se ji pokusit najít – např. Stack Overflow⁴ má striktní pravidla pro citace).

⁴<https://stackoverflow.blog/2009/06/25/attribution-required/>

Odevzdání

- ☐ Chci práci (na max. 3 roky) utajit? Pokud ano, nejpozději měsíc před termínem odevzdání práce si podám žádost (v IS), ke které přiložím případné stanovisko firmy, jejíž duševní vlastnictví je třeba chránit.
- ☐ Mám splněný minimální počet normostran textu (lze spočítat pomocí Makefile a odhadem přičíst obrázky). Pokud jsem těsně pod minimem, konzultoval(a) jsem to s vedoucím.
- ☐ Pokud chci tisknout oboustranně, konzultoval(a) jsem to s vedoucím a mám správně nastavenou šablonu. Kapitoly začínají na liché stránce.
- ☐ Technickou zprávu mám v deskách z knihařství (min. 1 výtisk, při utajení oba).
- ☐ Za titulním listem práce je zadání (tzn. mám jej stažené z IS a vložené do šablony).
- ☐ V IS jsou abstrakty a klíčová slova.
 - V abstraktu a klíčových slovech v IS nejsou zkopírované vlnky pro nezlomitelné mezery.
- ☐ V IS je PDF práce (s klikatelnými odkazy).
- ☐ Oba výtisky práce jsou podepsané.
- ☐ V jednom (při utajení obou) výtisku práce je paměťové médium, na kterém je fixkou napsaný login (fixku na CD lze zapůjčit v knihovně, na Studijním oddělení nebo až při odevzdání).

Príloha D

L^AT_EX pro začátečníky

V této kapitole jsou uvedeny některé často využívané balíčky a příkazy pro L^AT_EX, které mohou být při tvorbě práce potřeba.

Užitečné balíčky

Studenti při sazbě textu často řeší stejné problémy. Některé z nich lze vyřešit následujícími balíčky pro L^AT_EX:

- `amsmath` – rozšířené možnosti sazby rovnic,
- `float`, `afterpage`, `placeins` – úprava umístění obrázků/tabulek (specifikátor H),
- `fancyvrb`, `alltt` – úpravy vlastností prostředí Verbatim,
- `makecell` – rozšíření možností tabulek,
- `pdflscape`, `rotating` – natočení stránky o 90 stupňů (pro obrázek či tabulku),
- `hyphenat` – úpravy dělení slov,
- `picture`, `epic`, `eepic` – přímé kreslení obrázků.

Některé balíčky jsou využity přímo v šabloně (v dolní části souboru `fitthesis.cls`). Nahlédnutí do jejich dokumentace může být rovněž velmi užitečné.

Sloupec tabulky zarovnaný vlevo s pevnou šířkou je v šabloně definovaný „L“ (používá se jako „p“).

Pro odkazování v rámci textu použijte příkaz `\ref{navesti}`. Podle umístění návěští se bude jednat o číslo kapitoly, podkapitoly, obrázku, tabulky nebo podobného číslovaného prvku). Pokud chcete odkázat stránku práce, použijte příkaz `pageref{navesti}`. Pro citaci literárního odkazu `\cite{identifikator}`. Pro odkazy na rovnice lze použít příkaz `\eqref{navesti}`.

Znak – (pomlčka) se V L^AT_EXu vkládá jako dvě mínus za sebou: --.

Často využívané příkazy pro L^AT_EX

Doporučuji nahlédnout do zdrojového textu této podkapitoly a podívat se, jak jsou následující ukázky vysázeny. Ve zdrojovém textu jsou i pomocné komentáře.

Příklad tabulky:

Tabulka D.1: Tabulka hodnocení

Jméno		
Jméno	Příjmení	Hodnocení
Jan	Novák	7.5
Petr	Novák	2

Příklad rovnice:

$$\cos^3 \theta = \frac{1}{4} \cos \theta + \frac{3}{4} \cos 3\theta \quad (\text{D.1})$$

a dvou horizontálně zarovnaných rovnic:

$$3x = 6y + 12 \quad (\text{D.2})$$

$$x = 2y + 4 \quad (\text{D.3})$$

Pokud je třeba rovnici citovat v textu, lze použít příkaz `\eqref`. Například na rovnici výše lze odkázat (D.1). Pokud chcete srovnat číslo rovnic u soustavy, lze použít prostředí `split`:

$$\begin{aligned} 3x &= 6y + 12 \\ x &= 2y + 4 \end{aligned} \quad (\text{D.4})$$

Matematické symboly (α) a výrazy lze umístit i do textu $\cos \pi = -1$ a mohou být i v poznámce pod čarou¹.

Obrázek D.1 ukazuje široký obrázek složený z více menších obrázků. Klasický rastrový obrázek se vkládá tak, jak je vidět na obrázku D.2.



Obr. D.1: **Široký obrázek.** Obrázek může být složen z více menších obrázků. Chcete-li se na tyto dílčí obrázky odkazovat z textu, využijte balíček `subcaption`.

Někdy je potřeba do příloh umístit diagram, který se nevejde na stránku formátu A4. Pak je možné vložit jednu stránku formátu A3 a do práce ji poskládat (tzv. skládání do Z,

¹Vzorec v poznámce pod čarou: $\cos \pi = -1$



Obr. D.2: Dobrý text je špatným textem, který byl několikrát přepsán. Nebojte se prostě něčím začít.

kdy se vytvoří dva sklady – lícem dolů a lícem nahoru, angl. Engineering fold – existuje i anglický pojem Z-fold, ale při tom by byl problém s vazbou). Přepnutí se provádí následovně: `\eject \pdfpagewidth=420mm` (pro přepnutí zpět pak 210mm).

Další často využívané příkazy naleznete ve zdrojovém textu ukázkového obsahu této šablony.

Príloha E

Příklady bibliografických citací

Styl czplain vychází ze stylu vytvořeného v rámci práce pana Pyšného [?]. Obsahuje sadu podporovaných typů citací s konkrétními příklady bibliografických citací.

Na následujících stránkách přílohy jsou uvedeny příklady, jenž znázorňují bibliografické citace následujících publikací a jejich částí:

- článku v seriálové publikaci (časopisu) (str. 29),
- monografické publikace (str. 30),
- sborníku (str. 31),
- článku ve sborníku nebo kapitoly v knize (str. 32),
- manuálu, dokumentace, technické zprávy a nepublikovaných materiálů (str. 33),
- akademické práce (str. 34),
- webové stránky (str. 35),
- a webové domény (str. 36).

Položky jsou označeny barevně podle povinnosti:

- prvek je dle normy povinný
- prvek, který je dle normy volitelný
- prvek, který je dle normy povinný pro online informační zdroje
- prvek, který není předepsán normou a je v bibliografickém stylu v šabloně volitelný

Povinné položky se uvádí pouze pokud existují.

V souboru s bibliografií se záznamy uvádí následujícím způsobem:

```
@Article{Doe:2020,  
  author          = "Doe, John",  
  title           = "Jak citovat",  
  subtitle        = "Citace článku",  
  journal         = "Seriál o tvorbě prací",  
  journalsubtitle = "Formální náležitosti",  
  howpublished    = "online",  
  address         = "Brno",  
  publisher       = "Fakulta informačních technologií VUT v Brně",  
  contributory    = "Přeložil Jan NOVÁK",  
  edition         = "1",  
  version         = "verze 1.0",  
  month          = 2,  
  year            = "2020",  
  revised         = "revidováno 12. 2. 2020",  
  volume          = "4",  
  number         = "24",  
  pages           = "8--21",  
  cited           = "2020-02-12",  
  doi             = "10.1000/BC1.0",  
  issn            = "1234-5678",  
  note            = "Toto je zcela vymyšlená citace",  
  url             = "https://merlin.fit.vutbr.cz"  
}
```

Citace jsou seřazeny podle abecedy. Řazení jmen s písmeny s diakritikou můžeme ovlivnit prvkem **key**, jehož hodnotu nastavíme na příjmení bez diakritiky. Pokud není vyplněn autor, citace se řadí na začátek seznamu, což není vhodné. Řazení v tomto případě můžeme taktéž ovlivnit vhodně nastaveným prvkem **key**.

Příklad:

```
@Article{Cech:2020:Citace,  
  author          = "Čech, Jan",  
  key             = "Cech",  
  ...
```

Článek v seriálové publikaci - @Article

Položky záznamu

Prvek	Zápis v BibTeXu	Příklad
Tvůrce	author	Doe, John
Název příspěvku	title	Jak citovat
Vedlejší název	subtitle	Citace článku
Název seriálové publikace	journal	Seriál o tvorbě prací
Vedlejší názvy seriálu	journalsubtitle	Formální náležitosti
Typ nosiče	howpublished	online
Vydání	edition	1
Verze	version	verze 1.0
Další tvůrce	contributory	Přeložil Jan NOVÁK
Místo vydání	address	Brno
Nakladatel	publisher	Fakulta informačních tech- nologii VUT v Brně
Měsíc	month	2
Rok	year	2020
Svazek	volume	4
Číslo	number	24
Rozsah příspěvku	pages	8-21
Revize	revised	revidováno 12. 2. 2020
Datum citování	cited	2020-02-12
Název edice	series	Návody k tvorbě prací
Číslo edice	editionnumber	42
Identifikátor digitálního ob- sahu	doi	10.1000/BC1.0
Standardní číslo	issn	1234-5678
Poznámky	note	Toto je zcela vymyšlená ci- tace
Dostupnost a přístup	url	https://merlin.fit.vutbr.cz

Bibliografická citace

DOE, J. Jak Citovat: Citace článku. *Seriál o tvorbě prací: Formální náležitosti* [online]. 1. vyd., verze 1.0. Přeložil Jan NOVÁK. Brno: Fakulta informačních technologií VUT v Brně. Únor 2020, sv. 4, č. 24, s. 8–21, revidováno 12. 2. 2020, [cit. 2020-02-12]. Návody k tvorbě prací, č. 42. DOI: 10.1000/BC1.0. ISSN 1234-5678. Toto je zcela vymyšlená citace. Dostupné z: <https://merlin.fit.vutbr.cz>

Monografická publikace - @Book, @Booklet (kniha, brožura)

Položky záznamu

Prvek	Zápis v BibTeXu	Příklad
Tvůrce	author	John von Doe
Titul	title	Jak citovat
Vedlejší názvy	subtitle	Citace monografické publi- kace
Typ nosiče	howpublished	online
Vydání	edition	1
Další tvůrce	contributory	Přeložil Jan NOVÁK
Místo vydání	address	Brno
Nakladatel	publisher	Fakulta informačních tech- nologí VUT v Brně
Měsíc vydání	month	2
Rok vydání	year	2020
Revize	revision	revidováno 12. 2. 2020
Datum citování	cited	2020-02-12
Rozsah	pages	220
Edice	series	Návody k tvorbě prací
Číslo edice	editionnumber	2
Standardní číslo	isbn	01-234-5678-9
Poznámky	note	Toto je zcela vymyšlená ci- tace
Dostupnost a přístup	url	https://merlin.fit.vutbr.cz

Bibliografická citace

VON DOE, J. *Jak citovat: Citace monografické publikace* [online] . 1. vyd. Přeložil Jan NOVÁK. Brno:Fakulta informačních technologií VUT v Brně, únor 2020, revidováno 12. 2. 2020 [cit. 2020-02-12]. 220 s. Návody k tvorbě prací, č. 2. ISBN 01-234-5678-9. Toto je zcela vymyšlená citace. Dostupné z: <https://merlin.fit.vutbr.cz>

Sborník - @Proceedings

Položky záznamu

Prvek	Zápis v BibTeXu	Příklad
Tvůrce*	author	Čechmánek, Jan
Editor*	editor	Čechmánek, Jan
Titul	title	Jak citovat
Vedlejší názvy	subtitle	Citace monografické publi- kace
Typ nosiče	howpublished	online
Vydání	edition	1
Další tvůrce	contributory	Přeložil Jan NOVÁK
Místo vydání	address	Brno
Nakladatel	publisher	Fakulta informačních tech- nologii VUT v Brně
Měsíc vydání	month	2
Rok vydání	year	2020
Svazek	volume	4
Číslo svazku	number	24
Rozsah příspěvku	pages	8-21
Revize	revised	revidováno 12. 2. 2020
Datum citování	cited	2020-02-12
Edice	series	Návody k tvorbě prací
Číslo edice	editionnumber	2
Identifikátor digitálního ob- jektu	doi	10.1000/BC1.0
Standardní číslo	isbn nebo issn	01-234-5678-9
Poznámky	note	Toto je zcela vymyšlná ci- tace
Dostupnost a přístup	url	https://merlin.fit.vutbr.cz

*Uvádí se buď autor, nebo editor.

Bibliografická citace

ČECHMÁNEK, J. *Jak citovat: Citace sborníku* [online]. 1. vyd. Přeložil Jan NOVÁK. Brno: Fakulta informačních technologií VUT v Brně, únor 2020, sv. 4, č. 24, s. 8–21, revidováno 12. 2. 2020 [cit. 2020-02-12]. Návody k tvorbě prací, č. 2. DOI: 10.1000/BC1.0. ISBN 01-234-5678-9. Toto je zcela vymyšlená citace. Dostupné z: <https://merlin.fit.vutbr.cz>

Článek ve sborníku nebo kapitola v knize - @InProceedings, @InCollection, @Conference, @InBook

Položky záznamu

Prvek	Zápis v BibTeXu	Příklad
Tvůrce	author	John von Doe
Název příspěvku	title	Jak citovat
Vedlejší názvy	subtitle	Citace článku
Jméno tvůrce mateřského dokumentu	editor nebo organisation	Smith, Peter
Název mateřského dokumentu	booktitle	Sborník konference o tvorbě prací
Vedlejší názvy mateřského dokumentu	booksubtitle	Formální náležitosti
Typ nosiče	howpublished	online
Vydání	edition	1
Verze	version	verze 1.0
Další původce mateřského dokumentu	contributory	Přeložil Jan NOVÁK
Místo vydání	address	Brno
Nakladatel	publisher	Fakulta informačních technologií VUT v Brně
Měsíc	month	2
Rok	year	2020
Svazek	volume	4
Číslo svazku	number	24
Kapitola	chapter	5
Rozsah příspěvku	pages	8-21
Revize	revised	revidováno 12. 2. 2020
Datum citování	cited	2020-02-12
Edice	series	Návody k tvorbě prací
Číslo edice	editionnumber	2
Standardní číslo	isbn nebo issn	1234-5678
Poznámky	note	Toto je zcela vymyšlená citace
Dostupnost a přístup	url	https://merlin.fit.vutbr.cz

Bibliografická citace

DOE, J. Jak citovat: Citace článku. In: SMITH, P., ed. *Sborník konference o tvorbě prací: Formální náležitosti* [online]. 1. vyd., verze 1.0. Přeložil Jan NOVÁK. Brno: Fakulta informačních technologií VUT v Brně, únor 2020, sv. 4, č. 24, kap. 5, s. 8–21, revidováno 12. 2. 2020 [cit. 2020-02-12]. Návody k tvorbě prací, č. 2. ISSN 1234-5678. Toto je zcela vymyšlená citace. Dostupné z: <https://merlin.fit.vutbr.cz>

Manuál, dokumentace, technická zpráva a nepublikované materiály - @Manual, @TechReport, @Unpublished

Položky záznamu

Prvek	Zápis v BibTeXu	Příklad
Tvůrce (osoba nebo organizace)	author	Fakulta informačních technologií VUT v Brně
Titul	title	Manuál k tvorbě prací
Vedlejší názvy	subtitle	Citace manuálu
Typ nosiče	howpublished	online
Typ dokumentu	type	Uživatelský manuál
Číslo dokumentu	number	3
Vydání	edition	1
Další tvůrce	contributory	Editoval Jan NOVÁK
Místo vydání	address	Brno
Organizace nebo instituce	organization nebo institution	Fakulta informačních technologií VUT v Brně
Měsíc vydání	month	2
Rok vydání	year	2020
Revize	revised	revidováno 12. 2. 2020
Datum citování	cited	2020-02-12
Rozsah	pages	220
Poznámky	note	Toto je zcela vymyšlená citace
Dostupnost a přístup	url	https://merlin.fit.vutbr.cz

Bibliografická citace

FAKULTA INFORMAČNÍCH TECHNOLOGIÍ VUT V BRNĚ. *Manuál k tvorbě prací: Citace manuálu* [online]. Uživatelský manuál 3, 1. vyd. Editoval Jan NOVÁK. Brno: Fakulta informačních technologií VUT v Brně, únor 2020, revidováno 12. 2. 2020 [cit. 2020-02-12]. 220 s. Toto je zcela vymyšlená citace. Dostupné z: <https://merlin.fit.vutbr.cz>

Akademická práce - @BachelorsThesis, @MastersThesis, @PhdThesis, @Thesis

Položky záznamu

Prvek	Zápis v BibTeXu	Příklad
Tvůrce	author	Fakulta informačních technologií VUT v Brně
Titul	title	BiBTeX styl pro ČSN ISO 690 a ČSN ISO 690-2
Vedlejší názvy	subtitle	
Typ nosiče	howpublished	online
Typ dokumentu	type	Diplomová práce
Místo vydání	address nebo location	Brno
Škola	school	Vysoké učení technické v Brně, Fakulta informačních technologií
Rok vydání	year	2020
Datum citování	cited	2020-02-12
Rozsah	pages	220
Rozsah příloh	inserts	20
Standardní číslo	isbn	01-234-5678-9
Vedoucí práce	Supervisor	Dytrych, Jaroslav
Poznámky	note	Toto je zcela vymyšlená citace
Dostupnost a přístup	url	https://www.fit.vut.cz/study/theses

Bibliografická citace

NOVÁK, J. *BiBTeX styl pro ČSN ISO 690 a ČSN ISO 690-2* [online]. Brno, CZ, 2020. [cit. 2020-02-12]. 80 s., 20. s. příl. Diplomová práce. Vysoké učení technické v Brně, Fakulta informačních technologií. ISBN 01-2345-678-9. Vedoucí práce DYTRYCH, J. Toto je zcela vymyšlená citace. Dostupné z: <https://www.fit.vut.cz/study/theses>

Webová stránka - @Webpage

Položky záznamu

Prvek	Zápis v BibTeXu	Příklad
Tvůrce	author	Nováková, Jana
Název příspěvku	secondarytitle	Citace příspěvku
Název stránky	title	Web tvorby prací
Vedlejší název stránky	subtitle	
Typ nosiče	howpublished	online
Další tvůrce	contributory	Editoval Jan NOVÁK
Verze	version	Verze 1.0
Místo vydání	address	Brno
Vydavatel	publisher	Fakulta informačních technologií VUT v Brně
Den	day	12
Měsíc vydání	month	2
Rok vydání	year	2020
Čas publikování	time	14:00
Revize	revised	Revidováno 12. 2. 2020
Identifikátor digitálního objektu	doi	10.1000/BC1.0
Standardní číslo	issn	1234-5678
Poznámky	note	Toto je zcela vymyšlená citace
Dostupnost a přístup	url	https://merlin.fit.vutbr.cz
Cesta	path	Domů; Umění; Umění citace

Bibliografická citace

NOVÁKOVÁ, J. Citace příspěvku. *Web tvorby prací* [online]. Editoval Jan NOVÁK. Verze 1.0. Brno: Fakulta informačních technologií VUT v Brně, 2. března 1998 14:10. Revidováno 12. 2. 2020 [cit. 2020-02-12]. DOI: 10.1000/BC1.0. ISSN 1234-5678. Toto je zcela vymyšlená citace. Dostupné z: <https://merlin.fit.vutbr.cz> Path: Domů; Umění; Umění citace.

Webová doména - @Website

Položky záznamu

Prvek	Zápis v BibTeXu	Příklad
Tvůrce (osoba nebo organizace)	author	Nováková, Jana
Název webu	title	Web tvorby prací
Vedlejší název webu	subtitle	
Typ nosiče	howpublished	online
Další tvůrce	contributory	Editoval Jan NOVÁK
Verze	version	Verze 1.0
Místo vydání	address	Brno
Vydavatel	publisher	Fakulta informačních technologií VUT v Brně
Den	day	12
Měsíc vydání	month	2
Rok vydání	year	2020
Čas publikování	time	14:00
Revize	revised	Revidováno 12. 2. 2020
Datum	citování	cited 2020-02-12
Identifikátor digitálního objektu	doi	10.1000/BC1.0
Standardní číslo	issn	1234-5678
Poznámky	note	Toto je zcela vymyšlená citace
Dostupnost a přístup	url	https://merlin.fit.vutbr.cz

Bibliografická citace

NOVÁKOVÁ, J. *Web tvorby prací* [online]. Editoval Jan NOVÁK. Verze 1.0. Brno: Fakulta informačních technologií VUT v Brně, 2. března 1998 14:10. Revidováno 12. 2. 2020 [cit. 2020-02-12]. DOI: 10.1000/BC1.0. ISSN 1234-5678. Toto je zcela vymyšlená citace. Dostupné z: <https://merlin.fit.vutbr.cz>.