

JAK NA INTERNET

Vývoj a architektura počítače

Analytický stroj

Mnohé z principů, na nichž stojí koncepce moderního počítače, pocházejí překvapivě už z první poloviny 19. století. Kolem roku 1835 představil anglický matematik a vynálezce Charles Babbage svůj návrh mechanického *Analytického stroje* (angl. *Analytical Engine*), který měl být naplněním jeho myšlenky „výpočtů poháněných parou“. Navržený stroj již měl oddělený procesor, jemuž Babbage říkal „mlýn“, paměť i vstupní a výstupní zařízení (děrné štítky a tiskárnu).

Babbageova mladá spolupracovnice Augusta Ada King, jinak též dcera básníka Lorda Byrona a později hraběnka z Lovelace, připojila k popisu *Analytického stroje* své poznámky a vize, za něž by se nemusel stydět ani Jules Verne. Předpověděla třeba využití počítače pro nenumernické úlohy, například zpracování textu nebo hudby.

Babbageovi se ovšem nikdy nepodařilo *Analytický stroj* zkonstruovat, pokouší se o to až nyní skupina nadšenců v projektu *plan28.org*.

První opravdové počítače

Skutečně fungující počítače se začaly objevovat během druhé světové války. Ačkoliv se historici stále prou o to, kdo byl vlastně úplně první, je zcela namístě jmenovat tři výpočetní stroje, které vznikly nezávisle na sobě zhruba ve stejné době:

- V květnu roku 1941 byl v Německu uveden do provozu počítač *Z3*, jehož autorem byl Konrad Zuse.
- *ABC (Atanasoff-Berry Computer)* zkonstruovali a otestovali John V. Atanasoff a Clifford Berry na Iowa State College v roce 1942.
- V letech 1943–46 vznikl na Moore School of Electrical Engineering ve Philadelphii elektronkový počítač *ENIAC*. Vývojový tým vedli John Mauchly a J. Presper Eckert.

Z dnešního pohledu měl největší význam posledně jmenovaný *ENIAC*, především proto, že na jeho základě vybudoval John von Neumann, geniální matematik maďarského původu, architekturu počítače, která se používá dodnes. Její hlavní a vpravdě revoluční myšlenkou bylo využití paměti jak pro data, tak i pro zakódované programové instrukce, které procesor z paměti načítá a provádí. Nenápadná výzkumná zpráva von Neumannovy skupiny, ač původně vznikla jen ve strojopisné podobě ve 24 kopiích, se rychle rozletěla do celého světa a John von Neumann je od té doby považován za otce moderního počítače. Otázkou zůstává, zda právem, protože některé z jeho myšlenek si nechal patentovat už Konrad Zuse v roce 1937.

Co bude dál?

Během sedmdesáti let vývoje počítačů se všechny jejich podstatné parametry vylepšovaly exponenciálním tempem. Podle známého *Moorova zákona*, zformulovaného v roce 1965 pozdějším spoluzakladatelem společnosti *Intel*, se počet tranzistorů v integrovaných obvodech každé dva roky zdvojnásobuje. Některé jiné parametry rostly dokonce ještě rychleji. V posledních letech se však



JAK NA INTERNET

růst hustoty čipů výrazně zpomalil – narážíme už totiž na nepřekročitelné fyzikální limity. Nový průlom mají přinést až kvantové počítače.

Podstata kvantových výpočtů vypadá jako sci-fi, ale ve světě elementárních částic a fotonů nemůžeme aplikovat přirozenou intuici, kterou jsme nabyli v makrosvětě. Kvantová mechanika totiž u systémů, které nemůžeme pozorovat ani s nimi jinak interagovat, předpokládá velmi podivné „chování“, jemuž se říká princip superpozice. Nejen, že nevíme, v jakém stavu se takový systém aktuálně nachází, on se dokonce nachází zároveň ve všech možných stavech! Na tom je založen kvantový paralelismus: místo obvyklých bitů používá kvantový počítač qubity, s nimiž se jakoby zároveň provádějí dva výpočty, jeden s hodnotou nula a druhý s hodnotou jedna. Kdybychom měli takových qubitů stovky, můžeme najednou realizovat závratné množství výpočtů.

To, co ještě před pětadvaceti lety vypadalo jako kuriózní teoretická možnost bez praktického uplatnění, získalo na zajímavosti poté, co byly v polovině devadesátých let zveřejněny dva kvantové algoritmy, které by mohly odeslat celou současnou kryptografii do starého železa. Od té doby začala na kvantových počítačích intenzivně pracovat řada týmů na celém světě. Dnes již existuje hned několik různých technických podob qubitů založených na vlastnostech elektronů, fotonů anebo iontů. Celá věc má ale ještě mnoho háčeků a podle mínění odborníků jsme od použitelných kvantových počítačů vzdáleni desítky let.

