Adaptovatelné podpisy v kryptografii představují rozšíření standardních digitálních podpisů. Umožňují podepisujícímu vytvořit závazek k podpisu, který lze následně získat výměnou za tajnou hodnotu. Tato vlastnost adaptovatelných podpisů se v poslední době využívá v mnoha aplikacích souvisejících s kryptoměnami včetně podmíněných plateb. Naše práce se zabývá bezpečností adaptovatelných podpisových schémat pro Schnorrovy podpisy a ECDSA, motivovanou právě scénářem podmíněných plateb. Identifikujeme omezení stávajících definic bezpečnosti, pokud je uvažujeme vzhledem k praktickým adaptovatelným podpisům pro ECDSA, a představíme i konkrétní problém v kontextu Bitcoinu. Navrhneme nové definice bezpečnosti, které předcházejí těmto problémům, a dokážeme, že praktický adaptovatelný podpis pro ECDSA splňuje námi definovanou bezpečnost.