本书所用技术术语表

Dr Alexander Ressos, TEP
Attorney-at-Law (Switzerland and Germany),
Solicitor (England & Wales and Hong Kong)
Of Counsel, KGP Legal LLC
alexander.ressos@kgplegal.com.sg
www.ressos.com.sg

以下词条按字母顺序，依本书使用的含义对全书所用技术术语作出定义。如某一术语在瑞士法或新加坡法中有法定定义，词条会予以说明并注明出处。如技术人员与法律人士对某一术语的用法不同，词条采用本书所采纳的法律用法。对其他词条的交叉引用以斜体标出。

账户模型（Account model）——一种账本设计，每个地址都带有随交易增减的余额，以太坊即采用此种设计，与比特币所采用的*UTXO*模型相对。这一区别影响法院如何追踪资金，以及托管人如何归属混合存放的客户资产。

地址（Address）——由公钥派生的字符串，用于标识账本上代币的接收目的地。任何人都可以免费创建地址，地址不带有任何姓名。一旦地址能够与某一自然人关联，即构成瑞士和新加坡数据保护法意义上的个人数据。

空投（Airdrop）——无偿向现有地址分发代币，通常用于奖励早期用户或使持有更加分散。空投会产生税务后果：视接收人属于交易者还是私人投资者，空投可能被视为收入，也可能被视为零成本取得。

© 2026 Dr Alexander Ressos. General information only, not legal, tax or investment advice. No client relationship is created. All Singapore law advice is provided by a duly licensed and regulated firm of Singapore advocates and solicitors only on the basis of an express written letter of engagement. More information at SingaporeIQ.com and ressos.com.sg.

算法稳定币（Algorithmic stablecoin）——一种试图在没有足额抵押的情况下，通过调整供应量保持稳定价值的代币。在2022年5月崩盘之前，Terraform的UST是其主要代表。瑞士金融市场监督管理局和MAS均不将此类代币视为监管意义上的稳定币。

AMLA——《瑞士反洗钱法》（Geldwäschereigesetz，GwG），SR 955.0。该法适用于金融中介，FINMA将其解释为涵盖大多数对客户加密资产拥有处分权的服务提供者。[1]

资产参考代币（Asset-referenced token，ART）——MiCA依据第(EU) 2023/1114号条例第3条第1款第6项设立的类别，指通过参考任何价值或权利或其组合（包括多种货币）来保持稳定价值的加密资产。它与单一货币的电子货币代币相对应。

资产型代币（Asset token）——FINMA依据2018年2月16日《ICO指引》第3.1节设立的类别，指代表债权或股权、未来收益份额或资产权利的代币。在瑞士法下，此类代币几乎在所有情况下都属于证券，并会引发招股说明书和牌照方面的后果。

自动做市商（Automated market maker，AMM）——一种去中心化交易所，Uniswap是其主要代表。它依据公式、以汇集的流动性为对手方为交易定价，而不撮合买卖订单。按照第VI章的分析，AMM交易的对手方是资金池的全体流动性提供者。

区块（Block）——作为一个单元添加到账本中的一批交易，带有前一区块的哈希值，从而使各区块形成一条链，任何人都能发现对其的篡改。

区块浏览器（Block explorer）——以可读形式显示公共账本内容的网站，例如Etherscan或mempool.space。律师在对某笔交易发表任何意见之前，应当能够在区块浏览器上读懂该交易。

© 2026 Dr Alexander Ressos. General information only, not legal, tax or investment advice. No client relationship is created. All Singapore law advice is provided by a duly licensed and regulated firm of Singapore advocates and solicitors only on the basis of an express written letter of engagement. More information at SingaporeIQ.com and ressos.com.sg.

跨链桥（Bridge）——一种将某一账本上的代币在另一账本上加以表示的机制，通常是将原代币锁定在合约中，并在目标链上铸造封装代币。该行业历史上最大规模的盗窃事件都发生在跨链桥上。

销毁（Burn）——将代币发送至无法动用的地址，或调用减少供应量的合约函数，从而不可逆转地销毁代币。销毁用于赎回*LP*代币，以及在赎回时注销稳定币。

资本市场产品（Capital markets product）——新加坡《2001年证券与期货法》第2(1)条规定的法定类别，涵盖证券、集体投资计划单位、衍生品合约和某些外汇合约。属于资本市场产品的代币受SFA监管，无论其是否同时属于*DPT*。

CBDC——央行数字货币，即以代币形式存在的中央银行负债。其中批发型仅限于金融机构使用，零售型则面向公众。瑞士和新加坡都已在试点中发行批发型CBDC，两国均无推出零售型的计划。

链（Chain）——对分布式账本的通俗称呼，源于区块的链接。因此，“链上”指记录在账本上，“链下”指记录在别处，例如托管人的内部账簿。

冷钱包（Cold wallet）——其私钥保存在从不连接互联网的设备上的钱包，签名需要人工步骤，因而不可能远程盗取密钥。它与热钱包相对应。

集体投资计划（Collective investment scheme）——在瑞士法下，指向投资者募集、用于集体投资并由第三方为其账户管理的资产（《集体投资计划法》（CISA）第7条）。在新加坡法下，指参与者对作为整体管理的汇集财产缺乏日常控制的安排（SFA第2(1)条）。若干DeFi结构同时符合这两个定义。

担保有限公司（Company limited by guarantee，CLG）——依《1967年公司法》第17条设立的无股本新加坡公司，其成员承诺在公司清盘时出资一笔象征性款项。它被用作协议的法律包装，常被称为“基金会”，但它并不是基金会。

© 2026 Dr Alexander Ressos. General information only, not legal, tax or investment advice. No client relationship is created. All Singapore law advice is provided by a duly licensed and regulated firm of Singapore advocates and solicitors only on the basis of an express written letter of engagement. More information at SingaporeIQ.com and ressos.com.sg.

确认（Confirmation）——交易被纳入某一区块，以及其后每一个在其基础上构建的区块。因此，要求六次确认的交易所会再等待五个区块后才将存款入账。之所以需要等待，是因为公共账本上的最终性是概率性的。

共识（Consensus）——账本参与者在互不信任的情况下就下一个区块达成一致的协议，工作量证明和权益证明是其两大主要类型。

加密资产（Crypto asset）——本书对记录在分布式账本上的任何代币所使用的总称，对应于DEBA第242a条和BankA第16条中的瑞士法定术语"基于加密的资产"（kryptobasierter Vermögenswert）。

托管人（Custodian）——持有控制客户代币的私钥的人。在新加坡，这是《支付服务法》下需取得牌照的支付服务。在瑞士，这使持有人成为AMLA下的金融中介；如果其有权使用这些资产，还可能构成银行。

DAO——去中心化自治组织，即通过智能合约、以代币加权投票方式治理某一协议或资金库的群体。没有法律包装的DAO，在瑞士法下属于简单合伙，在新加坡法下属于合伙或非法人社团。

去中心化金融（Decentralised finance，DeFi）——由公共账本上的智能合约提供、无需中介持有客户资产的金融服务。联邦委员会2022年12月16日的报告是瑞士在这方面的参考文本。

委托质押（Delegated staking）——持有人保留提取密钥、仅将验证权委托给运营者的质押，与托管人持有全部密钥的托管式质押相对。

派生路径（Derivation path）——依据BIP-32标准由种子生成各个密钥对的序列，因此一个种子可通过不同路径控制多条链上的地址。因此，盘点持有资产时必须扫描所有常用路径。

数字支付代币（Digital payment token，DPT）——新加坡《2019年支付服务法》第2(1)条中的法定术语，指以数字形式表示价值、不以任何货币计价、用作交换媒介并可电子转让的代币。比特币和以太币都是DPT。[2]

© 2026 Dr Alexander Ressos. General information only, not legal, tax or investment advice. No client relationship is created. All Singapore law advice is provided by a duly licensed and regulated firm of Singapore advocates and solicitors only on the basis of an express written letter of engagement. More information at SingaporeIQ.com and ressos.com.sg.

数字代币服务提供商（Digital token service provider，DTSP）——从新加坡向新加坡境外客户提供数字代币服务的人，自2025年6月30日起须依《2022年金融服务与市场法》第9部分取得牌照。MAS已表示，只会在极其有限的情况下向DTSP发放牌照。

数字孪生（Digital twin）——代表在另一登记册中登记的资产（例如土地、股份或黄金）的代币。所有权由该另一登记册决定，因此代币是一种权利主张或表示，其效力取决于登记所有人与代币持有人之间的安排。

分布式账本技术（Distributed ledger technology，DLT）——对由众多参与者以相同副本持有并通过共识更新的数据库的总称。2020年9月25日的瑞士《DLT法》使用了这一术语，但未限定任何特定架构。

DLT交易设施（DLT trading facility）——依《金融市场基础设施法》第73a条及以下设立的瑞士牌照类别，指允许账本型证券进行多边交易、并可同时提供结算和托管的交易场所。SIX Digital Exchange持有首张此类牌照。

电子货币（E-money）——依《2019年支付服务法》第2(1)条，指以某种货币计价、预先支付、代表对发行人的债权并被第三方接受为支付手段的电子存储货币价值。赋予赎回请求权的锚定法定货币的稳定币可能属于电子货币。

电子货币代币（E-money token，EMT）——MiCA依据第(EU) 2023/1114号条例第3条第1款第7项设立的类别，指通过参考一种官方货币来保持稳定价值的加密资产。在欧盟，只有信贷机构和电子货币机构可以发行EMT。

ERC-20——以太坊的同质化代币标准，规定代币合约必须提供的函数，以太坊及兼容链上的大多数代币都遵循这一标准。ERC-721和ERC-1155是*NFT*的相应标准。

漏洞利用（Exploit）——利用智能合约中的缺陷，违背合约的预期运行方式提取价值。漏洞利用究竟构成盗窃、欺诈，还是对已公开代码的合法使用，是第H部分第I章和第N部分第I章所讨论的问题。

© 2026 Dr Alexander Ressos. General information only, not legal, tax or investment advice. No client relationship is created. All Singapore law advice is provided by a duly licensed and regulated firm of Singapore advocates and solicitors only on the basis of an express written letter of engagement. More information at SingaporeIQ.com and ressos.com.sg.

最终性（Finality）——依账本规则交易不能再被撤销的时点。在工作量证明链上，最终性是概率性的；在权益证明链上，经过规定期间后具有经济上的最终性；在许可制账本上则是确定性的。

金融中介（Financial intermediary）——瑞士AMLA第2条第3款中的术语，指以职业方式接受、持有、投资或转移他人资产的人。大多数拥有处分权的加密服务提供者都是金融中介，必须加入一个自律组织。

闪电贷（Flash loan）——在单笔交易内借入并偿还的无抵押贷款，如未偿还则整笔交易失败。闪电贷可合法用于套利，也可被非法用于操纵预言机和掏空协议。

分叉（Fork）——账本历史或规则出现分歧。软分叉以兼容方式收紧规则，硬分叉则产生两条链。硬分叉后，原代币的每一位持有人在两条链上持有同等数量的代币。

基金会（Foundation，Stiftung）——依《瑞士民法典》第80条及以下、通过将财产用于某一目的而设立的瑞士法人，由理事会管理并受公共机关监督。它已成为楚格协议资金库的标准法律包装形式。

前端（Front-end）——用户与智能合约交互所使用的网站或应用程序。联邦委员会和MAS都认为，前端运营者是DeFi监管的天然对象。

Gas费（Gas）——为处理交易而支付给账本验证者或矿工的费用，以账本的原生代币计价。Gas费是一项经营成本，在相关活动构成营业的情况下可作为经营成本扣除。

治理代币（Governance token）——赋予对协议参数、资金库或升级的表决权的代币。其监管定性取决于投票能否将经济价值导向持有人，以及事实上是否已经如此。

哈希值（Hash）——通过单向函数从数据计算出的固定长度指纹，数据的任何改动都会改变哈希值。哈希值使区块得以链接在一起，并使任何人都能验证账本的完整性。

© 2026 Dr Alexander Ressos. General information only, not legal, tax or investment advice. No client relationship is created. All Singapore law advice is provided by a duly licensed and regulated firm of Singapore advocates and solicitors only on the basis of an express written letter of engagement. More information at SingaporeIQ.com and ressos.com.sg.

热钱包（Hot wallet）——其私钥位于联网系统上、可即时签名的钱包。托管人将其用于提款备付，它也是盗窃的通常目标。它与冷钱包相对应。

混合型代币（Hybrid token）——具有一种以上经济功能的代币。依据2018年2月16日《ICO指引》第3.1节，FINMA对其累积适用每一相关类别的要求。

首次代币发行（Initial coin offering，ICO）——为项目融资而公开出售新创设的代币。这一术语在2017年和2018年占据主导地位，此后已在很大程度上被"代币销售"或"代币生成事件"所取代。尽管如此，FINMA 2018年的《ICO指引》仍是瑞士的定性参考依据。

密钥分片（Key share）——在多方计算安排中由一方持有的私钥片段。密钥分片在各方之间的配置决定了在监管和破产意义上由谁拥有控制权。

第二层（Layer 2）——为提高速度、降低成本而在主账本之外处理交易并定期向主账本提交汇总的网络，例如以太坊上的Arbitrum、Optimism和Base，或比特币上的闪电网络（Lightning）。第二层上的资产通常锁定在主链上的跨链桥合约中。

账本型证券（Ledger-based security，Registerwertrecht）——作为证券在分布式账本上发行、符合《瑞士债务法》第973d条第2款功能性要求的权利，从而使账本记录与权利融为一体。转让通过账本记录进行。该形式于2021年2月1日引入，是两个中心中唯一一种由账本本身充当证券登记册的形式。[3]

有限用途DPT（Limited-purpose DPT）——新加坡《2019年支付服务法》第2(1)条对*DPT*定义所作的排除，适用于仅能在封闭系统内使用的代币，例如游戏内道具或积分。一旦代币可以在系统外兑换为金钱或其他DPT，即不再适用这一排除。

© 2026 Dr Alexander Ressos. General information only, not legal, tax or investment advice. No client relationship is created. All Singapore law advice is provided by a duly licensed and regulated firm of Singapore advocates and solicitors only on the basis of an express written letter of engagement. More information at SingaporeIQ.com and ressos.com.sg.

流动性质押（Liquid staking）——通过协议进行的质押，该协议发行代表质押头寸的可转让收据代币，例如stETH或rETH。这类代币可自由交易，并在整个DeFi中被用作抵押品。

流动性池（Liquidity pool）——持有流动性提供者存入的代币、供*AMM*或借贷协议使用的智能合约。第VI章的分析将资金池视为代表提供者订立合同。

流动性提供者（Liquidity provider，LP）——将代币存入流动性池以换取*LP*代币，并分享资金池从交易者处赚取的费用的人。

LP代币（LP token）——代表流动性池按比例份额的代币，可通过销毁赎回持有人在资金池资产和累计费用中的份额。在DeFi代币中，它最明显地可能被定性为集体投资计划的单位。

模因币（Memecoin）——没有实用功能、没有对发行人的请求权、也没有项目的支付类代币，其价值取决于社区关注度。按FINMA的分类，它属于支付型代币；在新加坡则属于*DPT*。

内存池（Mempool）——已向网络广播但尚未被纳入区块的交易集合。待处理交易对所有参与者可见，因此任何愿意支付更高费用的人都可以抢先交易。

MiCA——第(EU) 2023/1114号关于加密资产市场的条例，自2024年6月30日起适用于稳定币，自2024年12月30日起适用于其他加密资产和服务提供者。它不适用于瑞士或新加坡，但规范两个中心在欧盟的交易对手。

矿工（Miner）——工作量证明网络中通过消耗算力提出区块并赚取新代币和费用的参与者。在挖矿活动构成营业的情况下，挖矿收入在两个中心均作为收入纳税。

铸造（Mint）——通过合约函数创设新代币。稳定币的发行、封装代币的创设以及存入流动性时*LP*代币的生成，均通过铸造进行。

© 2026 Dr Alexander Ressos. General information only, not legal, tax or investment advice. No client relationship is created. All Singapore law advice is provided by a duly licensed and regulated firm of Singapore advocates and solicitors only on the basis of an express written letter of engagement. More information at SingaporeIQ.com and ressos.com.sg.

多方计算（Multi-party computation，MPC）——一种密码学技术，持有密钥分片的多方可共同生成签名，而任何一方都不会获知完整的私钥。目前大多数机构托管平台都采用这一技术。

多重签名（Multi-signature，multisig）——在账本本身上配置的地址，任何交易都须达到若干密钥中的门槛数量（例如三分之二）签名。*MPC*在链下实现类似的效果。

节点（Node）——运行账本软件并持有账本副本的计算机。全节点验证所有交易，验证者和矿工则是还会提出区块的节点。

非同质化代币（Non-fungible token，NFT）——其合约为每个单位记录唯一标识符、从而使各单位可以区分的代币。其定性取决于所代表的权利。在两个中心，独一无二的NFT一般不受金融监管，而系列化或碎片化的NFT则可能受到监管。

混合钱包（Omnibus wallet）——一种托管安排，托管人在一个或少数几个地址中持有众多客户的代币，客户权益仅记录在托管人的账簿中，与隔离钱包不同。依《瑞士债务执行与破产法》第242a条，如果混合钱包客户的份额"易于归属"，瑞士法在破产时对其予以保护。

预言机（Oracle）——向智能合约提供价格等外部数据的服务，Chainlink是占主导地位的提供者。预言机失灵或被操纵是DeFi损失的主要原因之一，也是反复出现的责任问题。

支付型代币（Payment token）——FINMA对意在作为支付手段或价值转移手段、对发行人不享有请求权的代币所设的类别，例如比特币和以太币。其发行受AMLA约束，但不属于证券法范畴。

永续合约（Perpetual future，perp）——没有到期日的期货合约，通过多头与空头持有人之间的资金费用支付与现货价格保持一致。在瑞士法和新加坡法下，它都属于衍生品。

© 2026 Dr Alexander Ressos. General information only, not legal, tax or investment advice. No client relationship is created. All Singapore law advice is provided by a duly licensed and regulated firm of Singapore advocates and solicitors only on the basis of an express written letter of engagement. More information at SingaporeIQ.com and ressos.com.sg.

许可制账本（Permissioned ledger）——其节点为经预先批准的已知实体的账本，如银行联盟和大多数代币化试点所用的账本。它提供确定性的最终性和可识别的运营者，与比特币和以太坊等公共或无许可账本不同。

积分（Points）——项目在链下保存的、记录用户活动的计数，预期在未来上线时转换为代币。积分不属于任何监管分类，但可能引发虚假陈述索赔。

私钥（Private key）——一个很大的随机数，持有人可凭其签署从相应地址转移代币的交易。私钥是赋予对代币的事实处分权的唯一事实，也是本书中一切托管和破产分析的基础。

权益证明（Proof of stake）——一种共识机制，验证者锁定代币作为保证金，并按质押比例被选中提出区块，不当行为将受到罚没惩罚。以太坊自2022年9月起采用权益证明。

工作量证明（Proof of work）——比特币所采用的一种共识机制，矿工通过竞相求解计算难题来争夺提出区块的权利，并赚取相应奖励。

协议（Protocol）——构成某项DeFi服务或区块链网络的一整套规则和智能合约。协议不是人，而其背后是否有人，是第VI章和第VII章的核心监管问题。

公钥（Public key）——通过单向函数从私钥派生出的值，地址又由公钥派生。任何人都可以借助公钥验证签名，而无需知道私钥。

目的绑定货币（Purpose-bound money，PBM）——MAS于2023年6月发布的新加坡设计概念，将数字货币代币封装在一个可编程层中，限制其使用方式和使用场所。这种限制是合同性质的，底层货币不受影响。

易于归属（Readily attributable）——《瑞士债务执行与破产法》第242a条第2款b项规定的标准，用于在瑞士托管人破产时向客户释放混合存放的加密资产。如果托管人的记录无需重建即可显示每位客户的份额，即符合该标准。

© 2026 Dr Alexander Ressos. General information only, not legal, tax or investment advice. No client relationship is created. All Singapore law advice is provided by a duly licensed and regulated firm of Singapore advocates and solicitors only on the basis of an express written letter of engagement. More information at SingaporeIQ.com and ressos.com.sg.

登记协议（Registration agreement）——依《瑞士债务法》第973d条第1款，权利各方约定该权利应作为账本型证券在特定账本上发行的协议。该协议必须记录在账本中或与账本相关联，并应界定分叉后哪条链是"该账本"。

再抵押（Rehypothecation）——托管人为自身目的使用客户资产，例如出借或质押。在两个中心，这都会终止托管关系，使客户沦为无担保债权人。

再质押（Restaking）——将已质押的代币或流动性质押收据作为担保投入额外的服务，从而赚取额外奖励并承担额外的罚没风险。EigenLayer于2023年和2024年推出了这一做法。

Rollup——一种第二层，在链下执行交易，并向主链提交压缩数据或有效性证明。其中，乐观Rollup允许提出质疑，零知识Rollup则提交密码学证明。

助记词（Seed phrase）——由十二个或二十四个单词组成的序列，依据BIP-39标准对种子进行编码，钱包由该种子派生其全部私钥。谁持有助记词，谁就控制由其派生的每一个地址。

隔离钱包（Segregated wallet）——一种托管安排，每位客户的代币分别存放在由托管人控制的单独地址中。它与混合钱包相对应，在两个中心都能产生最清晰的破产结果。

简单合伙（Simple partnership，einfache Gesellschaft）——依《瑞士债务法》第530条及以下的瑞士兜底形式，适用于以共同资源追求共同目的而未采用其他法律形式的人，合伙人承担无限连带责任。它是无法律包装*DAO*的默认定性。

单一货币稳定币（Single-currency stablecoin，SCS）——MAS于2023年8月15日宣布的监管类别，指锚定新加坡元或某种G10货币、在新加坡依储备、资本、赎回和信息披露要求发行的稳定币。只有合规的发行人才可以使用"受MAS监管的稳定币"这一标签。

罚没（Slashing）——在权益证明下，作为对不当行为或停机的惩罚而销毁验证者部分质押代币。提供质押服务的托管人必须披露并管理这一风险。

© 2026 Dr Alexander Ressos. General information only, not legal, tax or investment advice. No client relationship is created. All Singapore law advice is provided by a duly licensed and regulated firm of Singapore advocates and solicitors only on the basis of an express written letter of engagement. More information at SingaporeIQ.com and ressos.com.sg.

智能合约（Smart contract）——存储在账本上、在被交易调用时执行的程序。它是一种履约工具，本身并不是法律意义上的合同。与其交互的各方之间是否存在法律上的合同，由一般合同法决定。

灵魂绑定代币（Soulbound token）——绑定于一个地址、不可转让的*NFT*，用作资格凭证或证明。由于它不能交易，也不能用作支付手段，因此不属于任何金融分类。

稳定币（Stablecoin）——旨在相对于某一参考物（通常是法定货币）保持恒定价值的代币。第IV章依其背后的赎回承诺，将其分为法币支持型、加密资产支持型和算法型。

质押（Staking）——将代币投入权益证明网络以赚取验证奖励，其模式从独立质押、委托质押、托管式质押到流动性质押不等。2023年12月20日FINMA第08/2023号指引规定了瑞士托管式质押的条件。

代币（Token）——记录在分布式账本上的价值或权利单位。本书用这一术语指任何此类单位，而将"加密资产"和"数字资产"保留用于指代总体类别。

总锁仓价值（Total value locked，TVL）——存入某一DeFi协议或整个行业的资产总值。它衡量的是规模，与安全性无关。

旅行规则（Travel rule）——FATF的要求，即受监管中介之间的加密资产转移必须附带汇款人和受益人的信息。瑞士通过AMLO-FINMA第10条实施这一要求，新加坡则通过MAS第PSN02号通知实施。

非托管钱包（Unhosted wallet）——由用户本人而非受监管中介控制的钱包，也称自托管钱包或私人钱包。在两个中心，与非托管钱包之间的转账都须遵守特定的旅行规则和尽职调查要求。

实用型代币（Utility token）——FINMA对提供应用程序或服务数字访问权的代币所设的类别。如果出售时该服务已经存在，它就不属于证券法范畴。如果它是为一项尚未上线的服务筹资而出售，FINMA则将其视为资产型代币。

© 2026 Dr Alexander Ressos. General information only, not legal, tax or investment advice. No client relationship is created. All Singapore law advice is provided by a duly licensed and regulated firm of Singapore advocates and solicitors only on the basis of an express written letter of engagement. More information at SingaporeIQ.com and ressos.com.sg.

UTXO模型（UTXO model）——比特币所采用的一种账本设计，价值以离散的未花费交易输出来追踪，每个输出都须整体花费，并由新的输出取代。与账户模型不同，它支持基于来源脉络的追踪。

验证者（Validator）——权益证明网络中锁定代币作为保证金后提出和证明区块的参与者，诚实参与可获得奖励，不当行为则面临罚没。

钱包（Wallet）——存储私钥并签署交易的软件或硬件。钱包中除密钥外不存储任何东西，因为代币本身始终留在账本上。

白皮书（White paper）——描述代币项目及其技术和经济模型的文件。在MiCA下，它是一份受监管的信息披露文件。在《金融服务法》和SFA下，如果代币属于证券且不适用任何豁免，它可能构成招股说明书。

封装代币（Wrapped token）——某一账本上的代币，代表通过跨链桥锁定在另一账本上的代币，WBTC是其主要代表。从经济上看，它是对控制被锁定资产者的请求权。

零知识证明（Zero-knowledge proof）——一种密码学方法，一方可借此证明某一陈述为真，而不披露底层数据。它被用于*Rollup*以提高可扩展性，也被用于身份系统，以证明年龄或司法管辖区等属性而不披露身份。第F部分和第L部分讨论了它与反洗钱合规设计的关联。

注释

1. Anti-Money Laundering Act, SR 955.0, Art. 2 para. 3（非银行业金融中介）。第F部分第I章。 ↩
2. Payment Services Act 2019 (Singapore), s. 2(1)。该定义排除了电子货币和有限用途*DPT*。第K部分第I章。 ↩
3. Code of Obligations, SR 220, Arts 973d–973i。第D部分第III章。 ↩

© 2026 Dr Alexander Ressos. General information only, not legal, tax or investment advice. No client relationship is created. All Singapore law advice is provided by a duly licensed and regulated firm of Singapore advocates and solicitors only on the basis of an express written letter of engagement. More information at SingaporeIQ.com and ressos.com.sg.

Disclaimer

This article is provided for general information only. It is based on publicly available sources as at its date of publication. These sources have not been independently verified against licences, regulatory registers or the records of the entities concerned. It is not legal, tax, financial or investment advice. Nor is it a recommendation to invest in, transact with or use the services of any entity mentioned. Law and regulation change frequently, so the content may be incomplete or outdated. To the fullest extent permitted by law, Dr Alexander Ressos and the publisher of SingaporeIQ exclude all liability for loss or damage arising from the use of or reliance on this article. Readers should obtain advice on their specific circumstances before acting or refraining from action.

Names and trademarks of the entities discussed belong to their owners and are used for identification only. Their mention implies no endorsement, affiliation or allegation of wrongdoing. All Singapore law advice is provided by a duly licensed and regulated firm of Singapore advocates and solicitors only on the basis of an express written letter of engagement. Corrections and updates: contact@ressos.com.

© 2026 Dr Alexander Ressos. This article may be quoted with attribution to SingaporeIQ (SingaporeIQ.com). Reproduction in full and any commercial use require prior written consent. The Legal Terms at https://singaporeiq.com/legal-terms apply.

Author contact: Dr Alexander Ressos, TEP · contact@ressos.com