泰德比特

香港加密货币交易所技术白皮书

TideBit v2.0.4 20230323

CONTENTS

TideBit

01

背景介绍

金融科技之发展与市場現況

近年来，金融科技高速发展吸引诸多企业投入，根据报导在 2021 年全球金融科技业投资总额达2,100 亿美元，在包括美洲、欧洲、中东和非洲和亚太地区等主要市场交易量都创下新高，其中以区块链以及区块链资产最受瞩目，也为现代的金融带来巨大的变革。

自 2009 年比特币问世之后，区块链资产逐渐走入投资人的视野，其中以至今暴涨超过两千万倍的比特币（Bitcoin）最受瞩目，吸引了大量投资者关注。加密货币暴涨暴跌的特性，促使各国央行或相关单位相继推出各种管制政策，尽管加密货币相较于全球主流金融市场仍有很大成长的空间，不少人对加密货币的未来仍抱持乐观态度。

除了早已为人熟知的比特币之外，众筹至今已上涨一万五千倍的以太坊（Ethereum）的发展也不容小觑，以太坊拥有图灵完备（Turing Complete）特性，具备自动执行完成交易的智能合约（Smart Contract）功能，造就了广大的生态系， 在 2015 年底，以太坊建立了以太坊代币标准（Ethereum Token Standard，简称 ERC20 ），透过 ERC20 标准 所设计出来的代币，就可以使用智能合约来进行代币的交换和流通，而这也催生了代币发售这类创新的募资方式，开启了代币经济（Token Economy）新时代的序幕。

根据瑞士金融市场监督管理局（FINMA）在 2018 年 2 月时发布的指南，将代币定义为三个种类：支付代币、功能代币以及资产代币。而加密货币交易所推出的代币即属于功能代币的范畴，仅提供使用交易所服务或应用程式的权利，由于平台币属于交易所专用，随着交易量提升，实用率高，价值稳当，升值空间也备受期待。

如今随着金融科技的发展，数字支付也蓬勃发展逐渐取代现金交易，为了因应越来越多金融科技的创新应用，各国央行也开始主动研究数字法币（Central Bank Digital Currency，简称 CBDC）的可行性，但每个国家对于 CBDC 的态度以及发展策略却是大相迳庭。其中，中国态度积极，欧盟则不保证未来一定会发行数字欧元。

金融科技正稳定且确实地改变全球化社会的运作形态，然而社会制度往往无法跟随着科技的脚步快速变革，这埋下了弊案的隐忧。

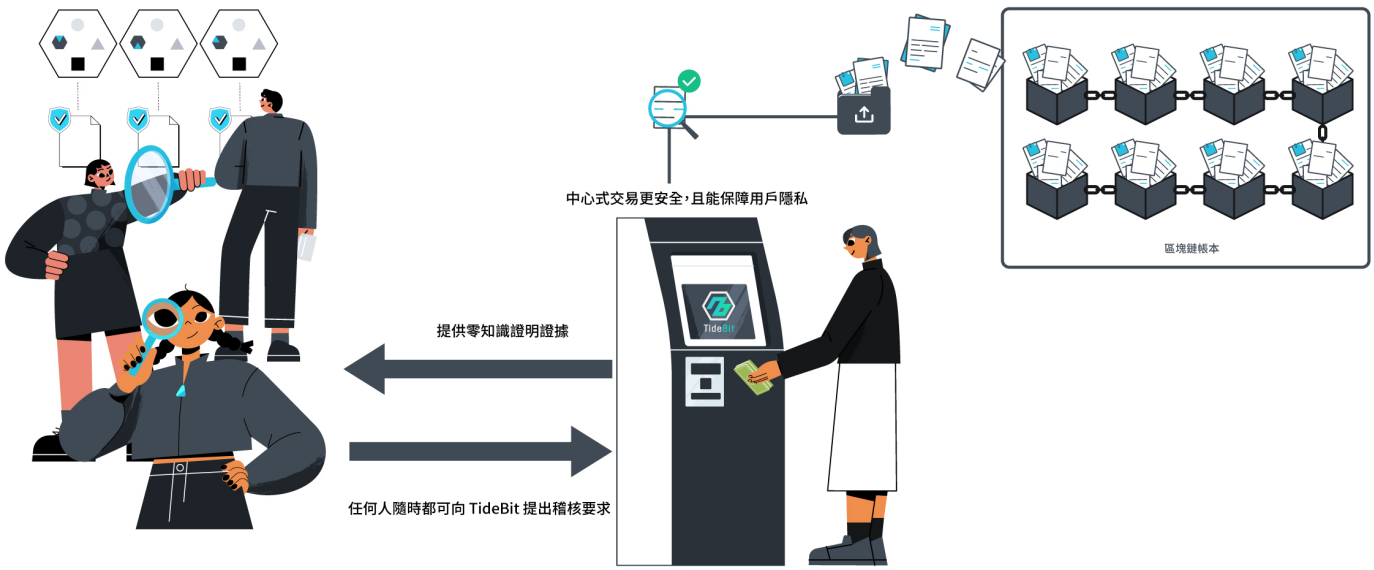
监管制度的困难与挑战

在技术上，国际大型交易所遭骇客入侵案件频传，许多用戶保存在交易所中的加密货币被骇客盗走且无法追回，造成用戶与交易所莫大的损失，然而这类事件却往往无法追查到犯案的凶手，也无法给予受害人合理的补偿。

在制度上，我们经历了 2020 年德国支付公司 Wirecard 宣布破产，2021 年财务科技公司 Greensill Capital 宣布破产，2022 年全球第二大加密货币交易所 FTX 破产。我们发现除了区块链资产交易所这类新兴金融科技服务缺乏有效的监理机制，传统的金融服务也逐渐反映出现有监管制度已无法应对新时代的金融服务。

金融科技领域的公司虽然比传统金融机构更加创新，更愿意导入新技术解决过往无法克服的问题。通过创新的产品和服务一方面提高金融效率和便利性，但也因此面临更大的风险和不确定性。因此随治理理念的进步和科技发展，金融科技公司以及监管单位都应该充分利用新技术优化其业务模式和风险管理措施；TideBit 团队提出了这份中心交易和去中心监管相融合的解决方案 (如图一)，应对未来金融科技持续进步的潜在的风险和挑战。

图一



中心化交易與去中心化監管

TideBit 发展与沿革

TideBit 由 TideBit 团队所开发并于 2017 年推出，是支持法币与区块链资产，于香港立案合规的中心式交易所。TideBit 客戶主要来自全球海内外华人包含阳光卫视收视戶，具备高度文化知识水平，高度关注国际政治局势，常态性用戶约六万人，自 2017 年上线至今积极配合各地政府合规营运。 TideBit 同时积极投入区块链审计、安全技术的研发，持有多项底层运行以及风险管控技术，至今维持零起入侵事件，零起异常灾害。

02

TideBit 2.0
技术概述

去中心化身份验证

去中心化身份验证是一种身份验证机制，其目的是在无需第三方权威机构的情况下，验证参与方的身份。这种机制基于区块链技术，使用加密算法和去中心化的存储方式，确保参与者的身份和数据不受篡改和伪造。TideBit 去中心化身份验证基于区块链身份，用分布式账本技术和加密算法，为参与者分配唯一的数字身份，每个数字身份可以绑定唯一的自然人或法人身份，并每个绑定都经过 TideBit 的审核认证，这种身份可以被用于在去中心化应用程序中验证参与者的身份，甚至是参与公众事务决策。

去中心化监管

许多人对区块链的常見误解中，有这么一条：因为区块链要求去中心化，而监管的主体本身是一个巨大的中心，这两者是不可能共存的。表面上看，这么说好像有点道理，但实际是有问题的，因为去中心化并不是不要中心，而是强调许多中心之间，不论大小，公平且自由。

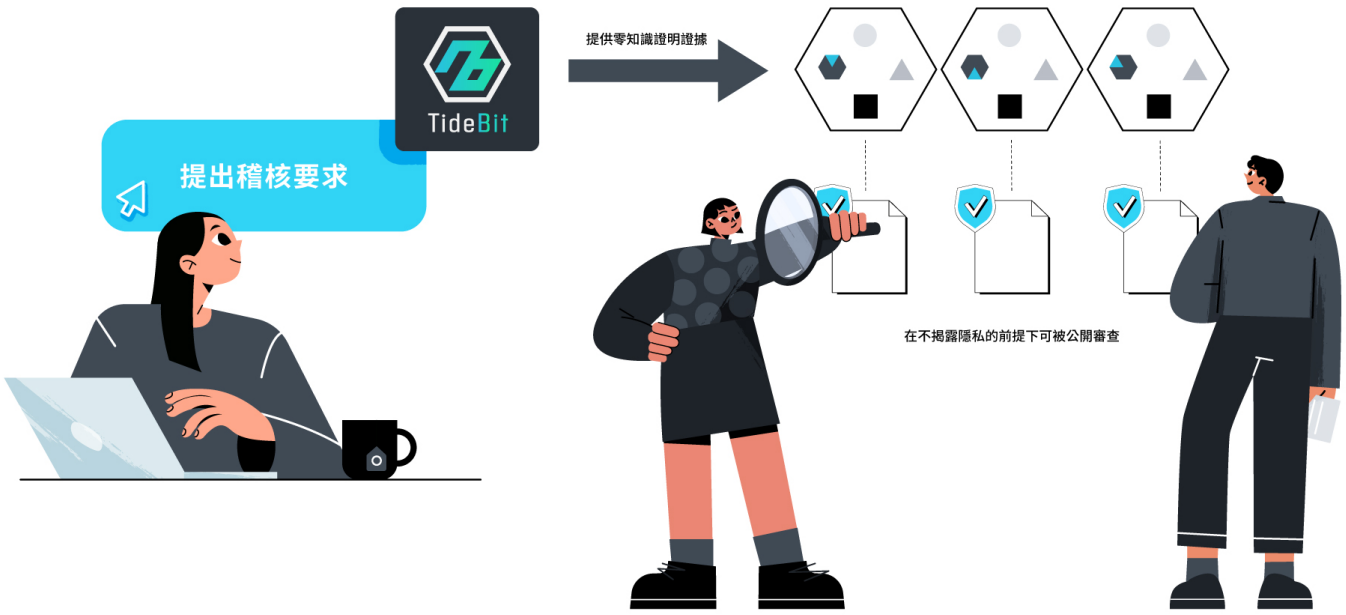
其实，去中心化这个概念自提出来起，就从没想过要消灭中心或者剥夺中心的权利。不管是比特币也好后来者也罢，它们的目的在于：不能让一切都是被少数人控制的强大中心，而不是说要排斥中心或抹杀中心。

去中心化系统是由许许多多的大小中心组成的一个分布式网路，在比特币的工作量证明机制中，大算力矿池其实也是一个大中心，大中心和所有小矿工都要遵守同等规则，多劳多得，避免出现大中心控制整个系统导致其他小矿工的分配不公平现象。因此，在未来类似这种公平的机制条件下，得到越来越多人的认可后，大小组织机构、甚至是一些国家，都可以自由地成为无数节点中的一员，受到系统公平的对待。所以，去中心化和中心机构是可以共存的。

去中心化的网路，似乎是人人平等，在上面可以为所欲为没有人能管，就像是网际网路发展早期的时候，网路上的匿名特性时常被作为不法行为的工具。在科技高速发展改变人们生活型态的同时，监管往往是滞后的。科技的发展速度非常快，没有人能知道它的方向是怎样的。同样大型机构不一定能掌握最先进的技术发展，往往只能跟随发展的脚步，去做一些既能维护社会稳定又不阻碍科学技术发展的事情，在这个前提下由少数组织（如政府）执行监管便是一项不切实际的任务，因此我们需要其他不同样的监管模式。

随着区块链的技术发展，尤其是零知识证明技术，资料开放的型式也变得更多元。证明一份资料的有效性不再需要将所有数据摊开给监管单位，而是在平时提交加密且压缩后的证据资料，当特定范围资料受到质疑时，再提交解密后的明文资料进行查证，并比对其是否符合区块链上的证据。至此，监管工作不再是由中心式的机构执行（尤其不应该由交易所自身来执行），而是由分布式网路中每一个参与的人员，都平等地拥有监管的权限。就如同每个用戶都可以从区块链网路上追溯每一个区块链钱包地址的资金来源以及资金走向，每个用戶也应该要能够针对自己使用的交易所进行监管，当交易所发生不当行为时及时举证并检举之，这便是我们所归从化的去中心式监管的概念 (图二)。

图二



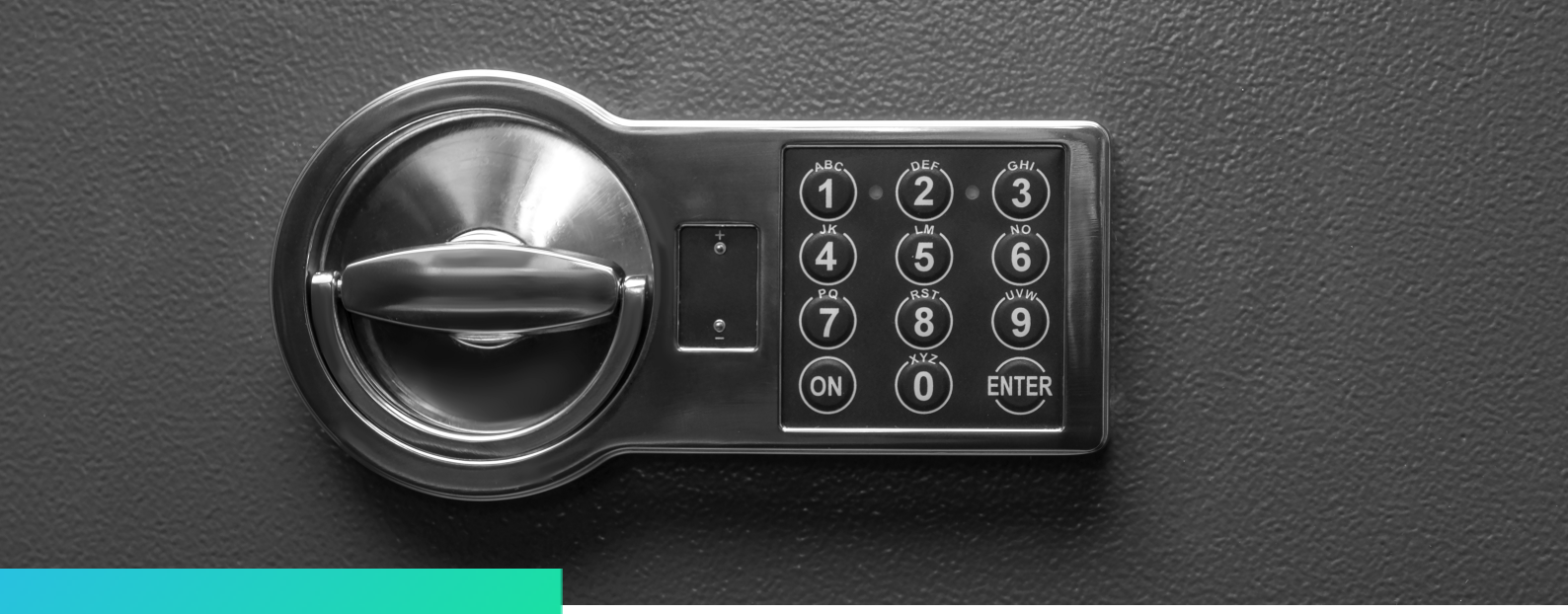
去中心监管 = 任何人 （用户、政府、商业伙伴）都可以实时监管

人工智能
数字治理

随着新兴科技的崛起、法规环境的转变，商业模式和客戶体验不断地演化与创新，金融科技发展所面临的风险管理议题，包含策略风险、营运风险、网路安全与资料风险、作业与财务风险等各个面向，都将更加复杂、多元且艰钜，因此，数字金融时代下金融机构的风险治理将从单点管理走向整合性价值链生态圈治理。运用法遵科技，亦即RegTech (Regulation Technology) 强化风险管理或为解决之道。例如企业布建资料风险分析平台应用蓝图，针对企业内部 (资讯安全、资料保护、内控回圈) 及外部 (竞争者资讯、协力厂商资料、以及开放资料)，从单一领域深度分析进展至跨领域的综合分析，同时建置有效的异常存取规则(人、事、时、地、物)，借由网路威胁情资分析平台，自动搜集外部威胁资讯，整合内部情资，产出资安趋势及风险分析报告，并针对审计轨迹进行主动管理，赋予数据应用崭新视野，强化数据分析于风险管理的地位。

03

去中心化身份验证与资产防护



TideBit Connect

TideBit Connect 是一个开放性的身份验证标准，得到了许多大型企业和组织的支持，它提供了一种更安全、更便利的身份验证方式。使用公私钥电子签章与验证技术，所有用戶可自行建立并保管专属的私钥，通过私钥签署登入任何系统，以及授权各项操作，大大提高安全性。

TideBit Connect 是一个标准化的技术，支持多种平台和设备，可使用热钱包软体包含 Metamask、imToken、Trust 等 APP，也可使用多种冷钱包包含 Ledger、CoolWallet、AT Wallet 等硬体，为用戶提供更多保管自己去中心化身份的选择。

整体而言，TideBit Connect 身份验证技术具有更高的安全性、更便利的使用体验、标准化和跨平台等优点，旨在成为身份验证领域的技术标准。

TideBit Vault

TideBit Vault 是一种区块链资产的保险箱技术，每一个 TideBit Connect 身份都可以产生一个独一无二的 TideBit Vault，用来保管该用戶的区块链资产。不同于一般中心式交易所技术，用戶将区块链资产存放至 TideBit 时，TideBit 会为每个用戶创建各自的 TideBit Vault 并将用戶资产保管其中。

TideBit Vault 使用自身研发的 Partial Private-Key Protection（P3）技术，动用资产必须取得指定私钥签署，并取得平台验证签署后，方能建立区块链交易转移指定资产，确保交易所无法动用用戶资产，即使恶意骇客入侵交易所亦无法影响用戶资产安全。

除此之外 TideBit Vault 也会分析用戶遭受盗用的风险可能性，当系统判定用戶可能遭受盗用或从事不法行为时，也能即时中断该操作，避免造成用戶损失。

区块链顾客身份尽职调查

用戶以 TideBit Connect 技术进行身份验证时，我们将该私钥是唯一独一无二的顾客个体，但在法律身份上该用戶仍处于匿名状态。基于维护顾客与其资产安全之需求，TideBit 使用多种风险管控技术确保交易市场的公平安全，并制止洗钱或资助恐怖活动发生在交易所内，区块链顾客身份尽职调查即是其中之一。

TideBit 要求并检验用戶提供当地政府合规的自然人或法人证明文件，在确认为本人后，担保该私钥可代表顾客执行一切当地政府法规认可行为。除此之外，TideBit 会在告知用戶的前提下，调查顾客于身份验证机构的合法性和信誉，同时比对国际机构提供的高风险犯罪名单，针对顾客风险等级执行相应措施。

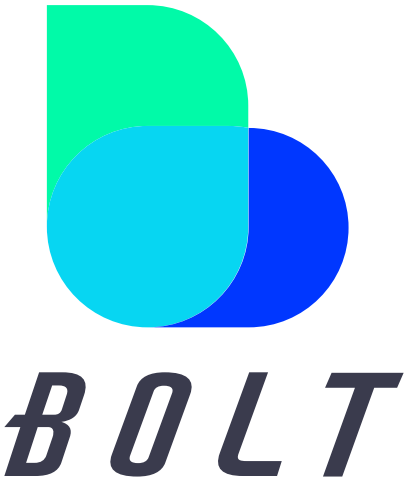
区块链资产来源分析

为了维护金融社会的善良公序，有效遏止金融犯罪行为，TideBit 自主研发 Blockchain Assets Source Tracker（BAST），针对每一笔存放至 TideBit 的区块链资产来源，比对国际份罪事件分析该笔资金来自金融犯罪所得的可能性。除了来源分析，我们也同时分析资金来源地址与资金提领地址与高风险犯罪名单的相关性，可以做到 1 小时内完成该用戶风险等级，并于 24 小时内完成当地政府通报等，临时性资产冻结等应变措施。

04

去中心化监管

BOLT 介绍



去中心化监管核心技术

TideBit 自 2016 年起，与各国金融机构以及香港交易所讨论区块链下的金融科技生态，根据其中需求而设计了自有的去中心式监管区块链技术 Blockchain Open Ledger Technology（BOLT），用来实作包含 TideBit 交易所在内的各种金融科技系统会计、审计、以及函证需求。此技术同时孕育台湾科技公司在政府指导下取得证券交易金融执照。

BOLT 作为开放的分散化帐本技术，任何人都能下载执行，作为区块链结点维持其运作。技术设计方面，BOLT 在确保资料不被篡改的区块链基础上，使用了零知识证明技术，使得存放于区块链上的资料得以在没有机密资讯泄漏风险的前提下，接受第三方审计单位检验调查。

BOLT 自 2018 年至 2019 年间与香港交易所（HKEX）合作，制定一系列区块链技术于审计上的应用包含：

金融产品 / 储备证明

以区块链型式将股票、基金、债券等金融产品转换为区块链资产，并根据智能合约完整记载其交易履历。

企业内控 / 法规遵循

以区块链实现企业人工智能数位治理，所有企业帐务皆透过零知识证明技术于链上存证，杜绝非法情事。

大数据应用 / 防伪溯源

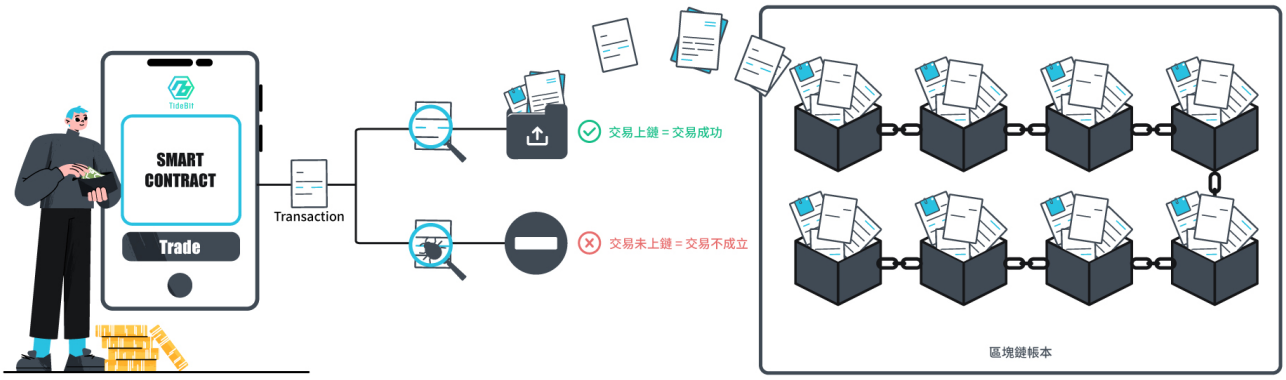
提供区块链结决方案应用于产品物流与供应链管理，同时为每一件产品提供一个独一无二的身份验证机制，在抵御仿冒品同时也提供用户完整产品履历。

零时证据与零时审计

所有 TideBit 上的用戶行为，包含存放或提领区块链资产，执行或取消现货交易都使用运行于 BOLT 上的智能合约，因此所有交易纪录都将存放于区块链上，每一笔用戶委托需求都公正地交由区块链上的智能合约运作，以演算法取代代理人机制，达到绝对的公正公开透明。用戶也能自行在区块链浏览器上确认之，同时取得相关证据。

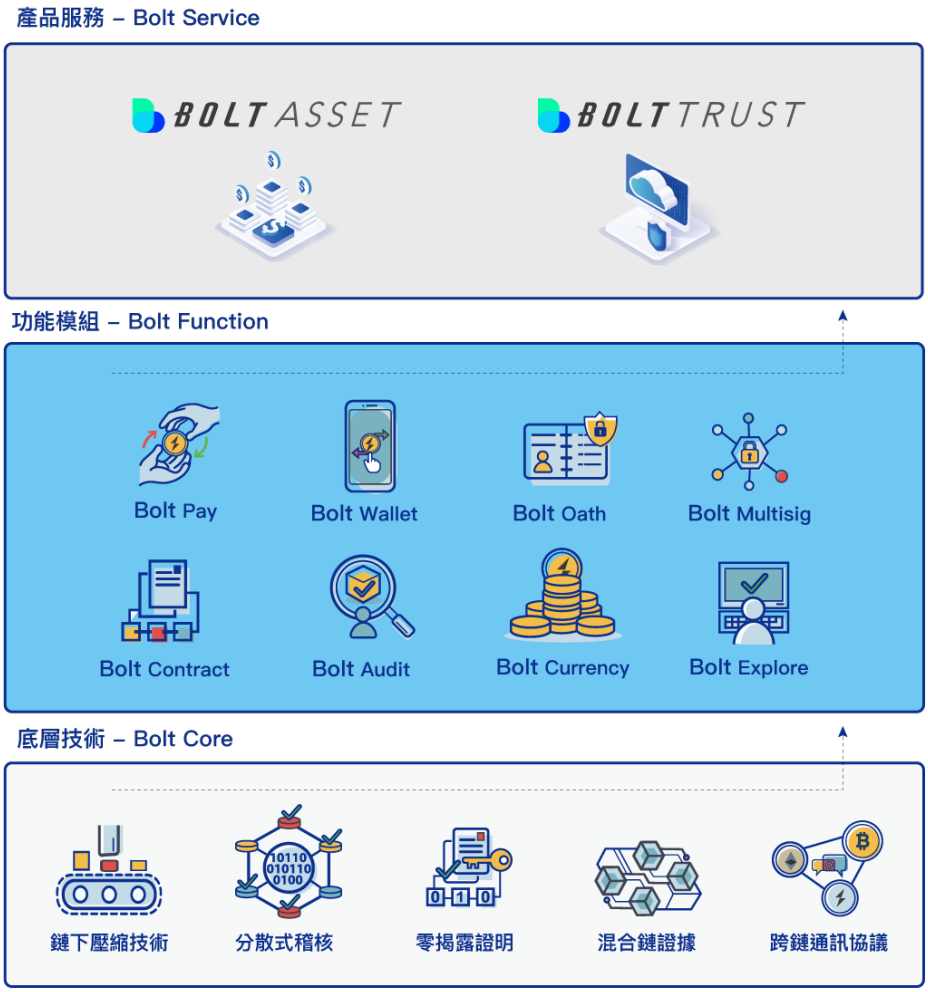
不同于传统的会计审计机制，TideBit 交易所的所有交易都是零时纪录，所有交易成立的瞬间便可在区块链上公开其证据，同时所有的交易在产生的瞬间便交付所有区块链节点（图三），根据智能合约上的规范及时进行审计，以演算法取代人工的审计除了摆脱了传统审计会计周期的限制，也形成一个最公正且透明的合约执行平台，任何违背用戶意愿或智能合约条文的交易，在证据提交后会的瞬间受到区块链否决。

图三



零时审计

图四



BOLT 平台化服务架构图

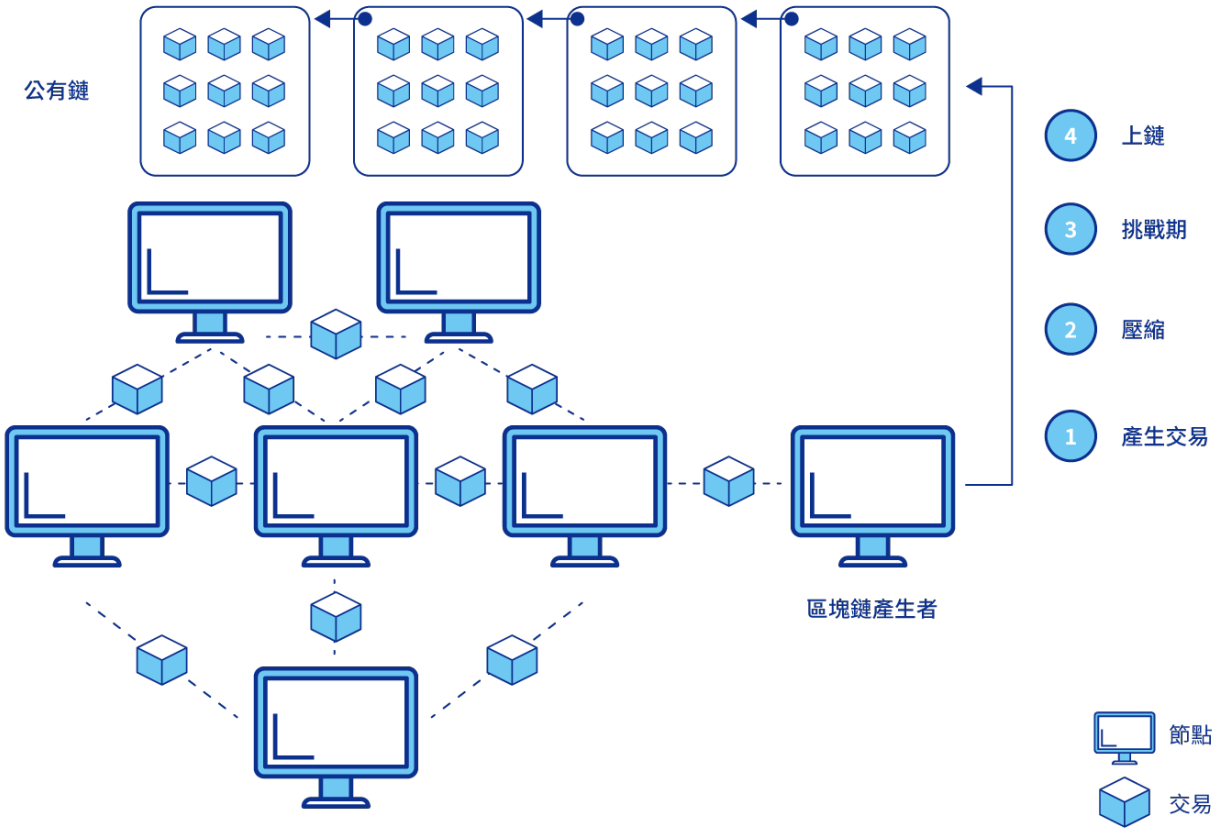
高速通讯协议

BOLT 使用特殊的通讯协议模式 Locutus，节点之间会定期根据共识定义出一张所有节点都可以互相连线的通讯树状网路 Borg-Tree。在这份网路中，从任何节点发出的资讯都会有一个最快速的传递模式，快速散布至所有节点中。

序列化压缩存证技术

为了达到全球共识，BOLT 被设计成可以在陌生的节点与节点之间协同运行，且不需要中心化的伺服器控管权限，以区块链上的智能合约来公布其运作协定。参与者在 BOLT 取得协定，遵循被公布的协定运作 (图五)。

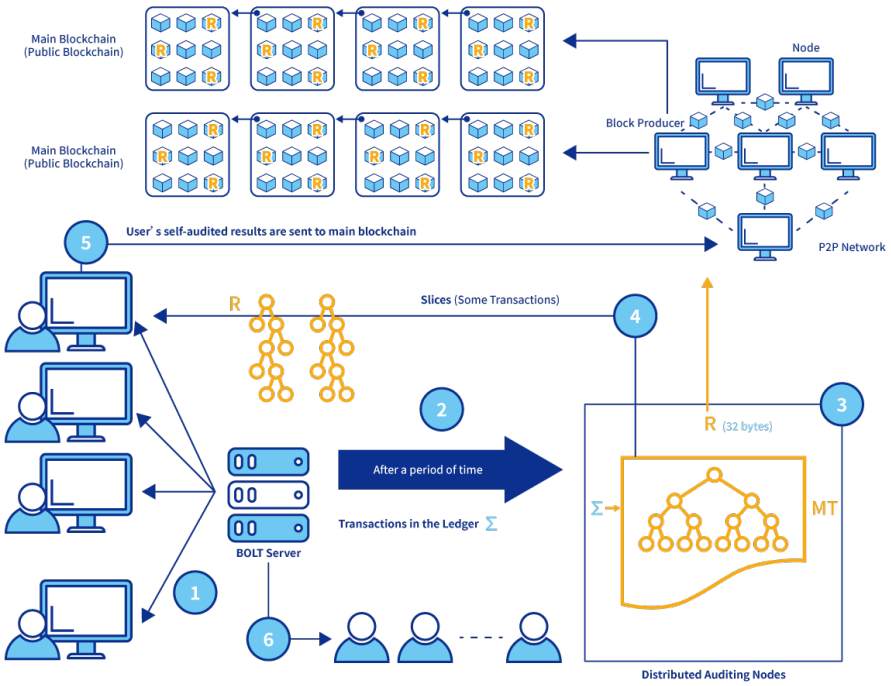
图五



序列化存证压缩

跨链协议 (Cross-chain channel)

图六



BOLT 的跨链区块链架构如图六所示。所谓跨链就是多条平行的区块链（Paralle Blockchain）之间组成的联合运作模式。一般的区块链交易，如加密货币交易或单一合约纪录，用户会直接将交易资讯送到该区块链的 P2P 网路中，最后由成为区块产生者的节点来固定到主链上，这样的交易受限于该区块链的特性，可能会带来较高的交易成本以及较慢的交易速度。因此当需要进行大量且高速交易时可以将交易送至 BOLT 上执行，BOLT 的运作高速，一段时间后累积大量数目的交易，由 BOLT 运作去中心化运行的稽核节点产生哈希值及相关识别码送给节点，透过跨链协议固定在其他公有链。整个 BOLT 的跨链区块链架构有『一般节点』（以下称为节点）及『稽核节点』来组成整体系统的去中心化运作。

BOLT 采取多层次架构（Hierachy-Based），将共识系统中的一致性交由最上层主链来达成，而各自应用的交易有效性则是下层的资料结构来实现，而这些下层的侧链（可以是任何资料结构所构成）需要时可以随时产生，数目无限制，非常适合用来解决现实场景与区块链介接的问题，在 BOLT 所提供的特性中，我们不仅仅是增加频宽、解决链上资料庞大以及隐私保护问题，更解决了现行应用系统与去中心化系统难以融合的情况。

BOLT 的多链运作中，主链的一致性使用公有链的全球共识，而侧链的有效性及如何保持正确及避免代理人（或是稽核节点）的单点失效或恶意攻击，则是利用 BOLT 所设计的侧链运作，包含分散化稽核功

PoHCE 共识

在 BOLT 运作过程，如同其他的区块链，每隔一段时间需要将链上交易证据进行封装成一个区块，并广播至所有节点形成共识，由于 BOLT 使用了上节混和链证据（HCE）确保其不可篡改特性，因此结点间进行共识时需要仰赖比其他区块链更加复杂的分工与处理，而所有参与整个 BOLT 共识过程的节点，根据其付出程度都能得到相对应的奖励，下面条列出在 BOLT 共识机制中的节点角色与其负担事项，每个节点可担任多种不同的角色。

集群管理者

在这个角色，节点有三项主要职责：维护节点成员清单、定期对成员进行评分并维护成员评价资讯、广播与协调各项资讯，共识机制的通讯行为皆由此角色代理进行，同时也确保节点的评价必须达到一定程度才能执行特定角色。BOLT 使用改良后的 Raft 演算法管理集群，并在一致的节点名单下使用独有的广播演算法技术 Locutus 确保所有的协议能在最短的时间内完成。

区块封装者

在这个角色，节点的主要职则便是将既有交易验证后打包，再根据上述技术产生压缩证据，节点之间根据证据确认彼此资料皆无误便完成了封装共识，其后便会继续生成跨链证据，并将打包后的交易加密后上传至 IPFS 上封存。

资料稽核者

在这个角色，其需要在区块封装者完成工作后快速进行资料抽查，结点会根据演算法决定此区块内自己所负责的稽核范围，借此在证据上传至其他区块链之前快速检验其都是正确无误的，然后产生稽核共识。这个共识环节需要复杂的机制确保其即时性，详细细节在下个章节会进行补充描述。

证据上链者

担任这个角色的节点会各自负责不同的区块链，在达成稽核共识后，便将前面完成的跨链证据上传到自身负责的区块链上，同时也需要支出上链成本。

借由这一系列的共识机制，除了可以确保攻击者更加难以突破 BOLT 的保护，同时新节点的加入也只需要向其他区块链及 IPFS 索取 BOLT 资料，让系统整体的安全性极大幅度提升。

分散化稽核

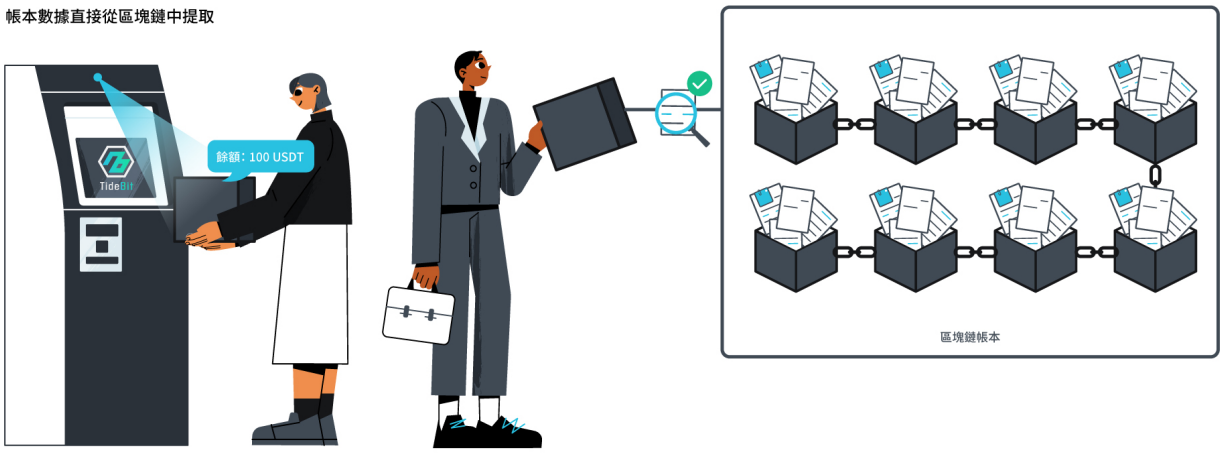
承上节，在使用 PoHCE 共识机制后，验证区块与交易资料的行为变得更加复杂，同时又牵涉到需要与其他区块链上的智能合约进行互动，时间成本也将大幅度的提升，因此我们需要一套机制将稽核作业进行分工，确保其不影响系统效能。

去中心化的系统，面对有代理人操作的运用，主要的问题是代理人是否将正确的交易记录放上区块链，BOLT 分散化稽核技术可以解决此问题。因为侧链的代理人的运作还是经由分散化的方式来稽核，所以整个系统的依然维持去中心化的运作概念。关于先让代理人处理一些交易，再放到区块链来记录，在早期比特币发展期间有一些系统被提出，但是这些系统无法解决代理人黑箱作业的问题，这和区块链去中心化的理念违背，因此无法被广泛的接受。BOLT 的分散化稽核技术，已彻底解决此问题。

在侧链运作中，所有交易都妥善储存于索引莫克树且其根哈希值被公布后，参与者及数字资产提供人的某个交易可以经由索引函数立即定位出在索引莫克树的那个底层节点。参与者要稽核自己的交易是否正确或是否有存在于交易帐本中，即对代理人提出某交易的稽核请求，因为参与者本身有交易的序列号（此交易的完成有代理人的电子签章，所以代理人不可否认），所以代理人必须呈现此交易的切片，消费者可以使用此帐本的根哈希值及此交易的切片来验证此交易是否正确或是否有存在于交易帐本中。

分散化稽核于侧链运作和整个区块链的生态系统结合，不仅区块产生者有仲裁的能力，也根据其产生区块的工作及验证贡献获得回馈。

图七



无法被修改的帐本

交易用戶自主審计办法

图八

交易用户自主稽核

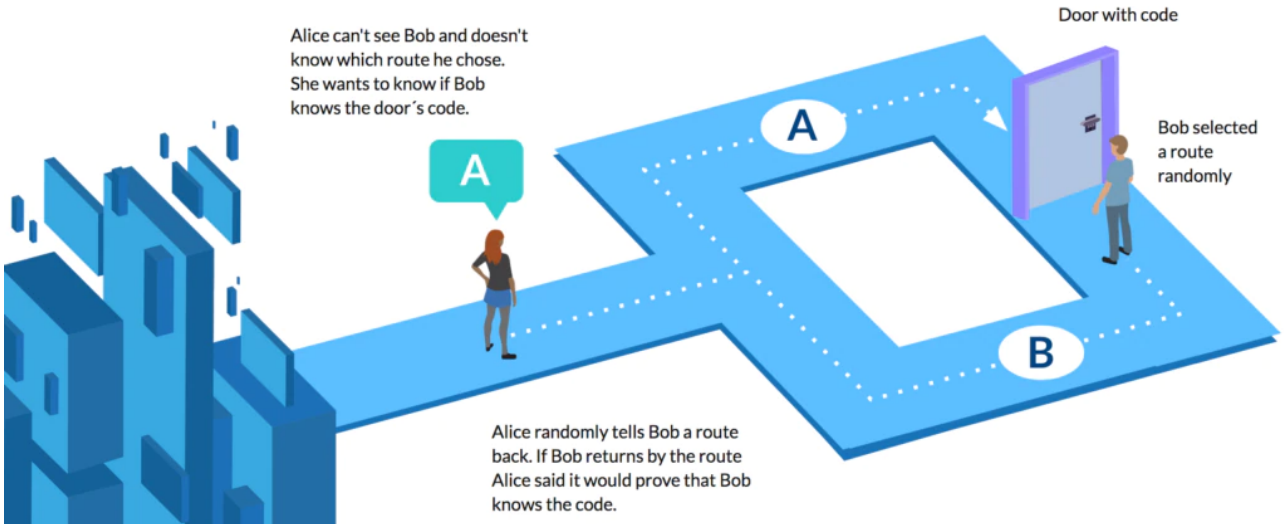
为确保用戶隐私，交易细节是以 BOLT Evidence 格式密文方式存放在区块链上，TideBit 用戶在任何情况下都可以从 TideBit 下载自身交易的明文资料；即使 TideBit 交易所损毁或停止运作的情况，都可以自行从区块链上下载记载自己所有交易纪录的 BOLT Evidence 。用戶的明文交易资料除了会永久保存于 TideBit 之外，用戶也可自行保存，在具备足够的区块链知识下，用戶得以针对所有内容自主进行审计 (图八)。这些交易纪录中存放了在多国政府法律中承认的电子签章证据，让用戶随时确认 TideBit 内无法存在违反用戶意愿的交易行为。

用戶除了自主监管自主审计外，也可以将相关证据提交给其他第三方区块链公司协助审计调查。

第三方单位零知识证明审计办法

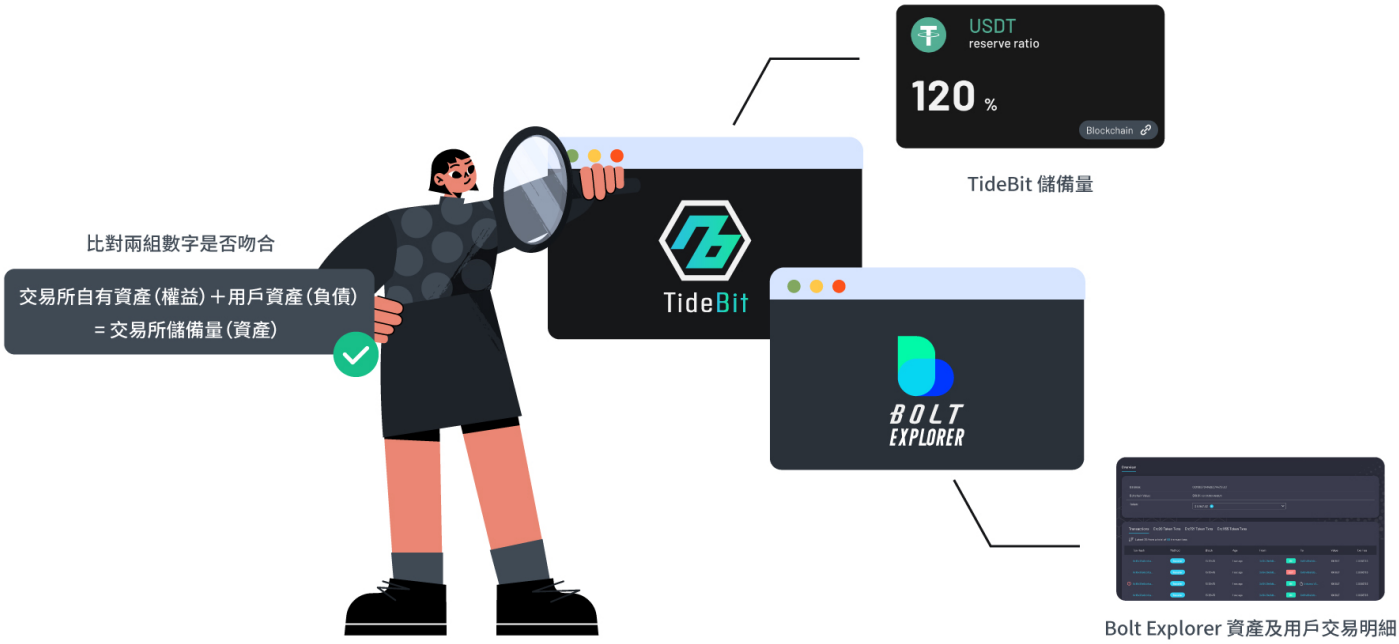
承上节为确保用戶隐私，交易细节是以密文方式存放在区块链上的，每一笔隐私资料都将转换为特殊的 BOLT Evidence 格式，在数学基础之上可以进行简易的运算验算。所有交易的明文未加密资料都会永久保存于 TideBit 内，在特定的情况下，第三方审计单位可能会需要解密后的实际交易资料来调查事件全貌。TideBit 设计了最周全的保管职责处理流程方针，第三方单位在持有用戶私钥签署的同意智能合约后即可自行于区块链上取得明文资料，或提供相关用戶所在当地政府合法授权文件后，由 TideBit 提供明文资料。

图九



零知识证明概念图

图十



交易所区块链资产存量证明

交易所区块链资产存量证明

TideBit 作为公开的金融科技服务平台，以最先进的金融科技确保运作的公平性与公正性，提供从学术上与技术上的检验标准，除此之外 TideBit 也恪守超过业界标准的风险管理流程。所有 TideBit 的用戶资金皆保管于 TideBit Vault 当中，我们也 24 小时不间断记录所有 TideBit Vault 的区块链资产流动，并及时公布于 TideBit。透过公开的资讯，用戶也能自行于区块链上验证资料可信度，确保 TideBit 永远都具备充足的区块链资产存量。

区块链流动性聚合引擎

截至 2022 年，全世界已存在超过一千家中心式或去中心式区块链资产交易所，交易所市场因此愈来愈分散，各个交易所因为彼此无法共享流动性，造成极大的市场行情差距，在这样的市场障碍下，除了减低交易的效率外，也大幅提升用戶交易成本。

为了解除这样的问题，TideBit 自行研发了基于 BOLT 区块链的流动性聚合引擎，整合不同交易所的行情资讯，即时提供用戶在 TideBit 上取得各个交易所间最佳的交易策略。

零时跨域委托单整合系统

承上，用戶在 TideBit 上执行的交易委托，除了会在 TideBit 上执行外，也可以即时映射至可提供服务的交易所上，在任何灾难下也能确保用戶权益不受影响。由于 TideBit 运行在 BOLT 区块链技术上，只要市面上存在正常运作的 BOLT 节点，用戶便能继续使用 TideBit 服务，用戶依旧可以自由提回存放在 TideBit 上的区块链资产，也能借由其他交易所继续执行交易。

跨域交易撮和引擎

基于零时跨域委托单整合系统，我们得以在 TideBit 上，基于区块链智能合约的审计技术，开发跨域交易撮和引擎，让用戶在不同的交易所间执行跨域撮合，大幅提升区块链资产的交易效率。

05

结语

从 2017 年至今，TideBit 接受了大量金融机构，尤其是香港交易所以及台湾金融监督管理委员会的指导，建议累积了极大量的实务经验，不间断地致力于区块链技术的研发与改良，期望持续不断在金融科技领域上为世界带来革新以及正面影响。为此我们设计了集合过往经验大成的 TideBit 2.0 更新计划，也在此同时发布团队研发多年的 BOLT 区块链技术，期望未来能在不停精进 TideBit 同时也促使金融服务的改革与进步，以促进人类社会的发展。

TideBit