Axelární síť:
Propojení aplikací s blockchainovými ekosystémy

Návrh 1.0

ledna 2021

Abstraktní

Objevuje se několik blockchainových ekosystémů, které poskytují jedinečné a odlišné funkce atraktivní pro uživatele a vývojáře aplikací. Komunikace napříč ekosystémy je však velmi řídká a roztříštěná. Aby aplikace mohly bez problémů komunikovat napříč blockchainovými ekosystémy, navrhujeme Axelar. Axelar stack poskytuje decentralizovanou síť, protokoly, nástroje a API, které umožňují jednoduchou cross-chain komunikaci. Sada protokolů Axelar se skládá z přeshraničních směrovacích a přenosových protokolů. Síť pohání decentralizovaná otevřená síť validátorů; kdokoli se může připojit, používat jej a účastnit se. Byzantský konsenzus, kryptografie a pobídkové mechanismy jsou navrženy tak, aby dosahovaly vysokých požadavků na bezpečnost a životnost, které jsou jedinečné pro požadavky napříč řetězci.

1. Úvod

Blockchainové systémy rychle získávají na popularitě a přitahují nové případy použití pro tokenizaci aktiv, decentralizované finance a další distribuované aplikace. Několik hlavních platforem jako Ethereum, Monero, EOS, Cardano, Terra, Cosmos, Avalanche, Algorand, Near, Celo a Polkadot nabízí odlišné funkce a vývojová prostředí, díky nimž jsou atraktivní pro různé aplikace, případy použití a koncové uživatele [5, 11, 4, 21, 20, 23, 24, 19, 6, 14, 25]. Užitečné funkce každé nové platformy jsou však v současnosti nabízeny méně než 1 % uživatelů ekosystému, konkrétně držitelům nativního tokenu na dané platformě. Můžeme vývojářům platforem umožnit snadno připojit své blockchainy do jiných ekosystémů? Můžeme tvůrcům aplikací umožnit stavět na nejlepší platformě pro jejich potřeby a přitom stále komunikovat napříč mnoha blockchainovými ekosystémy? Můžeme uživatelům umožnit interakci s jakoukoli aplikací na jakémkoli blockchainu přímo z jejich peněženek?

Abychom překlenuli blockchainové ekosystémy a umožnili aplikacím komunikovat mezi nimi bez tření, navrhujeme síť Axelar. Validátoři společně provozují byzantský konsensus protokol a spouštějí protokoly usnadňující cross-chain požadavky. Kdokoli se může připojit k síti, zúčastnit se a používat ji. Základní síť je optimalizována pro vysoké požadavky na bezpečnost a živost, jedinečné pro cross-chain požadavky. Síť Axelar také zahrnuje sadu protokolů a API. Základní protokoly jsou:

- Cross-Chain Gateway Protocol (CGP). Tento protokol je analogický protokolu Border Gateway na Internetu. Tento protokol se používá k propojení více autonomních blockchainových ekosystémů a je zodpovědný za směrování napříč nimi. Blockchainy nepotřebují „mluvit žádným vlastním jazykem“, vývojáři jejich platforem nemusí provádět žádné vlastní změny na svých řetězcích a jejich řetězce lze snadno zapojit do globální sítě.
- Cross-Chain Transfer Protocol (CTP). Tento protokol je analogický protokolům na úrovni aplikace File Transfer, Hypertext Transfer Protocols na internetu. Jedná se o zásobník protokolů na aplikační úrovni, který je umístěn nad směrovacími protokoly (jako je CGP a další směrovací technologie). Vývojáři aplikací mohou připojit své dapps k libovolnému řetězci a provádět meziřetězcové požadavky. Uživatelé mohou používat protokol CTP k interakci s aplikacemi v jakémkoli řetězci pomocí jednoduchých volání API analogických požadavkům HTTP GET/POST. Vývojáři mohou zamykat, odemykat a přenášet aktiva mezi libovolnými dvěma adresami napříč všemi blockchainovými platformami, spouštět spouštěče aplikací napříč řetězcem (např. dapps v řetězci A, může aktualizovat

jeho stav, pokud nějaká jiná aplikace v řetězci B splňuje některá kritéria vyhledávání (úroková sazba *> X*)) a provádět obecné požadavky napříč řetězci mezi aplikacemi napříč řetězci (inteligentní smlouva v řetězci A může volat k aktualizaci stavu inteligentní smlouvy v řetězci B). Tento protokol umožňuje skládání programů napříč blockchainovými ekosystémy.

Axelar network nabízí následující výhody:

- *Pro tvůrce blockchainové platformy*: Schopnost snadno připojit své blockchainy do všech ostatních blockchainových ekosystémů. Pro připojení k síti je třeba v řetězci nastavit pouze prahový účet.
- *Pro stavitele dapps*: Tvůrci aplikací mohou hostovat své dapp kdekoli, zamykat, odemykat, přenášet prostředky a komunikovat s aplikacemi v jakémkoli jiném řetězci prostřednictvím CTP API.
- *Pro uživatele*: Uživatelé mohou komunikovat se všemi aplikacemi v celém ekosystému přímo ze svých peněženek.

Platforma pro stavitele. Konečně, Axelar network je platforma pro vývojáře a globální komunitu. Její model řízení je otevřený komukoli. Vývojáři mohou navrhovat nové integrační body, směrování a protokoly na úrovni aplikací a uživatelé se mohou rozhodnout, zda je přijmou hlasováním o návrzích, a pokud budou schváleny, validátoři přijmou změny.

1.1 Stávající řešení interoperability

Předchozí pokusy vyřešit interoperabilitu napříč blockchainy spadají do jedné ze čtyř kategorií: centralizované burzy, interoperabilní ekosystémy, zabalená aktiva a token bridge. Tyto přístupy stručně shrnujeme níže.

Centralizované systémy. potřeby pro ekosystém. Dnes jsou centralizované systémy jedinými skutečně škálovatelnými řešeními interoperability Mohou poměrně snadno vypsat jakékoli aktivum nebo na palubě jakékoli platformy. Nicméně, je známo, že centralizované systémy mají různé bezpečnostní problémy a nejsou dost dobré na to, aby poháněly vznikající decentralizovaný finanční systém, který vyžaduje robustní zabezpečení, transparentnost a otevřenou správu. Samy o sobě nemohou pohánět decentralizované aplikace, jak rostou.

Rozbočovače interoperability. Projekty jako Cosmos, Polkadot, Ava labs řeší interoperabilitu mezi nimi *postranní řetězce* nativní pro jejich ekosystémy pomocí vlastních meziřetězcových komunikačních protokolů [23, 25, 24]. Například lze roztočit postranní řetězec (Cosmos Zone), který může komunikovat s Cosmos Hubem. Postranní řetězec musí být založen na konsensu Tendermint a musí mluvit protokolem, který nativně rozumí Cosmos Hub. Napojení na další blockchainy a ekosystémy, které mluví různými jazyky, je ponecháno na externích technologiích.

Párové mosty. Zabalená aktiva (např. zabalené bitcoiny) se snaží zaplnit chybějící mezeru v interoperabilitě napříč řetězci v ekosystému. Jedním příkladem je tBTC [9], což je vlastní protokol, kde se k zabezpečení převodů používá chytrá kombinace chytrých smluv a kolaterálu. Sestavení těchto řešení vyžaduje značné technické úsilí – pro každý pár řetězců musí vývojáři vytvořit nový inteligentní kontrakt na cílový řetězec, který analyzuje důkazy stavu z původního řetězce (podobně jako každý postranní řetězec by v zásadě mohl analyzovat stav jiných řetězců) . Pomocí tohoto přístupu bylo nasazeno pouze několik mostů. Tyto přístupy se neškálují, když jeden ze základních blockchainů chce upgradovat svá pravidla konsensu nebo formát transakce. Je to proto, že všechny chytré smlouvy, které závisí na stavu těchto řetězců, by musely být upgradovány. Je také nutné zřídit validátory a vyžadovat od nich, aby zablokovali různá aktiva, aby se překolateralizoval jakýkoli převod aktiv,

Viděli jsme také několik dalších jednoúčelových mostů od vývojářů platforem, které přepisují logiku přechodu stavu v inteligentních smlouvách, aby přemostily do jiných ekosystémů [1, 7]. Trpí mnoha problémy se škálovatelností, neumožňují ekosystému škálovat jednotně a zavádějí další závislosti pro aplikace. Pokud se například změní jedna platforma, bude nutné upgradovat všechny chytré smlouvy na všech mostech. Tento

nakonec uvede ekosystém do patové situace, kde nikdo nebude moci upgradovat. Konečně, pokud jeden jednoúčelový most spojuje platformy A a B a druhý jednoúčelový most spojuje B a C, neznamená to, že aplikace na A budou moci komunikovat s aplikacemi na C. Možná bude potřeba vytvořit další jednoúčelový most. účelový most nebo rewire aplikační logika.

Mezi další pokusy o řešení interoperability patří federovaná orákula (např. Ren [8]) a interoperabilní blockchainy specifické pro aplikaci [10].

Abychom to shrnuli, stávající řešení pro interoperabilitu vyžadují náročnou inženýrskou práci jak od vývojářů platforem, tak od tvůrců aplikací, kteří musí rozumět různým komunikačním protokolům, aby mohli komunikovat napříč každým párem ekosystémů. A tak interoperabilita v dnešním blockchainovém prostoru prakticky neexistuje. Na konci dne se vývojáři platforem chtějí zaměřit na vytváření platforem a optimalizovat je pro jejich případy použití a být schopni se snadno připojit k jiným blockchainům. A vývojáři aplikací chtějí stavět dapps na nejlepších platformách pro jejich potřeby a přitom stále využívat uživatele, likviditu a komunikovat s ostatními dapps v jiných řetězcích.

2 Hledání škálovatelné mezičetězové komunikace

V jádru mezičetězcová komunikace vyžaduje, aby heterogenní sítě našly schopnost komunikovat pomocí stejného jazyka. Abychom to vyřešili, vysvětlíme sadu protokolů Axelar, popíšeme její vlastnosti na vysoké úrovni a vysvětlíme, jak tyto vlastnosti řeší jádro škálovatelné cross-chain komunikace.

1. *"Plug-and-play" integrace.* Od tvůrců blockchainových platforem by se nemělo vyžadovat, aby prováděli těžké inženýrské nebo integrační práce, aby mluvili nějakým „vlastním jazykem" na podporu cross-chainu. Crosschain protokol by měl být schopen bez tření připojit jakýkoli stávající nebo nový blockchain. Nová aktiva by měla být přidávána s minimálním úsilím.
2. *Křížové směrování.* Funkce, jako je zjišťování síťových adres, směrovacích cest a sítí, jsou jádrem internetu a usnadňují je BGP a další směrovací protokoly. Podobně, abychom usnadnili komunikaci napříč blockchainovými ekosystémy, musíme podporovat zjišťování adres napříč nimi, aplikací a směrování.
3. *Podpora upgradovatelnosti.* Pokud se změní jeden z blockchainových ekosystémů, nemělo by to mít vliv na interoperabilitu ostatních blockchainů. Systém potřebuje rozpoznat aktualizace a k jejich podpoře by mělo být vyžadováno minimální úsilí (tj. neměla by se přepisovat žádná „logika přechodu stavu" a aplikace by se neměly přerušovat).
4. *Jednotný jazyk pro aplikace.* Aplikace potřebují jednoduchý protokol pro zamykání, odemykání, přenos a komunikaci s jinými aplikacemi bez ohledu na to, ve kterém řetězci se nacházejí. Tento protokol musí být řetězově agnostický a musí podporovat jednoduchá volání, analogická protokolům HTTP/HTTPS, které umožňují uživatelům a prohlížečům komunikovat s libovolným webovým serverem. S tím, jak se ke směrovacím protokolům nižší úrovně připojuje více sítí a aktiv, by je aplikace měly být schopny používat pro komunikaci bez přepisování svých softwarových balíků.

Dále si shrneme bezpečnostní požadavky, které musí tyto protokoly splňovat.

1. *Decentralizovaná důvěra.* Síť a protokoly musí být decentralizované, otevřené a umožnit všem spravedlivou účast.
2. *Vysoká bezpečnost.* Systém musí splňovat vysoké záruky bezpečnosti. Systém potřebuje zachovat bezpečnost aktiv a stavu, jak jej zpracuje cross-chain síť.
3. *Vysoká živost.* Systém musí splňovat vysoké záruky životnosti pro podporu aplikací využívajících jeho cross-chain funkcí.

Uspokojit podmnožinu těchto vlastností je snadné. Například je možné vytvořit federovaný multisig účet s jejich přáteli a uzamknout/odemknout aktiva na odpovídajících řetězcích. Takové systémy jsou ze své podstaty zranitelné vůči tajným dohodám a útokům cenzury a postrádají náležité pobídky pro validátory, aby je chránili. Vytvoření decentralizované sítě a sady protokolů, do kterých se může zapojit kdokoli a přitom je správně motivován, může umožnit komunikaci napříč řetězci bez tření, ale řešení tohoto problému je obtížným problémem, který vyžaduje pečlivou kombinaci konsenzu, kryptografických protokolů a protokolů pro návrh mechanismu.

3 Axelární síť

Axelar network poskytuje jednotné řešení cross-chain komunikace, které splňuje potřeby jak vývojářů platforem – není od nich vyžadována žádná integrační práce, tak tvůrců aplikací – jeden jednoduchý protokol a API pro přístup ke globální likviditě a komunikaci s celým ekosystémem.

Síť Axelar se skládá z decentralizované sítě, která přemosťuje blockchainové ekosystémy, které mluví různými jazyky, a sadu protokolů s API navrchu, což aplikacím usnadňuje provádění požadavků napříč řetězci. Síť propojuje stávající samostatné blockchainy, jako jsou bitcoiny, Stellar, Terra, Algorand, a centra interoperability, jako jsou řešení jako Cosmos, Avalanche, Ethereum a Polkadot. Naším posláním je umožnit vývojářům aplikací snáze vytvářet takové aplikace pomocí univerzálního protokolu a API, aniž by pod nimi zaváděli své proprietární cross-chain protokoly nebo přepisovali aplikace při vývoji nových mostů. Za tímto účelem jsme navrhli sadu protokolů, která zahrnuje Cross-Chain Gateway Protocol (viz část6) a Cross-Chain Transfer Protocol (viz oddíl 7).

Základní součástí sítě jsou decentralizované protokoly. Validátoři společně udržují síť Axelar a provozují uzly, které zajišťují blockchain Axelar. Jsou voleni prostřednictvím procesu delegování uživateli. Validátoři dostávají hlasovací právo pro-rata podle podílu, který jim byl delegován. Validátoři dosáhnou konsensu ohledně stavu více blockchainů, ke kterým je platforma připojena. Blockchain je zodpovědný za údržbu a provoz meziřetězcových směrovacích a přenosových protokolů. Pravidla správy umožňují účastníkům sítě přijímat rozhodnutí o protokolu, jako například, které blockchainy přemostit a která aktiva podporovat.

Axelar blockchain se řídí modelem Delegated Proof-of-Stake (DPoS) podobným Cosmos Hub. Uživatelé volí validátory, kteří musí spojit svůj podíl, aby se mohli účastnit konsensu a udržovat vysoce kvalitní služby. Model DPoS umožňuje údržbu velké sady decentralizovaných validátorů a robustní pobídky, které zaručují, že validátoři jsou zodpovědní za udržování mostů a sdílení kryptografických prahových schémat. V rámci konsensu spouštějí validátoři lehký klientský software jiných blockchainů, což jim umožňuje ověřit stav jiných blockchainů. Validátoři nahlásí tyto stavy do blockchainu Axelar a jakmile jich nahlásí dostatek, stav Bitcoinu, Etherea a dalších řetězců se zaznamená na Axelar.

Následně je základní vrstva Axelar informována o stavu externích blockchainů v kterémkoli okamžiku a vytváří „příchozí mosty" z jiných blockchainů. Validátoři společně udržují*prahové podpisové účty* na jiných blockchainech (např. 80 % validátorů musí schválit a spolupodepsat jakoukoli transakci z toho), což jim umožňuje uzamknout a odemknout aktiva a stav napříč řetězci a zveřejňovat stav na jiných blockchainech, „odchozích mostech". Celkově lze na síť Axelar nahlížet jako na a*decentralizovaný crosschain oracle pro čtení/zápis*.

Zbývající část dokumentu popisuje přípravné práce a stavební bloky za sítí (oddíl 4), některé technické detaily sítě (oddíl 5), protokol cross-chain brány (oddíl 6) a protokol pro přenos mezi řetězci (oddíl 7).

4 Předběžná utkání

4.1 Notace a předpoklady

Nechat $PROTI_r$ označují sadu Axelar validátorů v kole R. Každý validátor má a *hmotnost*, číslo v (0, 1] označující hlasovací právo tohoto konkrétního validátora. Součet vah všech validátorů je 1. Validátor je *opravit* pokud provozuje uzel, který je v souladu s pravidly protokolu Axelar. Pro finalizaci bloků nebo podepisování cross-chain požadavků vyžaduje Axelar správné validátory celkové hmotnosti $> F$. Parametr nazýváme $F \in [0.5, 1]$ *prahová hodnota protokolu*.

Axelar může být založen na an *okamžitá konečná platnost Delegovaný-Proof-of-Stake* blockchain. Validátory běží *Konsenzus byzantské odolnosti vůči poruchám (BFT).* v každém kole i dokončit $i_{čt}$ blok. Jednou $i_{čt}$ blok je dokončen, je spuštěn nový konsensus BFT k dokončení $i + 1_{čt}$ blok a tak dále. Validátoři jsou voleni prostřednictvím delegování kůlu. Uživatel s určitým podílem se může rozhodnout provozovat uzel validátoru nebo delegovat svou hlasovací pravomoc (podíl) na stávajícího validátora, který pak hlasuje jeho jménem. Sada validátorů může být aktualizována, validátoři se k ní připojují/ opouštějí a uživatelé delegují/zrušují delegování svých hlasovacích práv.

Různé blockchainy fungují za různých síťových předpokladů. *Synchronní komunikace* znamená, že existuje pevná horní mez Δ času potřebného k doručení zpráv, kde Δ je známá a může být zabudována do protokolu. *Asynchronní komunikace* znamená, že doručení zpráv může trvat libovolně dlouho a je známo, že protokoly BFT nelze sestavit pro asynchronní sítě ani v přítomnosti pouze jednoho škodlivého validátoru. Předpokladem je realistický kompromis mezi synchronií a asynchronií *částečně synchronní komunikace*. Síť může být zcela asynchronní až do určité neznámé globální stabilizační doby (GST), ale poté, co se komunikace GST stane synchronní se známou horní hranicí Δ [17].

Typické blockchainy fungují za předpokladu $> F$ správné validátory. Pro synchronní sítě $F = 1/2$ je typicky nastaven, ale pro slabší předpoklad částečně synchronní sítě $F = 2/3$. Bitcoin, jeho forky a aktuální verze Etherea Proof-of-Work fungují pouze za předpokladu synchronizace. Jiné jako Algorand a Cosmos vyžadují pouze částečnou synchronizaci. Při propojování řetězců přes Axelar funguje připojení za předpokladu nejsilnějších síťových předpokladů z těchto řetězců, což je synchronizace například v případě propojení Bitcoinu a Cosmosu. Samotný Axelar blockchain funguje v částečně synchronním nastavení a tedy vyžaduje $F = 2/3$, ale je možné zlepšit požadavek na prahovou hodnotu za předpokladu, že ostatní existující blockchainy jsou bezpečné, a využít jejich zabezpečení.

4.2 Kryptografické předběžné testy

Digitální podpisy. A *schéma digitálního podpisu* je n-tic algoritmů (*Keygen, Sign, V ověřit*). *Keygen* vypíše pár kláves (*PK, SK*). Pouze majitel *SK* může podepisovat zprávy, ale kdokoli může ověřit podpisy dané veřejným klíčem *PK*. Většina blockchainových systémů dnes používá jedno ze standardních podpisových schémat, jako je ECDSA, Ed25519 nebo několik jejich variant [2, 3].

Podpisy prahu. A *prahové podpisové schéma* umožňuje skupinu n strany rozdělit tajný klíč pro schéma podpisu takovým způsobem, že jakákoli podmnožina $t + 1$ nebo více stran může spolupracovat na vytvoření podpisu, ale žádná podmnožina t nebo méně stran může vytvořit podpis nebo se dokonce dozvědět jakékoli informace o tajném klíči. Signatury vytvořené prahovými protokoly pro ECDSA a EdDSA vypadají identicky jako signatury vytvořené samostatnými algoritmy.

Schéma prahového podpisu nahrazuje schéma *Keygen* a *Podepsat* algoritmy pro běžné podpisové schéma s distribu n-stranické protokoly $T.Keygen$, $T.Podepsat$. Tyto protokoly obvykle vyžadují jak veřejný vysílací kanál, tak soukromé párové kanály mezi stranami a obvykle zahrnují několik kol komunikace. Po úspěšném absolvování $T.Keygen$ každý uživatel má podíl s_i tajného klíče SK a odpovídajícího veřejného klíče PK. The $T.Podepsat$ protokol umožňuje těmto stranám vytvořit podpis pro a

daná zpráva, která je platná pod veřejným klíčem PK. Tento podpis může ověřit kdokoli pomocí *Ověřte* algoritmu původního podpisového schématu.

4.3 Vlastnosti prahových podpisů

Existuje několik vlastností, které může mít prahové schéma, které jsou zvláště žádoucí pro decentralizované sítě:

Zabezpečení proti nepoctivé většině.Některá prahová schémata mají omezení, že jsou bezpečná pouze tehdy, když většina n strany jsou čestné. Tedy parametr prahu t musí být menší než $n/2$ [15]. Toto omezení je obvykle doprovázeno skutečností, že $2t + K$ podpisu je potřeba 1 čestných stran, i když jen $t + 1$ poškozené strany se mohou dohodnout na obnovení tajného klíče. Schémata, která tímto omezením netrpí, prý ano *zabezpečit proti nepoctivé většině*.

Jak je uvedeno dále v části 5.2, musí cross-chain platformy maximalizovat bezpečnost svých sítí a být schopny tolerovat co nejvíce zkorumpovaných stran. Proto jsou nezbytná schémata, která mohou tolerovat nepoctivou většinu.

Předběžné podpisy, neinteraktivní online podepisování. Ve snaze snížit zátěž komunikace na straně, aby podepsaly zprávu, několik posledních protokolů identifikovalo významnou část práce na podpisu, kterou lze provést „offline“, než je známa zpráva k podpisu [18, 13]. Výstup této offline fáze se nazývá a *předběžný podpis*. Na vyhotovení předpodpisů se pohlíží jako na samostatný protokol $T.Předpis$ odlišný od $T.Keygen$ a $T.Podepsat$. Výstupy předpodpisového protokolu musí strany uchovávat v tajnosti, dokud je nepoužijí ve fázi podpisu. Později, když se zpráva k podpisu stane známou, zbývá provést jen malé množství další „online“ práce $T.Podepsat$ za účelem dokončení podpisu.

Online $T.Podepsat$ fáze nevyžaduje žádnou komunikaci mezi stranami. Každá strana jednoduše provede místní výpočet zprávy a předběžného podpisu a poté oznámí svůj podíl s_i podpisu. (Jakmile jsou tyto podpisy zveřejněny, sdílejí je $s_1, \ldots, s_{t+1}$ jsou snadno kombinovány kýmkoli, aby odhalily skutečný podpis s .) Tato vlastnost se nazývá *neinteraktivní online podepisování*.

Robustnost. Prahová schémata zaručují pouze to, že podskupina škodlivých stran nemůže podepisovat zprávy nebo naučit tajný klíč. Tato záruka však nevylučuje možnost, že špatní herci mohou zablokovat všechny ostatní ve výrobě klíčů nebo podpisů. V některých schématech může způsobit škodlivé chování i jedné strany $T.Keygen$ nebo $T.Podepsat$ přerušit bez užitečného výstupu. Jedinou možností je restartovat protokol, případně s různými stranami.

Místo toho chceme decentralizované sítě $T.Keygen$ a $T.Podepsat$ uspět, pokud alespoň $t +$ Jedna ze stran je čestná, i když některé strany se zlými úmysly posílají chybné zprávy nebo zanechávají zprávy v protokolech. Tato vlastnost se nazývá *robustnost*.

Atribuce chyby. Schopnost identifikovat špatné hráče v $T.Keygen$ nebo $T.Podepsat$ je nazýván *připisování zavinění*. Bez připisování zavinění je obtížné spolehlivě vyloučit nebo potrestat špatné aktéry, v takovém případě musí náklady způsobené špatnými aktéry nést každý. Tato vlastnost je také důležitá pro decentralizované sítě, kde by škodlivé chování mělo být identifikovatelné a ekonomicky demotivované prostřednictvím seškrtávacích pravidel.

Zabezpečení v souběžných nastaveních. Podpisové schéma musí být zabezpečené v souběžném nastavení, kde paralelně může být zapojeno více instancí keygen a podepisovacích algoritmů. (Drijvers a kol. [16] například v těchto nastaveních ukázal útok proti schématům více podpisů Schnorr). Existují verze schémat ECDSA i Schnorr, které splňují tyto vlastnosti [13, 22].

ECDSA a EdDSA jsou zdaleka nejrozšířenější podpisová schémata v blockchainovém prostoru. Jako takové byly prahové verze obou schémat předmětem nedávného oživení výzkumu a vývoje. Čtenáři, kteří se zajímají o nejnovější stav techniky, se mohou obrátit na [22, 13, 18] a nedávný průzkum [12].

5 Axelární síť

5.1 Návrh otevřené cross-chain sítě

Mosty, které síť Axelar udržuje, jsou zálohovány prahovými účty, takže (téměř) všichni validátoři musí kolektivně autorizovat jakýkoli cross-chain požadavek. Návrh sítě, kde se kdokoli může podílet na zabezpečení těchto mostů, vyžaduje splnění následujících technických požadavků:

- *Otevřené členství.* Každý uživatel by měl mít možnost stát se validátorem (podle pravidel sítě).
- *Aktualizace členství.* Když validátor poctivě opustí systém, je třeba jeho klíč náležitě zrušit.
- *Pobídky a sekání.* Škodlivé validátory by měly být identifikovatelné a jejich akce musí být identifikovány a řešeny protokolem.
- *Konsensus.* Samotná schémata prahů jsou definována jako samostatné protokoly. K šíření zpráv mezi uzly potřebujeme jak vysílací, tak dvoubodové soukromé kanály. Kromě toho se validátoři musí dohodnout na nejnovějším stavu každého vyvolání prahových schémat, protože často mají více kol interakcí.
- *Správa klíčů.* Stejně jako běžní validátoři v jakémkoli PoS systému musí pečlivě střežit své klíče, tak i validátoři Axelar musí hlídat své prahové podíly. Klíče je třeba otáčet, rozdělit mezi online a offline části atd.

Axelar začíná modelem Delegated Proof-of-Stake, kde komunita volí sadu validátorů, kteří budou konsensus provádět. Všimněte si, že standardní schémata prahových hodnot zacházejí s každým hráčem stejně a v konsensu nemají žádnou představu o „váze“. Síť je proto musí přizpůsobit tak, aby zohledňovala váhu validátorů. Jednoduchým přístupem je přiřadit více prahových podílů větším validátorům. Níže jsou uvedeny tři základní funkce, které validátoři společně vykonávají.

- *Generování prahových klíčů.* Stávající algoritmy generování prahových klíčů pro standardní bloková schémata podpisů (ECDSA, Ed25519) jsou interaktivní protokoly mezi více účastníky (viz část 4). Speciální transakce v síti Axelar instruuje validátory, aby zahájily provádění tohoto stavového protokolu. Každý validátor spouští proces prahového démona, který je zodpovědný za bezpečné udržování tajného stavu. Pro každou fázi protokolu:

  1. Validátor uchovává stav protokolu ve své lokální paměti.
  2. Zavolá tajného démona, aby vygeneroval zprávy podle popisu protokolu pro ostatní validátory.
  3. Šíří zprávy buď prostřednictvím vysílání, nebo prostřednictvím soukromých kanálů dalším validátorům.
  4. Každý validátor provádí funkce přechodu stavu, aby aktualizoval svůj stav, pokračoval do další fáze protokolu a opakoval výše uvedené kroky.

  Na konci protokolu je vygenerován prahový veřejný klíč v řetězci Axelar a může být zobrazen zpět uživateli (např. pro vklady) nebo aplikaci, která generovala počáteční požadavek.

- *Podepisování prahu.* Požadavky na podepisování v síti Axelar jsou zpracovávány podobně jako požadavky na generování klíčů. Ty se vyvolají například, když chce uživatel odebrat aktivum z jednoho z těchto řetězy. interaktivních protokolů a přechod stavu mezi koly je spuštěn jako funkce zpráv šířených prostřednictvím pohledu Axelar blockchain a místní paměti každého validátoru.

- *Zpracování změn členství Validator.* Sada validátorů se musí pravidelně střídat, aby se k ní mohly připojit nové zúčastněné strany. Po aktualizaci sady validátorů musíme aktualizovat klíč prahu, který bude sdílen v nové sadě. Pokud bychom tedy umožnili komukoli se kdykoli připojit, museli bychom velmi často aktualizovat prahový klíč. Abychom tomu zabránili, vždy střídáme validátory T bloky. V intervalech od T kola, sada $PROTI_R$ a prahový klíč jsou pevné. V každém kole je to celý násobek parametru T, aktualizujeme sadu validátorů následovně:

1. V každém kole R, stav Axelar sleduje aktuální sadu validátorů $PROTI_R$. $PROTI_{R+1} = PROTI_R$ ledaže $R + 1$ je násobkem T.
2. Během kol $((já - 1)T, iT]$, uživatelé posílají zprávy o spojení/rozpojení.
3. Na konci kola to, tyto zprávy jsou aplikovány na $PROTI_{iT-1}$ dostat $PROTI_{to}$.

- *Generování prahových klíčů a podepisování za přítomnosti rotujících validátorů.* Axelar blockchain může při kole vydat požadavek na nový klíč nebo prahový podpis R. Proces podepisování trvá déle než jedno kolo a my nechceme zpomalovat konsensus, proto požadujeme, aby byl podpis vyroben před kolem $R + 10$ startů. Zejména validátoři začínají kolo $R + 10$ pouze po shlédnutí certifikátu pro kolo $R + 9$ a podpis pro každý klíčový gen/požadavek na podpis vydaný v kole R. Výsledek celého kola R požadavky musí být zahrnuty do bloku $R + 11$. Jinými slovy, kolo R blokový návrh, který neobsahuje výsledky z kola $R - 11$ je považován za neplatný a validátoři o něm nehlasují. Aby bylo zajištěno, že všechny prahové zprávy budou podepsány před aktualizací sady validátoru, Axelar nevydává žádné prahové požadavky během kola rovného $-1, -2, \ldots, -9$ modulů T.

5.2 Zabezpečení sítě

Bezpečnost blockchainových systémů se opírá o různé kryptografické a herní teoretické protokoly a také o decentralizaci sítě. Například v blockchainech typu proof-of-stake se mohou validátoři bez náležitých pobídek dohodnout a přepsat historii, přičemž v procesu ukradnou finanční prostředky ostatních uživatelů. V proof-of-work sítích, bez dostatečné decentralizace, je docela snadné vytvářet dlouhé forky a dvojité utrácení, jak dokázaly vícenásobné útoky na Bitcoin Gold a Ethereum Classic.

Většina výzkumu bezpečnosti blockchainu se zaměřila na suverénní řetězce. Ale jakmile budou řetězce interoperovat, je třeba zvážit nové vektory útoku. Předpokládejme například, že Ethereum mluví s malým blockchainem X prostřednictvím přímého mostu řízeného dvěma inteligentními smlouvami, jednou na Ethereu a jednou na X. Kromě technických výzev, které jsme shrnuli v části1.1, je třeba rozhodnout, co se stane, když jsou porušeny předpoklady důvěry X. V tomto případě, pokud se ETH přesunulo do X, validátoři X se mohou dohodnout, aby vytvořili historii X, kde drží všechna ETH, zveřejní podvržené konsensuální důkazy na Ethereum a ukradnou ETH. Situace je ještě horší, když je X spojeno s několika dalšími řetězci přes přímé můstky, kde pokud X forks, efekty se šíří každým mostem. Nastavení pokynů pro řízení obnovy pro každý párový most je ohromujícím úkolem pro každý jednotlivý projekt.

Síť Axelar řeší bezpečnostní problémy pomocí následujících mechanismů:

- *Maximální bezpečnost.* Axelar nastavuje bezpečnostní práh na 90 %, což znamená, že téměř všichni validátoři se budou muset dohodnout, aby mohli vybrat jakékoli prostředky, které jsou uzamčeny jeho sítí, nebo padělat státní doklady.[1]. V praxi bylo pozorováno, že validátory PoS mají velmi vysokou dobu provozuschopnosti (téměř 100 %), za předpokladu, že jsou řádně motivovány. Síť Axelar tedy bude vyrábět bloky i přes tento vysoký práh. Avšak ve vzácných případech, kdy se něco pokazí a síť se zastaví, potřebuje síť robustní záložní mechanismy pro restartování systému popsaného dále.
- *Maximální decentralizace.* Protože síť používá schémata prahových podpisů, počet validátorů může být co největší. Síť není omezena počtem validátorů, které můžeme podporovat, transakčními limity nebo poplatky, které by vznikly například používáním více podpisů v různých řetězcích, kde složitost (a poplatky) lineárně rostou s počtem validátorů.[2]
- *Robustní zpětné mechanismy.* První otázkou, kterou je třeba řešit v síti s vysokými bezpečnostními prahy, jak je uvedeno výše, je to, co se stane, když se síť sama zastaví. Předpokládejme, že samotná síť Axelar se zastaví. Můžeme mít nouzový mechanismus, který by uživatelům umožnil získat zpět své prostředky? Aby bylo možné vyřešit jakékoli potenciální zablokování samotné sítě Axelar, každý účet prahového mostu na blockchainu X, který validátoři Axelar společně ovládají, má „klíč pro nouzové odemknutí“. Tento klíč lze sdílet

[1] Konečný parametr, který bude vybrán pro síťové nasazení, lze upravit.

[2] U některých blockchainů nabízejí vícenásobné podpisy rozumnou alternativu tam, kde je množství plynu malé a podporované formáty zpráv jsou vhodné. Ale neškálují pro dvě z největších platforem, jako je Bitcoin a Ethereum.

napříč tisíci stranami a může to být dokonce vlastní klíč pro blockchain X, který je sdílen napříč komunitou tohoto řetězce. Pokud se tedy síť Axelar zablokuje, bude tento klíč fungovat jako záložní a umožní obnovu aktiv (další podrobnosti viz níže).

- *Maximální decentralizace záložních mechanismů.* Tento nouzový mechanismus zahrnuje sekundární *obnovovací set* uživatelů, do kterého se může bez jakýchkoli nákladů zapojit opravdu každý. Tito uživatelé nemusí být online, spouštět uzly ani se navzájem koordinovat. Jsou „povoláni do služby" pouze v případě, že se síť Axelar zastaví a nemůže se zotavit. Bezpečnost sítě je zvýšena velmi vysokým prahem na primární sadě validátorů a maximálně decentralizovanou sekundární sadou obnovy.
- *Sdílené řízení.* Síť Axelar řídí společný protokol. Uživatelé mohou společně hlasovat o tom, který řetězec by měl být podporován prostřednictvím své sítě. Síť také přidělí fond finančních prostředků, které lze použít k úhradě nákladů uživatelům v případě neočekávaných mimořádných událostí, a to rovněž řízených prostřednictvím protokolů řízení.

Různé bezpečnostní mechanismy jsou diskutovány níže.

Zpětné mechanismy. Když se Axelar zablokuje kvůli vysokému prahu, „klíč pro nouzové odemknutí" převezme kontrolu nad sítí. Existuje několik způsobů, jak vytvořit instanci tohoto klíče pro odemknutí, a některé řetězce/aplikace se mohou rozhodnout použít jinou variantu pro „sada pro obnovení" nebo se zcela odhlásit:[3]

- *Možnost a.* Sdílejte klíč napříč základy blockchainových projektů a renomovanými lidmi v komunitě.
- *Možnost b.* Sdílejte mezi stranami zvolenými prostřednictvím mechanismu delegovaných PoS.
- *Možnost c.* Pro účty spravující aktiva a informace pro řetězec/aplikaci X sdílejte vlastní klíč mezi zainteresovanými stranami/validátory X. Za předpokladu, že X má zavedeny mechanismy řízení, lze stejné mechanismy řízení použít k určení postupu, pokud se Axelar zastaví.

Nyní, s ohledem na identity uživatelů pro obnovení a jejich veřejné klíče, jednoduchý protokol generuje sdílené položky klíče pro obnovení, které nikdo nezná. Uživatelé sady pro obnovu navíc nemusí být online, dokud nejsou vyzváni k obnově prostřednictvím mechanismů řízení. Podle standardních distribuovaných protokolů generování klíčů sdílí každý validátor Axelar náhodnou hodnotu. Tajný klíč pro obnovení je generován sečtením těchto hodnot. Namísto sčítání jsou všechny sdílené položky zašifrovány veřejnými klíči uživatelů obnovy a poté homomorfně sečteny (to předpokládá aditivně homomorfní šifrování a další vrstvu nulových znalostí, obojí lze snadno získat). Výsledkem tohoto protokolu je obnovovací veřejný klíč *RPK* a potenciálně tisíce šifrování (pod veřejnými klíči uživatelů obnovy) sdílených položek odpovídajícího tajného klíče $Enc(s_i)$, které jsou distribuovány jejich vlastníkům (např. zveřejněny na řetězu). Kontrakty Axelar bridge zahrnují možnost získat zpět finanční prostředky pomocí *RPK* za určitých podmínek. Konečně je také možné aktualizovat tento obnovovací klíč a dokonce změnit skupinu uživatelů držících jeho akcie, aniž by to vyžadovalo jakoukoli práci od zúčastněných akcionářů.

Pokud se řetěz X, který je připojen k Axelar, přeruší, existuje několik možností:

- Stanovte limity na hodnotu aktiv v USD, která mohou být přesunuta dovnitř/ven z X v kterýkoli den. Škodlivý řetězec X tedy může ukrást jen malý zlomek všech aktiv, která jsou k němu připojena, dříve, než to zjistí validátoři Axelar a než se spustí mechanismy řízení z následujících odrážek.
- Modul Axelar governance lze použít k hlasování o tom, co se v těchto situacích stane. Pokud se například vyskytne benigní chyba a komunita restartuje X, Axelar governance může rozhodnout o restartu připojení tam, kde skončilo.
- Pokud se ETH přesunulo na X, vlastní klíč pro obnovu Etherea může určit, co se stane s aktivy ETH.

[3] Finální nasazení v síti Axelar bude dokončeno těsně před spuštěním sítě.

6 Cross-Chain Gateway Protocol (CGP)

V této části vysvětlíme protokol cross-chain brány a směrovací mechanismy na dvou základních příkladech společných pro potřeby mnoha aplikací:

Synchronizace stavu (oddíl 6.2). Zveřejněte informace o stavu zdrojového blockchainu *S* do stav cílového blockchainu *D*.

(Například zveřejněte hlavičku bitcoinového bloku do blockchainu Ethereum.)

Převod majetku (oddíl 6.3). Převeďte digitální aktivum z *S* na *D* a zase zpět.

(Například převeďte bitcoiny z bitcoinového blockchainu do blockchainu Ethereum a poté zpět do bitcoinového blockchainu.)

Pro jednoduchost předpokládáme tento řetězec *D* má alespoň minimální podporu pro chytré smlouvy, ale *S* může být jakýkoli blockchain.

6.1 Účty v jiných řetězcích

Pro překlenutí různých řetězců jsou v každém řetězci vytvořeny prahové účty, které řídí tok hodnot a informací napříč nimi. Pro řetěz*Řetěz*, označte účet $Řetěz_{Axelar}$.

Bitcoinový účet. Pro bitcoiny a další neinteligentní smluvní řetězce vytvoří validátory Axelar prahový klíč ECDSA podle oddílu 5.1. Tento klíč ovládá účet ECDSA na bitcoinech a je cílovou adresou, kam uživatelé posílají vklady. Personalizované prahové klíče mohou být vytvořeny na žádost uživatele. Klíč může být pravidelně aktualizován a nejnovější klíč a personalizované klíče lze nalézt dotazem na uzel Axelar.

Threshold bridge účet na řetězcích s chytrými kontrakty. Řetěz označte SC. validátory vytvoří prahový klíč ECDSA nebo ED25519 podle sekce5.1, podle toho, jaký typ klíče řetěz podporuje. Tento klíč označujemePK_{Axelar}, kdy není nejednoznačnost, o jaký řetězec se jedná. Tento klíč ovládá účet inteligentní smlouvy na SC, označený jakoSC_{Axelar}a jakákoli aplikace na SC může dotazovat SC_{Axelar} zjistit adresu PK tohoto klíče. Tímto způsobem může jakákoli SC aplikace rozpoznat zprávy podepsané uživatelemSK_{Axelar}. Protokol také musí počítat s rotujícími hodnotamiPK_{Axelar}. To se děje následovně:

1. Inicializujte SC_{Axelar} na SC. Ukládá sePK_{Axelar} jako součást jeho stavu, který je inicializován jako jeho genesis hodnota na Axelar. SC_{Axelar} obsahuje i pravidla pro aktualizaci PK.
2. Aktualizovat PK_{Axelar}, transakce ve formátu (*aktualizace,* $PK_{Nový}$) musí být předložen s podpisem z aktuálního SK_{Axelar}. Pak se uzavírá smlouva$PK_{Axelar} = PK_{Nový}$.
3. Pokaždé, když validátory aktualizují prahový klíč pro SC od PK_i na PK_{i+1}, Axelar požadavky, které používají validátoři SK_i k podpisu (*aktualizace,* PK_{i+1}). Následně je tento podpis zaslánSC_{Axelar} který aktualizuje PK_{Axelar}.

6.2 Synchronizace stavu

Nechat q_S označují libovolnou otázku o stavu řetězce *S*. Příklady takových otázek:

- *"V jakém blokovém kole, pokud vůbec, se objevil transakční tx?*
- *"Jakou hodnotu má určité datové pole?"*
- *"Jaký je Merkle root hash celého státu? S na bloku 314159?"*

Nechat A_S označte správnou odpověď na q_S a předpokládejme, že to požaduje koncový uživatel nebo aplikace A_S být zveřejněn v řetězci *D*. Axelar síť splňuje tento požadavek následovně:

1. Uživatel zadá požadavek q_S na jednom z mostních účtů (které následně vyzvednou validátoři) nebo přímo na blockchain Axelar.

2. V rámci konsensu Axelar musí každý validátor provozovat software uzlů pro řetězce S, D. Validátory Axelar se dotazují na API svého řetězce S uzlový software pro odpověď A_S a nahlaste odpověď řetězci Axelar.

3. Jednou $> F$ vážení validátoři hlásí stejnou odpověď v kole R Axelar žádá validátory, aby podepsali A_S.

4. Pomocí prahové kryptografie se validátoři podepisují A_S. Podpis je součástí bloku $R + 11$.

5. Podepsanou hodnotu může převzít kdokoli A_S z bloku $R + 11$ a pošlete to na D.

6. Požadavek byl vyřízen. Jakákoli aplikace zapnutá D nyní může mít podepsanou hodnotu A_S, dotaz D_{Axelar} pro nejnovější PK_{Axelar} a ověřte, že podpis A_S odpovídá PK_{Axelar}. Validátoři také zveřejňují A_S na účet mostu na řetězu D, které aplikace mohou načíst.

6.3 Křížový převod aktiv

Síť umožňuje mezičetězcové přenosy digitálních aktiv rozšířením pracovního toku synchronizace stavu sekce 6.2.

Dostatečná zásoba fixovaných S tokeny jsou vytištěny a kontrolovány D_{Axelar} při jeho inicializaci. Předpokládejme, že uživatel požaduje výměnu X množství tokenů ve zdrojovém řetězci S pro X množství fixovaného -S tokeny v cílovém řetězci D, k uložení u a D-adresa w_D dle volby uživatele. Představujeme plně obecný pracovní postup, který podporuje libovolné zdrojové řetězce S—dokonce i řetězce, jako je bitcoin, které nepodporují chytré smlouvy:

1. Uživatel (nebo aplikace jednající jménem uživatele) odešle žádost o převod (x, w_D) na účet prahového mostu, který je následně směrován do sítě Axelar.

2. Axelar validátory používají prahovou kryptografii ke společnému vytvoření nové adresy pro vklad d_S pro S. Zveřejňují d_S na blockchain Axelar.

3. Uživatel (nebo aplikace jednající jménem uživatele) se učí d_S sledováním blockchainu Axelar. Uživatel odešle X množství S-tokeny na adresu d_S přes obyčejný S-transakce TX_S pomocí svého oblíbeného softwaru pro řetěz S.

   (Vzhledem k vlastnosti prahu d_S, žetony nelze utratit d_S ledaže by se k tomu koordinoval prahový počet validátorů.)

4. TX_S je zveřejněno na Axelar. Validátoři se dotazují na API svého řetězce S uzlový software pro existenci TX_S a pokud je odpověď „pravda“, nahlaste odpověď řetězci Axelar.

5. Jednou $> F$ vážené validátory hlásí „pravda“ pro TX_S na kole R, Axelar žádá validátory, aby podepsali transakci A_D který posílá X množství fixovaného -S tokeny od D_{Axelar} na w_D.

6. Pomocí prahové kryptografie se validátoři podepisují A_D. Podpis je součástí bloku $R + 11$.

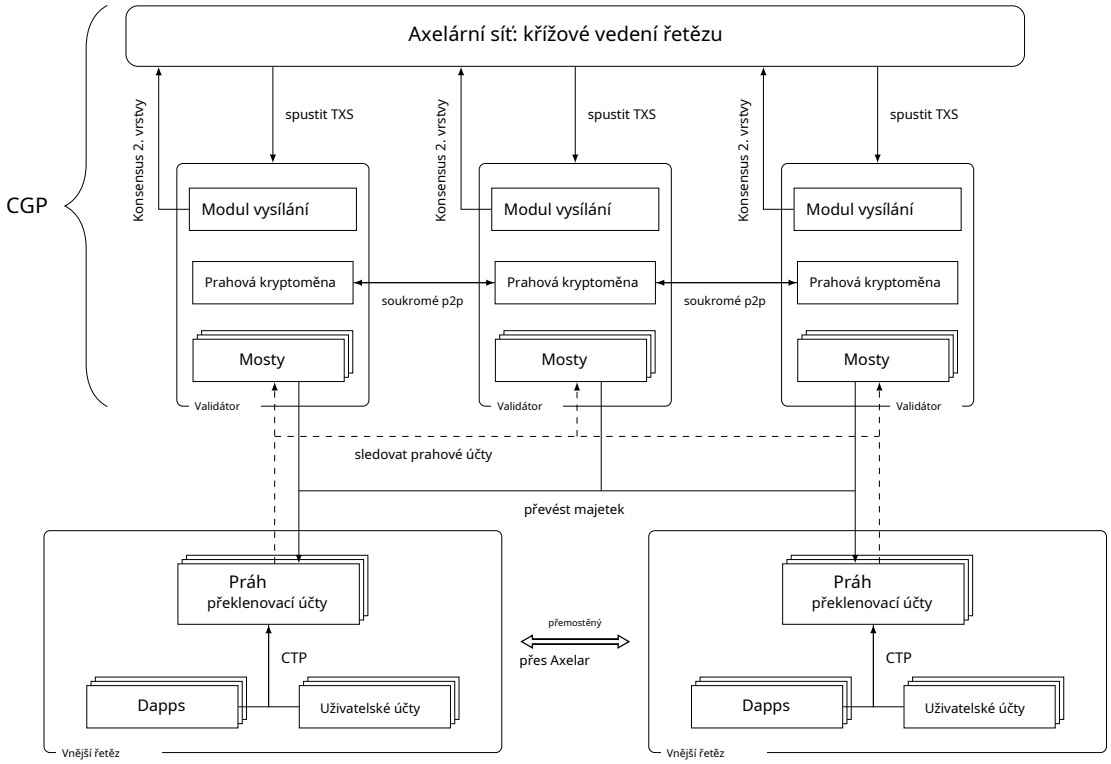
7. Podepsanou hodnotu může převzít kdokoli A_D z bloku $R + 11$ a pošlete to na D.

8. Požadavek byl vyřízen jednou A_D je zveřejněno na D převod je zpracován.

Nyní předpokládejme, že uživatel požaduje vyplacení X' množství zabaleného -S žetony z řetězce D zpět k řetězu S, k uložení u a S-adresa w_S dle volby uživatele. Pracovní postup je následující:

1. Uživatel zahájí požadavek na přenos (X', w_S) uložením X' množství zabaleného -S žetony do C_D přes obyčejný D-transakce pomocí jejího oblíbeného softwaru pro řetěz D.

2. (X', w_S) je zveřejněn na Axelar. Validátoři se dotazují na API svého řetězce D software uzlu pro existenci (X', w_S) a pokud je odpověď „pravda“, nahlaste odpověď řetězci Axelar.



Obrázek 1: Schéma součásti

3. Jednou $> F$ vážené validátory hlásí „pravda“ pro (X', w_S) v kole R, Axelar žádá validátory, aby podepsali transakci A_S který posílá X' množství S tokeny od S_{Axelar} na w_S.
4. Pomocí prahové kryptografie se validátoři podepisují A_S. Podpis je součástí bloku $R + 11$.
5. Podepsanou hodnotu může převzít kdokoli A_S z bloku $R + 11$ a pošlete to na S.
6. Požadavek byl vyřízen jednou A_S je zveřejněno na S převod je zpracován.

Mezi další požadavky podporované směrovací vrstvou CGP patří zamykání, odemykání nebo přenos aktiv napříč řetězci.

Dosažení toku atomových křížových transakcí. V závislosti na typu cross-chain požadavku se Axelar snaží zajistit, aby byly odpovídající transakce provedeny ve více řetězcích nebo žádné. K tomu může být každý požadavek v Axelar blockchainu v jednom z následujících stavů:*(inicializováno, čeká na vyřízení, dokončeno, vypršel časový limit)*. Pokud *Časový limit* ve fázi čekající na vyřízení požadavek vrátí chybový kód. Začínají také některé události časového limitu a *vrácení peněz* událost: například, pokud je třeba převést aktivum z jednoho řetězce do aktiva v jiném řetězci, pokud přijímající řetězec transakci nezpracoval, je aktivum vráceno zpět původnímu uživateli.

7 Cross-Chain Transfer Protocol (CTP)

CTP je protokol na aplikační úrovni, který aplikacím usnadňuje využití cross-chain funkcí. Vysvětlujeme integraci zaměřením na funkce převodu aktiv (např. používané v DeFi). Tyto aplikace se obvykle skládají ze tří hlavních komponent: front-end GUI, chytré kontrakty na jednom řetězci a zprostředkovatelský uzel, který účtuje transakce mezi front-endem a chytrými kontrakty. Front-endy komunikují s peněženkami uživatele a přijímají vklady, zpracovávají výběry atd. Aplikace mohou využívat cross-chain funkce

voláním CTP dotazů analogických metodám HTTP/HTTPS GET/POST. Tyto dotazy jsou následně vyzvednuty vrstvou CGP k provedení a výsledky jsou vráceny zpět uživatelům.

- *CTP dotazy*. Vývojáři aplikací mohou hostovat své aplikace v jakémkoli řetězci a integrovat své chytré smlouvy s účty prahového mostu pro provádění CTP dotazů.
- *Účty prahového mostu*. Předpokládejme, že vývojář aplikace staví své smlouvy na řetězci A. Pak by odkazoval na smlouvy prahového mostu, aby získal podporu napříč řetězci. Tato smlouva umožňuje aplikacím:
  - Zaregistrujte blockchain, se kterým by chtěl komunikovat.
  - Zaregistrujte na tomto blockchainu aktiva, která by chtěl využít.
  - Provádějte operace nad aktivy, jako je přijímání vkladů, zpracování výběrů a další funkce (podobné, řekněme, smluvním hovorům ERC-20).

Předpokládejme prominentní aplikaci DeFi, MapleSwap, která nativně sídlí v registrech řetězce A s účtem prahového mostu. Validátoři Axelar společně spravují samotnou smlouvu v odpovídajícím řetězci. Předpokládejme, že uživatel chce vložit vklad do obchodního páru mezi aktivy X a Y, které se nacházejí napříč dvěma řetězci. Poté, když uživatel odešle takový požadavek, je směrován přes účet prahového mostu do sítě Axelar ke zpracování. Ve formuláři se provedou následující kroky:

1. Síť Axelar chápe, že tato aplikace se zaregistrovala pro cross-chain podporu napříč aktivy. Generuje klíč vkladů využívající prahovou kryptografii a konsensus pro uživatele na odpovídajících řetězcích A a B.
2. Přidružené veřejné klíče se vrátí do aplikace a zobrazí se uživateli, který může používat své oblíbené peněženky k odesílání vkladů. Odpovídající tajný klíč je sdílen všemi validátory Axelar.
3. Když jsou vklady potvrzeny, Axelar aktualizuje svůj cross-chain adresář, aby zaznamenal, že uživatel na odpovídajících řetězcích vložil tato aktiva.
4. Validátory Axelar spouštějí protokoly s více stranami pro generování podpisu prahu, který umožňuje aktualizaci účtu prahového mostu v řetězci A, kde se aplikace nachází.
5. Dotaz CTP je poté vrácen inteligentním kontraktům aplikace DeFi, které mohou aktualizovat svůj stav, aktualizovat vzorce výnosů, směnné kurzy nebo provádět další podmínky související se stavem aplikace.

V průběhu tohoto procesu síť Axelar na vysoké úrovni funguje jako decentralizované oracle pro čtení/zápis s křížovým řetězcem, CGP je vrstva směrování mezi řetězci a CTP je aplikační protokol.

Dodatečné cross-chain požadavky. CTP podporuje obecnější cross-chain mezi aplikacemi napříč blockchainy, jako jsou:

- Proveďte služby názvů veřejných klíčů (PKNS). Toto je univerzální adresář pro mapování veřejných klíčů na telefonní čísla/twitter úchyty (několik projektů, jako je Celo, poskytuje tyto funkce v rámci svých platforem).
- Mezičetězcové spouštěče aplikací. Aplikace v řetězci A může aktualizovat svůj stav, pokud některá jiná aplikace v řetězci B splňuje vyhledávací kritéria (úroková sazba $< X$).
- Inteligentní skládání smluv. Inteligentní smlouva v řetězci A může aktualizovat svůj stav na základě stavu smluv v řetězci B nebo spustit akci k aktualizaci inteligentní smlouvy v řetězci B.

Na vysoké úrovni mohou být tyto požadavky zpracovány, protože společně protokoly CTP, CGP a Axelar network mohou předávat a zapisovat libovolné ověřitelné informace o stavu napříč blockchainy.

8 Shrnutí

Během příštích let budou na více blockchainových ekosystémech postaveny významné aplikace a aktiva. Axelární síť lze použít k zapojení těchto blockchainů do jednotné komunikační vrstvy napříč řetězci. Tato vrstva poskytuje směrovací protokoly a protokoly na úrovni aplikací, které splňují požadavky tvůrců platforem i vývojářů aplikací. Vývojáři aplikací mohou stavět na nejlepších platformách pro své potřeby a využívat jednoduchý protokol a API pro přístup ke globální cross-chain likviditě, uživatelům a komunikaci s ostatními řetězci.

Reference

[1] Althea peggy. https://github.com/cosmos/peggy. [Citováno na stránce 2.]

[2] Deterministické použití algoritmu digitálního podpisu (dsa) a algoritmu digitálního podpisu eliptické křivky (ecdsa). https://tools.ietf.org/html/rfc6979. [Citováno na stránce 5.]

[3] Algoritmus digitálního podpisu podle Edwardsovy křivky (eddsa). https://tools.ietf.org/html/rfc8032. [Citováno dne strana 5.]

[4] Technická bílá kniha Eos.io v2. https://github.com/EOSIO/Documentation/blob/master/TechnicalWhitePaper.md. [Citováno na straně 1.]

[5] Ethereum: Bezpečná decentralizovaná zobecněná účetní kniha transakcí. https://ethereum.github.io/yellowpaper/paper.pdf. [Citováno na stránce 1.]

[6] Téměř bílý papír. https://near.org/papers/the-official-near-white-paper/. [Citováno na stránce 1.]

[7] Duhový most. https://github.com/near/rainbow-bridge. [Citováno na stránce 2.]

[8] Ren: Virtuální stroj chránící soukromí, který pohání finanční aplikace s nulovými znalostmi. // https: whitepaper.io/document/419/ren-litepaper. [Citováno na stránce 3.]

[9] tbtc: Decentralizovaný vyměnitelný token erc-20 podporovaný btc. https://docs.keep.network/tbtc/index.pdf. [Citováno na stránce 2.]

[10] Thorchain: Decentralizovaná síť likvidity. https://thorchain.org/. [Citováno na stránce 3.]

[11] Kurt M. Alonso. Z nuly na monero.https://www.getmonero.org/library/Zero-to-Monero-1-0-0.pdf. [Citováno na stránce 1.]

[12] Jean-Philippe Aumasson, Adrian Hamelink a Omer Shlomovits. Průzkum podepisování prahových hodnot ecdsa. Archiv kryptologie ePrint, zpráva 2020/1390, 2020.https://eprint.iacr.org/2020/1390. [Citováno dne strana 6.]

[13] Ran Canetti, Nikolaos Makriyannis a Udi Peled. Uc neinteraktivní, proaktivní, prahová ecdsa. Archiv kryptologie ePrint, zpráva 2020/492, 2020. https://eprint.iacr.org/2020/492. [Citováno dne strana 6.]

[14] Bílé knihy cLabs. https://celo.org/papers. [Citováno na stránce 1.]

[15] Ivan Damgård, Thomas Pelle Jakobsen, Jesper Buus Nielsen, Jakob Illeborg Pagter a Michael Bæksvang Østergård. Rychloprahové ECDSA s poctivou většinou. v*SCN*, svazek 12238 z *Poznámky z přednášek z informatiky*, strany 382–400. Springer, 2020.[Citováno na stránce 6.]

[16] Manu Drijvers, Kasra Edalatnejad, Bryan Ford, Eike Kiltz, Julian Loss, Gregory Neven a Igors Stepanovs. O zabezpečení dvoukolových více podpisů. v*IEEE Symposium o bezpečnosti a soukromí*, strany 1084–1101. IEEE, 2019.[Citováno na stránce 6.]

[17] Cynthia Dwork, Nancy Lynch a Larry Stockmeyer. Konsensus za přítomnosti částečné synchronizace. https://groups.csail.mit.edu/tds/papers/Lynch/jacm88.pdf. [Citováno na stránce 5.]

[18] Rosario Gennaro a Steven Goldfeder. Jedno kulaté prahové ecdsa s identifikovatelným přerušením. Archiv kryptologie ePrint, zpráva 2020/540, 2020.https://eprint.iacr.org/2020/540. [Citováno na stránce 6.]

[19] Yossi Gilad, Rotem Hemo, Silvio Micali, Georgios Vlachos a Nickolai Zeldovich. Algorand: Škálování byzantských dohod pro kryptoměny. Sborník příspěvků z 26. sympozia o principech operačních systémů, 2017.https://dl.acm.org/doi/pdf/10.1145/3132747.3132757. [Citováno na stránce 1.]

[20] Evan Kereiakes, Do Kwon, Marco Di Maggio a Nicholas Platias. Terra peníze: Stabilita a přijetí.

https://terra.money/Terra_White_paper.pdf. [Citováno na stránce 1.]

[21] Aggelos Kiayias, Alexander Russell, Bernardo David a Roman Oliynykov. Ouroboros: Prokazatelně bezpečný protokol blockchainu s důkazem o sázce.https://eprint.iacr.org/2016/889.pdf. [Citováno na stránce 1.]

[22] Chelsea Komlo a Ian Goldberg. Frost: Flexibilní okrouhlé optimalizované prahové signatury Schnorr. Archiv kryptologie ePrint, zpráva 2020/852, 2020.https://eprint.iacr.org/2020/852. [Citováno na stránce 6.]

[23] Jae Kwon a Ethan Buchman. Cosmos: Síť distribuovaných účetních knih. https://cosmos.network/resources/whitepaper. [Citováno na stránkách 1 a 2.]

[24] Avalanche Team. Lavinová plošina. https://www.avalabs.org/whitepapers. [Citováno na stránkách 1 a 2.]

[25] Gavin Wood. Polkadot: Vize pro heterogenní víceřetězcový rámec. https://polkadot.network/PolkaDotPaper.pdf. [Citováno na stránkách 1 a 2.]