GÖTEBORGS UNIVERSITET

Utveckling av Ethereum

Förändring av Ethereum som nyligen genomförts, är på väg att genomföras eller sannolikt kommer att genomföras

Samuel Bjelkemyr

Innehållsförteckning

Sammanfattning

Rapportens syfte är att förmedla en kondenserad vy av de mest betydelsefulla förändringarna av Ethereum och bidra med diskussion och slutsatser kring dessa. Utgångspunkten är att Ethereum historiskt prioriterat decentralisering och säkerhet men nu har siktet inställt på skalbarhet, vilket är svårt att förena med dessa två attribut. Ethereum har nyligen bytt konsensusmekanism till proof of stake, vilket kan ses som det första stora steget mot framtida skalning, även om förändringen i sig inte innebär några skalningsfördelar. Nästa utvecklingssteg bär namnet sharding men den pågående implementationen, danksharding, skiljer sig från begreppets normala innebörd. Danksharding är menat att erbjuda datautrymme till rollups. Storskalig användning av rollups är slutmålet för Ethereum och utformningen av deras nollkunskapsbevis är föremål för pågående forskning.

1. Inledning

Läsaren antas bekant med blockkedjor men inte nödvändigtvis med Ethereum. Här följer en övergripande genomgång för att nå bekantskap med några betydelsefulla grundstenar eller distinktioner. Avgränsningar och struktur finns därefter att ta del av i nästa avsnitt.

1.1 Ether och transaktioner

Ether är den valuta som har sitt hem på blockkedjeplattformen Ethereum. Att få sina transaktioner utförda på Ethereum kostar Ether. Begreppet transaktion avser både valutaöverföringar såväl som interaktion med, eller upprättande av, smarta kontrakt.

1.2 Smarta kontrakt

Smarta kontrakt är programmerade entiteter som kan läggas upp på Ethereum och sedan interageras med av andra. Denna funktionalitet är vad som gör Ethereum till en plattform i ordets fulla utsträckning. Poängen med att skriva kontrakt i kod (i sammanhang som exempelvis decentralized finance, DeFi) är att sådan är deterministisk och därmed inte kräver något förtroende. Ordet kontrakt är i detta fall mindre begränsande än vad som annars kan antas och många av användningsområdena för smarta kontrakt skulle i vardagligt språk inte beskrivas som kontrakt. Oavsett består de alltid uteslutande av kod.

1.3 Ethereum som blockkedja

Tillståndslösa blockkedjor, därmed Ethereum, bygger på att många utspridda noder (klienter) sparar en gemensam identisk historik över allt som har skett, samt reglerna för vad som får ske och hur det ska gå till. Historik och protokoll med andra ord. En brett överenskommen version av historiken vid en viss tidpunkt är blockkedjans tillstånd, state.

Den som vill genomföra en transaktion signerar den kryptografiskt för att bevisa äganderätt över en viss adress i historiken (kopplad till ett saldo). Därefter sänds transaktionen till andra noder som kontrollerar signeringens validitet, lägger till den i sitt temporära minne (bland många andra transaktioner) om den anses legitim (enligt protokollets regler) och vidare sänder ut de väntande transaktionerna till andra noder.

Ethereum producerar ett nytt block var tolfte sekund. En nod utses till blockproducent för ett givet block. Transaktionerna i producentens temporära lokala minne (som aktivt synkas med andra noder) packas ihop till ett block som föreslås. Detta block skickas ut i sin helhet till andra noder som, avsiktligt redundant, validerar det enligt sina lokala versioner av protokollet. Idealt uppnås brett konsensus (mer om konsensusmekanism senare), Ethereum når ett nytt state, nästa blockperiod påbörjas och en ny blockproducent tar vid.

2. Avgränsningar

Denna rapport ägnas åt förändringar (uppgraderingar) av Ethereum som nyligen skett, är på väg att ske eller sannolikt kan komma att ske, samt diskussion kring detta. Rapporten har två syften, dels att förmedla en kondenserad vy av de mest betydelsefulla förändringarna, dels att bidra med diskussion och slutsatser kring detta. Diskussion förs delvis löpande genom rapporten och delvis samlat i det fjärde och avslutande avsnittet. Härnäst följer den mest utförliga delen, förändring av Ethereum, och sedan diskussionen.

3. Förändring av Ethereum

3.1 Blockchain Trilemma

Ethereum strävar efter att uppnå, utöka eller bibehålla decentralisering, säkerhet och skalbarhet (Cointelegraph, 2022). Svårigheten att kombinera dessa tre mål är känt som blockchain trilemma. Ethereum har fokuserat på de två målen säkerhet och decentralisering, varpå skalbarheten har blivit lidande (Cointelegraph, 2022).

Högre effektivitet och skalbarhet kan enklast uppnås genom att minska den avsiktliga redundansen (Binance, 2022) och därmed låta färre noder verifiera och exekvera. Problemet är att en sådan förändring direkt motverkar decentraliseringen. Dessutom påverkas säkerheten negativt eftersom lägre deltagande ökar risken för majoritetsattacker (Aponte m.fl., 2021).

3.2 Proof of Stake

Ethereum använder konsensusmekanismen proof of stake. Den som vill delta i den demokratiska processen (validera eller producera block) måste låsa fast en monetär insats. Denna insats kan sedan reduceras eller helt raderas enligt förbestämda regler menade att motverka illegitimt beteende (Buterin, 2017).

Tidigare verkade Ethereum enligt proof of work. Ändringen av konsensusmekanism har förberetts under lång tid och genomfördes slutligen för några månader sedan, i vad som kallats för The Merge (Ethereum Foundation, 2022e). Proof of work är en mer välkänd metod för att nå konsensus vars kärna utgörs av så kallad mining, alltså lösandet av genererade matematiska problem för att bli utsedd till blockproducent. Konsekvenser av förändringen inkluderar lägre energiförbrukning (proof of stake förbrukar avsevärt mindre energi, ingen mining krävs), potentiellt svagare förtroende (proof of work är simplare att implementera, proof of stake är nyare) och stärkt säkerhet mot majoritetsattacker eftersom de blir dyrare att genomföra (Buterin, 2017).

Ethereums implementation av proof of stake gick innan hopslagningen under namnet Beacon Chain (Ethereum Foundation, 2022e), vilket testades utanför mainnet. Även efter hopslagningen kan denna Beacon Chain beskrivas till viss grad separerad eftersom konsensusklienter och exekveringsklienter skickar meddelanden på sina egna respektive nätverk (Prysmatic Labs, 2022). Ethereum kräver dock att en nod opererar både konsensus- och exekveringsklient. Därtill kommer också valideringsklient som verkar tätt ihop med konsensusklienten och är nödvändig för de som validererar och producerar.

Aktiva validerare (med fastlåst insats) tar, enligt proof of stake, emot andra blockproducenters förslag (förutsatt att de inte själva är producent vid tillfället), verifierar metadatan, exekverar transaktionerna lokalt och röstar huruvida blocket är legitimt (Ethereum Foundation, 2022c). Blockproducent utses slumpmässigt och det samma gäller den, för blocket tillfälliga, utvalda delmängden validerare som bildar röstande kommittéer (Ethereum Knowledge Base, 2022).

Blocken placeras i en på förhand bestämd ordning i grupperingar kallade epoker. Varje epok består av 32 block. Ibland händer det att blockproducenter inte föreslår något block vilket leder till att den nästföljande producenten utgår från blocket innan den tomma platsen (Ethereum Knowledge Base, 2022). Om det överhoppade blockets producent snarare är för långsam men ändå föreslår sitt block, som det efterföljande ignorerat, finns regler som avgör vilket block som ska byggas vidare på (Buterin, 2021b). Transaktionerna i ett block som nyligen offentliggjorts riskerar därmed att inte utföras i den kedja som slutligen blir den riktiga. Blocket anses först delvis säkert (justified) när, enligt Ethereums proof of stake, två tredjedelar av validerarna attesterat det (Alchemy, 2022b). När ytterligare en epok har lagts till och blocket fortfarande ingår i den kanoniska kedjan anses blocket i praktiken omöjligt att förändra (finalized).

3.3 Sharding

Database sharding innebär att databaser distribueras på flera separata maskiner. Det här är en vanlig metod utanför blockkedjevärlden och syftar till att motverka flaskhalsar som annars uppstår av för mycket trafik till en enskild server. Effektiviteten påverkas positivt av två anledningar. För det första tar varje ny del emot färre förfrågningar och för det andra behöver varje enskild del söka igenom och indexera färre rader av databasen. Sharding är en horisontellt sätt att skala och är skiljt från horisontell partitionering på så sätt att sharding delas upp på separata maskiner tvärtemot partitionering som görs på en maskin (Amazon, 2022). Det går också att välja motsatt tillvägagångssätt, vertikal skalning, och i stället använda de flera maskinernas hårdvara för att uppgradera en enskild maskin. Problemen med vertikal skalning är att det endast är effektivt till en viss grad och snabbt når avtagande avkastning på ytterligare hårdvara samt är olämpligt för Ethereum tack vare centraliseringen det leder till. Horisontell skalning däremot är proportionerligt skalbart utan någon betydelsefull gräns och kan tänkas förenligt med decentralisering.

Den sharding som planeras för Ethereum skiljer sig från begreppets normala innebörd. Eftersom Ethereum är decentraliserat och tillståndslöst är det ingen rimlig lösning att be, än mindre beordra, att de många noderna alla stärker sin kapacitet eller att fler noder deltar. Dels eftersom ingen har formell auktoritet över vem eller hur många som deltar, dels för att krav på bättre hårdvara skulle direkt motverka önskan om ytterligare decentralisering som kan uppnås genom att tvärtemot sänka hårdvarukraven. Att försöka åstadkomma högre deltagande och fler noder har (med nutida version av Ethereum) en specifik likhet med vertikal skalning, vilket kan upplevas märkligt eftersom noderna är så pass horisontellt utspridda. Noderna är ju dock (till hög grad) kopior av varandra och kan beskrivas som del av en och samma maskin, Ethereum Virtual Machine (Ethereum Foundation, 2022b). Likheten med vertikal skalning är att fler noder för Ethereum inte innebär en proportionerlig ökning av kapaciteten att behandla fler transaktioner simultant eftersom allt är redundant. Återigen kolliderar vi med blockchain trilemma-väggen.

”Alla vägar leder till *centraliserad* blockproduktion [och] decentraliserad förtroendelös blockvalidering” (Charbonneau, 2022b). Eftersom den totala redundansen verkar logiskt oförenlig med kostnadseffektiv skalning är Ethereums tillvägagångssätt att låta den krävande blockproduktionen centraliseras men ändå som helhet uppnå decentralisering och säkerhet genom teknisk forskning och nyutveckling. Siktet är därmed inställt på sharding (mer om detta i följande stycken) och rollups (mer om detta i nästa avsnitt). Sharding blir i detta sammanhang en implementation på layer one (ungefär mainnet) för att tillåta effektiva rollups på layer two, alltså utanför Ethereum (exempel på rollups finns redan aktivt fungerande i dagsläget men är inte ideala). Den centraliserade blockproduktionen (rollups) utanför mainnet kräver stora mängder data och sharding blir därmed ett sätt att uppnå kapacitet att leverera data till rollups.

Det är inte helt uppenbart hur Ethereums implementation av sharding kommer att bli men det finns några teman som alla beskrivningar och förslag har gemensamt. I grund och botten går sharding ut på att inte längre låta alla noder validera och exekvera allting, utan i stället dela upp arbetsbördan, på ett sådant sätt att säkerhet och decentralisering ändå kvarstår (Buterin, 2021a). Det finns i huvudsak två stora problem kopplade till att dela upp arbetet och båda dessa problem är kopplade till validering. För det första behöver de som inte utför ett visst arbete kunna verifiera att arbetet utförts korrekt, utan att själva utföra arbetet. För det andra behöver de som inte utför arbetet kunna säkerställa att arbetet har utförts på all data som borde ingå i arbetet, samt att denna data finns allmänt tillgänglig, utan att själva ladda ner all data. Det förstnämnda ser ut att lösas med en av två typer av metoder, nollkunskapsbevis (Ethereum Foundation 2022f) eller bedrägeribevis (Ethereum Foundation 2022d), mer om dessa i nästa avsnitt. Metoderna för att lösa det sistnämnda problemet, datatillgängligheten, påverkas också av valet av metod för validering av beräkningen (Polygon Team, 2021).

Danksharding ser ut att bli Ethereums implementation av sharding och utvecklas i skrivande stund (Buterin, 2022). Tidigare förslag för sharding har avsett att, utöver att erbjuda data till rollups, också utöka utrymmet för transaktioner på mainnet (Buterin, 2022). Danksharding däremot är en simplare lösning som helt omfamnar Ethereums alltmer cementerade framtidsplan med laserfokus på rollups (Charbonneau, 2022b). Med danksharding skapas utrymme på layer one för så kallade blobs (binary large objects) som layer one inte behöver läsa (och alltså finns till för rollups utanför mainnet). Det nyskapande med danksharding är dess merged fee market. Kortfattat leder danksharding och merged fee market till (jämfört med andra implementationer av sharding) mer centraliserad blockproduktion. Detta ställer höga hårdvarukrav på blockproducenter. För att validerare inte ska utsättas för samma hårdvarukrav implementeras i så fall proposer/builder-separation (Buterin, 2022).

3.4 Rollups

Rollups buntar ihop många transaktioner till färre större transaktioner och minimerar resursförbrukningen som krävs för att utföra transaktionerna samt sänker kostnaderna (avgift i Ether) för de ingående transaktionerna (Ethereum Foundation, 2022a). Arbetet med att kombinera och utföra transaktioner sker utanför Ethereums kedja. Användare överlämnar alltså signerade transaktioner till en centraliserad part på en annan kedja (ägnad åt detta syfte). Själva överlämnandet är riskfritt och är att likställa med att skicka ut sin transaktion på mainnet. (Signeringar går inte att återanvända eller missbruka, de visar endast äganderätt över privatnyckeln utan att avslöja själva nyckeln). Interaktionen med de fristående centraliserade aktörerna bakom rollups är inte tekniskt förtroendelös men det värsta som kan hända är att transaktionen inte blir utförd, alltså precis som mainnet, och att vänta på slutgiltig status (finalized) görs alltid oavsett.

Rollups blir säkra och decentraliserade, trots sin egen centralisering, genom att använda layer one för datatillgänglighet, konsensus och (eventuellt, beroende på implementation) settlement layer (Charbonneau, 2022a). Rollups hjälper alltså till med den tredje (fjärde) komponenten, exekvering. Utmaningarna består av att, vid inskickning från rollup till mainnet, kunna säkerställa att rollupen har utfört alla ingående transaktioner korrekt och att alla data finns tillgänglig – utan att varken utföra transaktionerna eller ladda ner all data. (Om det görs motverkas syftet med rollups, alltså skalning genom att eliminera redundans.) Det finns två koncept för att säkerställa att transaktionerna exekverats korrekt. Dessa är nollkunskapsbevis och bedrägeribevis.

Nollkunskapsbevis är menade att låta en informerad part styrka att den har viss information utan att avslöja informationen. För Ethereum är de inte avsedda att gömma någon sorts privat information, de är i stället till för att slippa slösa resurser på att läsa informationen. De metoder som utvecklas för Ethereum fungerar på så sätt att de härleder polynomer utifrån de transaktioner som exekverats off-chain (Alchemy, 2022a). Det finns olika matematiska modeller för att ta fram dessa polynomer, gemensamt är att de är någorlunda krävande att ta fram för den enskilda insändaren, vilket är en nödvändig detalj. Den som vill kontrollera att en mängd inskickade transaktioner är legitima tar en slumpmässig handfull av de ingående

transaktionerna, beskådar polynomet och ber insändaren (från lager två till lager ett) peka ut punkter av polynomet som härletts från de utvalda transaktionerna. Sannolikheten att polynomet representerar samtliga påstådda ingående transaktioner ökar exponentiellt med antalet test som görs. Testen görs i snabb följd och potentiellt av flera olika noder samtidigt vilket gör att avsändaren inte har tid att beräkna svar, vilket alltså styrker att de redan är uträknade. Dessa nollkunskapsbevis bygger på sannolikhet. I dagsläget anses de fullkomligt säkra men det finns viss risk att kvantdatorer och signifikanta ökningar av beräkningskraft i framtiden kan göra vissa av metoderna osäkra (Ethereum Foundation, 2023).

Bedrägeribevis används för optimistiska rollups och bygger på att transaktioner kan utmanas i efterhand (Alchemy, 2022a). Initialt antas alla inskickade transaktioner legitima och om ingen utmanar transaktionen under en bestämd tidsperiod blir de till slut oföränderliga. Rollups med bedrägeribevis liknar implementationerna av nollkunskapsbevis på så sätt att även dessa bygger på tester av en delmängd och förlitar sig på sannolikhet. Det eventuella ifrågasättandet av en transaktion bygger på jämförelser med trädstrukturers rötter (komprimerad information om hela trädet i form av en hash) och utvalda transaktioner (Alchemy, 2022a). Den största nackdelen med bedrägeribevis är att transaktionen inte kan anses helt säker under tidsperioden för ifrågasättande, oftast en vecka, vilket i sammanhanget är mycket länge. Fördelarna är enkelheten och framför allt hur lite resurser de förbrukar.

Det finns i dagsläget implementationer av både nollkunskapsbevis och bedrägeribevis, även om de dras med brister som önskas lösas inför mer storskaligt användande av rollups. En jämförelse av genomsnittlig resursåtgång kommer fram till att nollkunskapsbevis är ungefär tio gånger dyrare (Alchemy, 2022a), vilket fördelas på slutanvändarna. Det bör dock poängteras att båda metoder möjliggör avsevärda skalningsmöjligheter, vilket alltså inkluderar nollkunskapsbevis trots de stora skillnaderna sinsemellan. Vidare är nollkunskapsbevis omedelbara medan bedrägeribevisen har långa vänteperioder. Sett till säkerhet och decentralisering anses nollkunskapsbevisen ha bättre egenskaper. I dagsläget sker mer forskning på och utveckling av nollkunskapsbevis (Charbonneau, 2022a), vilket kan förklaras av delvis ett behov att förstå något mer komplext och delvis en preferens.

4. Diskussion

Det är en tolkningsfråga om diskussionen angående Blockchain Trilemma fortfarande är relevant efter införandet av de nämnda förändringarna. Å ena sidan görs viss uppoffring av en av de tre komponenterna i utbyte mot en annan (decentralisering byts mot skalning) i enlighet med den påstådda begränsningen. Å andra sidan ser denna uppoffring ut att kunna kompenseras med metoder som gör att en nästintill identisk grad av decentralisering uppnås.

Proof of stake har nu fungerat väl för Ethereum under flera månaders tid och så småningom lär även denna konsensusmekanism anses stridstestad, i enlighet med hur proof of work ofta beskrivs. En potentiellt betydelsefull detalj är att aktiva validerare i dagsläget inte kan avsluta sina positioner. Man har med andra ord ännu inte infört funktionalitet för att ta tillbaka sin insättning. I dagsläget är ungefär tio procent av hela utbudet Ether fastlåst i dessa insättningar. Hur många som överhuvudtaget vill avsluta sina positioner är högst oklart. Incitamentet att

fortsätta är att validerare får en del av avgifterna som lön för sitt deltagande. Om en betydande mängd tar ut sina insättningar i samma stund som det tillåts riskerar det att påverka hur väl konsensusmekanismen fungerar. Detta är dock känt och belöningen för att validera höjs, sett till den absoluta mängden Ether, i takt med att färre deltar. Men låt säga att Ether tappar värde samtidigt som färre vill validera. Då kan Ethers värdetapp motverka funktionen som är tänkt att skydda mot mindre intresse att validera (åtminstone subjektivt, avkastningen i procent kvarstår god eftersom insättningen också minskar lika mycket i värde).

När det gäller sharding görs stora framsteg och det finns konkreta EIPs (Ethereum Improvement Proposals) som är menade att förbereda och implementera en delmängd av förändringarna. Tidigare utformningar av sharding såg ut att bli mer invecklade att införa än de som är på väg att bli verklighet, eftersom de i lägre grad omfamnade rollups som mål. Men idag råder inte mycket tvivel om att rollups är vägen som bör väljas och då räcker simplare varianter av sharding. Rollups med nollkunskapsbevis föredras och dessa bevis är fortsatt invecklade att implementera på ett bra sätt. Mycket av forskningen sker inom detta område.

En diskussion om Ethereums framtid riskerar att upplevas ofullständig om valutan Ethers framtid inte berörs. Valutans eventuella värdeförändring är onekligen knuten till den tekniska utvecklingen och dess framgångar eller misslyckanden. Samtidigt är det ett begränsande perspektiv att anta att Ethers förändring speglar Ethereums förändring. Den slutgiltiga implementationen av en viss förändring resulterar ibland i värdetapp för valutan – de tekniska framstegen till trots. Medan valutan går upp, ner eller i cirklar går plattformen stadigt framåt. Inte bara plattformen i singular, utan tekniken bakom blockkedjor överlag. Ethereum kan inte beskrivas som annat än motståndskraftigt, med hängivna utvecklare, ambitiösa mål och en stark kultur med god arbetsmoral och villighet att arbeta runt hinder. Kortsiktigt kan valutan krascha och/eller EVM upphöra att fungera men långsiktigt finns i dagsläget få signifikanta hot mot blockkedjors fortsatta utveckling. Om ett hot ändå ska utses är det sannolikt lagstiftning. Tillståndslösheten, decentraliseringen och svårigheten att spåra transaktioner gör tekniken mycket attraktiv för de som agerar utanför lagen. Det är fullt möjligt att vissa förändringar kommer behöva göras för att anpassa blockkedjorna till ny lagstiftning men att tekniken som helhet, med dess många användningsområden, skulle förbjudas helt och hållet (i väst) får anses osannolikt.

I dagsläget är det fortfarande svårt för de största kryptovalutorna att konkurrera med fiatvalutor (exempelvis SEK). Få företag accepterar dem som betalmedel, transaktionsavgifterna är höga, väntetiden är för lång, interaktionen med valutan är för krånglig, värdet är för volatilt, problematiska handlingar och grupper är kopplade till dess image och framtida lagstiftning är oklar. Värt att poängtera är dock att ungefär hälften av dessa problem har någon slags koppling till Ethereums effektivitet, som ju alltså är på väg att stärkas avsevärt.

Det finns en mängd funktioner som användare av Ethereum hoppas ska utvecklas på plattformen. Något som plattformen är väl utformad för att hantera är identifiering. I Sverige använder vi i huvudsak BankID för att identifiera oss online. Frågan är hur bra det är att ett centraliserat företag agerar mellanhand i vår interaktion med myndigheter, företag och banker, i tider då ransomware blir vanligare.

Mycket av finansieringen som är menad att incentivera utveckling av Ethereum kommer från Ethereum Foundation (fortsättningsvis EF), alltså samma organisation som för många år sedan lanserade Ethereum. Organisationen har ingen formell kontroll över blockkedjan (den är tillståndslös) men har betydande inflytande, både socialt och monetärt. Bidrag ges till grupper av utvecklare och andra som bidrar till Ethereums framtid. Dessa bidrag ges eftertänksamt. När det gäller klientutvecklare försöker man motverka nätverkseffekter, och därmed öka decentraliseringen, genom att ge (sett till andel användande) oproportionerligt mycket till klienter med färre användare, eftersom användare annars alla strömmar till den mest populära klienten. Poängen är att EF är betydelsefullt för Ethereum. Frågan som bör ställas är därmed vad som händer om EF inte längre finns till eller agerar på samma sätt. Att Ethereum i sin nuvarande utformning fortsätter verka råder inga tvivel om men däremot är den fortsatta utvecklingen sannolikt beroende av välfungerande koordinering och stödjande finansiering. Samtidigt är dessa grupper utvecklare inte kända för att vara drivna av endast pengar – altruistiska motiv är relativt utbredda. För många handlar blockkedjor om mer än ny teknik och pengar. För vissa är decentraliseringen och konkurrerandet mot statlig kontroll den primära motivationen. Den önskade användargruppen, den breda allmänheten, prioriterar sannolikt praktiskhet och bekvämlighet över sådana motiv. Idag är decentraliseringen något av det mest genredefinierande för blockkedjor men det är möjligt att något annat attribut till slut visar sig mer användbart och formar den fortsatta utvecklingen.

Källförteckning

Alchemy (2022a). *Validity (ZK) Proofs vs. Fraud Proofs.* https://www.alchemy.com/overviews/validity-proof-vs-fraud-proof

Alchemy (2022b). *What are Ethereum commitment levels? Latest, Safe, Finalized.* https://www.alchemy.com/overviews/ethereum-commitment-levels

Amazon (2022). *What is database sharding?* https://aws.amazon.com/what-is/database-sharding/

Aponte-Novoa, F. A., Orozco, A. L. S., Villanueva-Polanco, R., & Wightman, P. (2021). *The 51% attack on blockchains: A mining behavior study.* IEEE Access, 9, 140549-140564.

Binance (2022). *What Is the Blockchain Trilemma?* https://academy.binance.com/en/articles/what-is-the-blockchain-trilemma

Buterin, V. (2022). *Proto-Danksharding FAQ.* https://notes.ethereum.org/@vbuterin/proto_danksharding_faq#Proto-Danksharding-FAQ

Buterin, V. (2021a). *Why sharding is great: demystifying the technical properties.* https://vitalik.ca/general/2021/04/07/sharding.html

Buterin, V. (2021b). *Serenity Design Rationale.* https://notes.ethereum.org/@vbuterin/serenity_design_rationale

Buterin, V. (2017). *Proof of Stake FAQ.* https://vitalik.ca/general/2017/12/31/pos_faq.html

Charbonneau, J. (2022a). *The Complete Guide to Rollups.* https://members.delphidigital.io/reports/the-complete-guide-to-rollups/

Charbonneau, J. (2022b). *The Hitchhiker's Guide to Ethereum.* https://members.delphidigital.io/reports/the-hitchhikers-guide-to-ethereum

Cointelegraph (2022). *A beginner's guide to understanding the layers of blockchain technology*. https://cointelegraph.com/blockchain-for-beginners/a-beginners-guide-to-understanding-the-layers-of-blockchain-technology

Ethereum Foundation (2022a). *Ethereum for everyone.* https://ethereum.org/en/layer-2/

Ethereum Foundation (2022b). *Ethereum virtual machine.* https://ethereum.org/en/developers/docs/evm/

Ethereum Foundation (2022c). *Networking layer.* https://ethereum.org/en/developers/docs/networking-layer

Ethereum Foundation (2022d). *Optimistic rollups.* https://ethereum.org/en/developers/docs/scaling/optimistic-rollups/

Ethereum Foundation (2022e). *The Merge.* https://ethereum.org/en/upgrades/merge/

Ethereum Foundation (2022f). *Zero-knowledge rollups.* https://ethereum.org/en/developers/docs/scaling/zk-rollups/

Ethereum Foundation (2023). *What are zero-knowledge proofs?* https://ethereum.org/en/zero-knowledge-proofs/

Ethereum Knowledge Base (2022). *Glossary.* https://kb.beaconcha.in/glossary

Polygon Team (2021). *The Data Availability Problem*. https://polygon.technology/blog/the-data-availability-problem-6b74b619ffcc

Prysmatic Labs (2022). *Nodes and networks*. https://docs.prylabs.network/docs/concepts/nodes-networks