Dynex: Moore yasasının ötesinde bilgi işlem için ölçeklenebilir ve güvenilir bir platform

Dynex Geliştiricileri

22 Eylül 2022 v1.2

Özet

Moore yasasının sonu yaklaşırken ve **Dennard ölçeklendirmesi sona ererken, bilgi işlem** topluluğu sürekli performans iyileştirmeleri sağlamak için giderek daha fazla yeni teknolojilere bakıyor. Nöromorfik bilgisayar, yapısı ve işlevi biyoloji ve fizikten esinlenen von Neumann olmayan bir bilgisayardır. Günümüzde bu tür sistemler mevcut teknoloji kullanılarak, hatta ölçeklendirilerek inşa edilip işletilebilmekte ve **mevcut** sistemlerden daha iyi **performans** gösterebilmektedir.
kuantum bilgisayarlar[1,2] .

Dynex, yeni bir esnek blok zinciri protokolüne dayanan **nöromorfik bilgi** işlem **için** yeni nesil bir **platformdur.** Nöromorfik donanım kullanan ve hesaplamayı hızlandırabilen yazılım uygulamaları ve algoritmaların geliştirilmesi için tasarlanmıştır. Bu amaca ulaşmak için platform, nöromorfik çip kümelerini çalıştıran ana bilgisayarları, bu yeni nesil donanımı kullanan kullanıcılar ve uygulamalarla birbirine bağlar. Dynex platformunda, hesaplama süresi Dynex yerel belirteci ile değiştirilir.

Dynex ayrıca Dynex ekosistemini tamamlayan ve herhangi bir modern sahada programlanabilir kapı dizisi (FPGA) tabanlı çipi, çok çeşitli uygulamalar için klasik veya kuantum metodolojilerinden çok daha hızlı performans gösterebilen nöromorfik bir bilgi işlem çipine dönüştüren tescilli bir devre tasarımı olan Dynex **Neuromorphic Chip'i** geliştirmiştir. ASIC'lerin proof-of-work token madenciliği endüstrisindeki hakimiyeti nedeniyle, yüksek performanslı yeni nesil nöromorfik bilgi işlem kümelerine dönüştürülebilecek büyük miktarda atıl FPGA altyapısı mevcuttur.

[1] Mniszewski, S. M. Spiking nöromorfik donanım üzerinde ikinci dereceden kısıtsız ikili optimizasyon (QUBO) olarak grafik bölümleme. *Proc. International Conference on*

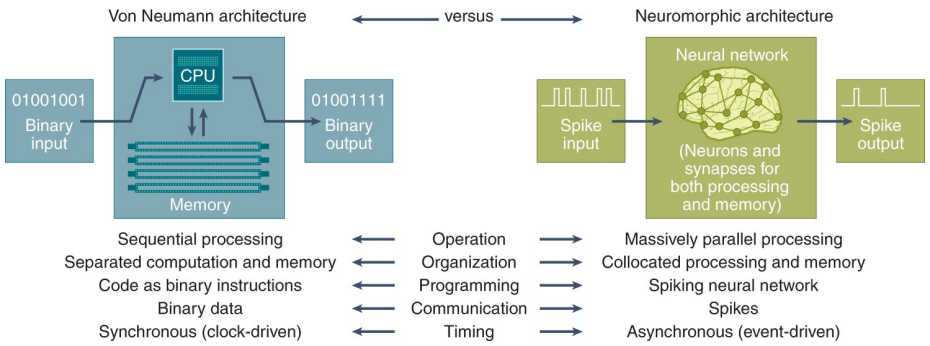
Neuromorphic içinde
Sistemler 1-5 (ACM, 2019).

[2] Yakopcic, C., Rahman, N., Atahary, T., Taha, T. M. & Douglass, S. Loihi spiking nöromorfik işlemci kullanarak kısıt memnuniyet problemlerini çözme. *2020 Design, Automation & Test in Europe Conference & Exhibition (DATE)* 1079-1084 içinde (IEEE, 2020).

1. Giriş

Moore yasasının sonu yaklaşırken ve Dennard ölçeklendirmesi sona ererken, bilgi işlem topluluğu performans iyileştirmelerinin devam etmesini sağlamak için giderek daha fazla yeni teknolojilere bakıyor. Bu yeni teknolojiler arasında nöromorfik bilgisayarlar da yer alıyor. **Nöromorfik bilgi işlem** 1980'lerin sonunda Carver Mead tarafından ortaya atılmıştır[3,4] ve o zamanlar öncelikle beyinden ilham alan bilgi işlemin analog-dijital uygulamalarını ifade etmektedir. Ancak son yıllarda, nöromorfik terimi, alan gelişmeye devam ettikçe ve DARPA Synapse projesi ve Avrupa Birliği İnsan Beyni Projesi de dahil olmak üzere beyinden ilham alan bilgi işlem sistemleri için büyük ölçekli finansman fırsatları ortaya çıktıkça, çok çeşitli donanım uygulamalarını kapsar hale gelmiştir.

Nöromorfik bilgisayar terimi, yapısı ve işlevi **biyoloji ve fizikten etkilenen Von Neumann olmayan bilgisayarları** ifade eder. Veri ve talimatlar, ayrı CPU ve bellek birimlerinden oluşan Von Neumann bilgisayarlarının bellek birimlerinde saklanır. Öte yandan, nöromorfik bir bilgisayarda hem işlem hem de bellek nöronlar ve sinapslar tarafından yönetilir. Von Neumann bilgisayarların aksine, nöromorfik bilgisayarlar programlarını açık talimatlardan ziyade sinir ağının yapısına ve ağın parametrelerine göre tanımlar. Ayrıca, von Neumann bilgisayarları bilgiyi ikili terimlerle ifade edilen sayısal değerler olarak kodlarken, nöromorfik bilgisayarlar, meydana geldikleri zaman, büyüklükleri ve çıktılarının şekli ile ilişkili sayısal olarak kodlanan sivri uçları girdi olarak alır.



Şekil 1: Von Neumann mimarisinin nöromorfik mimari ile karşılaştırılması

[3] Mead, C. Nöromorfik elektronik sistemler. *Proc. IEEE* 78, 1629-1636 (1990).

[4] Mead, C. Nöromorfik mühendisliği nasıl yarattık. *Nat. Electron.* 3, 434-435 (2020).

İki mimari arasındaki zıt özelliklerin bir sonucu olarak (Şekil 1), nöromorfik bilgisayarlar bir dizi temel operasyonel farklılık sunar:

- **Doğası gereği paralel çalışma,** tüm nöronların ve sinapsların potansiyel olarak aynı anda çalışabildiği nöromorfik bilgisayarların bir özelliğidir; ancak, paralelleştirilmiş von Neumann sistemleriyle karşılaştırıldığında, nöronlar ve sinapslar nispeten basit hesaplamalar gerçekleştirir.

- **Bellek ve işlem bir arada bulunur:** nöromorfik donanımda bellek ve işlemeyi ayıran bir kavram yoktur. Nöronların bazen işlem birimleri ve sinapsların bellek birimleri olarak düşünülmesine rağmen, birçok uygulamada nöronlar ve sinapslar birlikte işlem yapar ve değerleri depolar. İşlemci ve belleğin birleştirilmesiyle, işlemci/bellek ayrımına ilişkin von Neumann darboğazı hafifletilerek maksimum verimde azalma sağlanır. Ayrıca bu birleştirme, işlem enerjisine kıyasla büyük miktarda enerji tüketen ana bellekten veri erişimi ihtiyacını azaltır.[5] .

- Daha fazla nöromorfik çip eklenmesi nöron ve sinaps sayısını artırdığı için nöromorfik bilgisayarlar **doğal ölçeklenebilirliğe** sahiptir. . Daha büyük ve daha geniş ağları çalıştırmak için, birden fazla fiziksel nöromorfik çipi tek bir büyük nöromorfik uygulama olarak ele almak mümkündür. SpiNNaker[6,7] ve Loihi[8] dahil olmak üzere birkaç büyük ölçekli nöromorfik donanım sistemi başarıyla uygulanmıştır.

- Nöromorfik bilgisayarlar **olay güdümlü hesaplama** (yani, yalnızca mevcut veriler mevcut olduğunda hesaplama) ve zamansal olarak seyrek hesaplama kullanır

[5] Sze, V., Chen, Y.-H., Emer, J., Suleiman, A. & Zhang, Z. Makine öğrenimi için donanım: zorluklar ve fırsatlar. *2017 IEEE Özel Entegre Devreler Konferansı (CICC)* 1-8 (IEEE, 2017).

[6] Mayr, C., Hoeppner, S. & Furber, S. SpiNNaker 2: beyin simülasyonu ve makine öğrenimi için 10 milyon çekirdekli bir işlemci sistemi. Ön baskı https://arxiv.org/abs/1911.02385 (2019).

[7] Furber, S. B., Galluppi, F., Temple, S. & Plana, L. A. SpiNNaker projesi. *Proc. IEEE* 102, 652-665 (2014).

[8] Davies, M. ve diğerleri Loihi: çip üzerinde öğrenmeye sahip nöromorfik bir çok çekirdekli işlemci. *IEEE Micro* 38, 82-99 (2018).

son derece yüksek hesaplama verimliliği elde etmek için aktivite[9,10] . İşlenecek sivri uçlar olmadıkça nöronlar ve sinapslar tarafından gerçekleştirilen hiçbir iş yoktur ve tipik olarak sivri uçlar ağ işleminde nispeten seyrektir.

- Nöromorfik bilgisayarlara, örneğin nöronlar ateşlendiğinde, gürültüye uyum sağlamak için **stokastiklik** dahil edilebilir.

Nöromorfik bilgisayarlar literatürde iyi bir şekilde belgelenmiştir ve özellikleri genellikle uygulanmaları ve kullanılmaları için motive edici faktörler olarak belirtilmektedir [11,12,13,14]. Nöromorfik bilgisayarların çekici bir özelliği **son derece düşük güç tüketimleridir**: geleneksel bilgisayarlardan çok daha az güç tüketirler. Bu düşük güç tüketimi, herhangi bir zamanda tüm sistemin yalnızca küçük bir kısmının aktif olmasıyla, olay güdümlü ve büyük ölçüde paralel olmalarından kaynaklanmaktadır. Tek başına enerji verimliliği, bilgi işlemle ilişkili artan enerji maliyetlerinin yanı sıra enerji kısıtlaması olan uygulamaların (örneğin uç bilgi işlem uygulamaları) sayısının artması ışığında nöromorfik bilgisayarların kullanımını araştırmak için zorlayıcı bir nedendir. Nöromorfik bilgisayarlar sinir ağı tarzı hesaplamaları doğal olarak uyguladığından, günümüzün birçok yapay zeka ve makine öğrenimi uygulaması için doğal bir platformdur. Nöromorfik bilgisayarların doğal hesaplama özelliklerinden, çok çeşitli hesaplama türlerini gerçekleştirmek için de yararlanılabilir[15] .

---

[9] Mostafa, H., Müller, L. K. & Indiveri, G. Kısıt memnuniyet problemlerini çözmek için olay tabanlı bir mimari. *Nat. Commun.* 6, 1-10 (2015).

[10] Amir, A. ve diğerleri. Düşük güçlü, tamamen olay tabanlı bir hareket tanıma sistemi. In *2017 IEEE Bilgisayarla Görme ve Örüntü Tanıma Konferansı (CVPR)* 7388-7397 (IEEE, 2017).

[11] Schuman, C. D. ve diğerleri. Donanımda nöromorfik hesaplama ve sinir ağları üzerine bir araştırma. Ön baskı https://arxiv.org/abs/1705.06963 (2017).

[12] James, C. D. ve diğerleri. Sinirsel esinli ve nöromorfik hesaplama uygulamaları için algoritmalar ve donanım mimarilerinin tarihsel bir incelemesi. *Biol. Inspired Cogn. Archit.* 19, 49-64 (2017).

[13] Strukov, D., Indiveri, G., Grollier, J. & Fusi, S. Beyinden ilham alan bilişimin inşası. *Nat. Commun.* 10, 4838-2019 (2019).

[14] Davies, M. ve diğerleri. Loihi ile nöromorfik hesaplamayı ilerletmek: sonuçlar ve görünüm üzerine bir anket. *Proc. IEEE* 109, 911-934 (2021).

[15] Aimone, J. B. ve diğerleri. Spiking nöromorfik donanım için nöral olmayan ağ uygulamaları. *Proc. 3rd International Workshop on Post Moores Era Supercomputing* 24-26 (PMES, 2018) içinde.

2. Dynex Vizyonu

Bir Dynex nöromorfik çipi ve protokolü esnektir ve topluluk bunları gelecekte değiştirebilir. Bu bölümde Dynex'in uyması gereken ana ilkeleri tanımlıyoruz. Bu Dynex'in sosyal sözleşmesi olarak adlandırılabilir. Bu ilkelerden herhangi biri kasıtlı olarak ihlal edildiğinde, ortaya çıkan çip ve protokolden Dynex olarak bahsedilmemelidir.

- **Merkeziyetsizlik her şeyden önce gelir.** Dynex'in mümkün olduğunca merkezi olmaması önemlidir: yokluğu veya kötü niyetli davranışları ağın güvenliğini tehlikeye atabilecek taraflardan (sosyal liderler, yazılım geliştiriciler, donanım üreticileri, madenciler, fonlar vb. Dynex'in ömrü boyunca, bu taraflardan herhangi biri ortaya çıkarsa, topluluk etkilerini azaltacak önlemleri düşünmelidir.

- **Sıradan insanlar için tasarlandı.** Dynex sıradan insanlar için bir platformdur ve büyük partilere fayda sağlamak için onların çıkarlarından ödün verilmemelidir. Bu nedenle, merkezi madencilik önlenmeli ve sıradan insanlar tam düğümleri çalıştırma ve blokları çıkarma fırsatına sahip olmalıdır (küçük bir olasılıkla da olsa).

- **Geleceğin nöromorfik bilişimi için bir platform.** Dynex, üzerine inşa edilen uygulamalar ve algoritmalar için temel görevi görür. Çeşitli uygulamalar için tasarlanmış olmasına rağmen, birincil amacı yüksek verimli yeni nesil bilgi işlem sistemlerini kullanmak için verimli, güvenli ve kolay bir yol sağlamaktır.

- **Enerji tüketiminin azaltılması**: Çevremize ve geleceğimize yönelik artan iklim değişikliği tehdidi ışığında, enerji tüketimimizi azaltmak için gerekli her türlü önlemi almamız zorunludur. Bu nedenle nöromorfik bilişimin hızla benimsenmesi tüm toplumumuza fayda sağlayacaktır çünkü nöromorfik bilişim geleneksel bilişim sistemlerine kıyasla çok daha az enerji kullanır.

- **Uzun vadeli bakış açısı.** Dynex'in uzun vadeli başarısını sağlamak için, geliştirmenin tüm yönlerine uzun vadeli bir perspektiften bakılmalıdır. Dynex projesi, herhangi bir hard fork, donanım veya yazılım iyileştirmesi veya diğer öngörülemeyen değişiklikler olmaksızın yüzyıllar boyunca ayakta kalabilmelidir. Dynex'in bir platform olarak tasarlanmış olması nedeniyle, Dynex üzerine inşa edilen uygulama ve algoritmaların da uzun vadede hayatta kalması mümkün olmalıdır. Dynex'in esnekliği ve uzun vadede hayatta kalma kabiliyeti nedeniyle, iyi bir değer saklama aracı olma potansiyeline de sahip olabilir.

- **Açık ve izinsiz.** Dynex nöromorfik çipleri ve Dynex protokolü herhangi bir kullanım kategorisini kısıtlamaz veya sınırlamaz. Bir kullanıcı herhangi bir ön adım atmadan ağa katılabilmeli ve protokole dahil olabilmelidir. Dynex, geleneksel süper bilgisayar sistemlerinde olduğu gibi çekirdek seviyesinde ayrımcılığa veya sınırlı erişime izin vermez. Buna karşılık, uygulama geliştiricileri, çalışmalarının etik ve yasal sonuçlarından sorumlu oldukları sürece istedikleri mantığı uygulamakta özgürdürler.

3. Dynex Nöromorfik Çip

Dynex makinesi, bilginin aynı fiziksel konumda işlendiği ve depolandığı bellek sistemlerine dayalı genel amaçlı bilgi işlem makineleri sınıfıdır. Dynex makinesinin bellek özelliklerini analiz ederek **evrensel hesaplama** gücüne (Turing-tam), **içsel paralelliğe**, **işlevsel çok** biçimliliğe ve **bilgi ek yüküne** sahip olduklarını, yani kolektif durumlarının kolektif durumları aracılığıyla doğrudan bellekte üstel veri sıkıştırmayı destekleyebildiğini gösteriyoruz. Dahası, Dynex makinesinin tıpkı deterministik olmayan bir Turing makinesi gibi NP-tam problemleri polinom zamanda çözebildiğini gösteriyoruz. Bununla birlikte Dynex makinesi, bilgi ek yükü nedeniyle yalnızca polinom sayıda bellek hücresi gerektirir. Bu sonuçlar Turing paradigması içinde NP=P'yi kanıtlamasa da, Dynex makineleri kavramının mevcut von Neumann mimarisinden bir paradigma değişimini temsil ettiğini ve bizi beyin benzeri sinirsel hesaplama kavramına yaklaştırdığını belirtmek önemlidir.

Alan Turing'in 1936 yılında ideal makinesini icat etmesinden bu yana[16,17] , matematikçiler bu kavramı günümüzde hesaplama karmaşıklığı teorisi[18] olarak bilinen ve esasen bir algoritmanın verilen girdi verileriyle bir problemi çözmesinin ne kadar süreceğini belirlemek için kullanılan güçlü bir araç haline getirmeyi başardılar. Artık evrensel Turing makinesi (UTM) olarak bilinmekte ve günümüzün tüm dijital bilgisayarları için kavramsal bir temel oluşturmaktadır. Bir UTM'nin pratikte gerçekleştirilmesi genellikle von Neumann mimarisi[19] kullanılarak yapılır.

---

[16] A. M. Turing, "On computational numbers, with an application to the entscheidungsproblem," Proc. of the London Math. Soc., cilt 42, s. 230-265, 1936.

[17] A. M. Turing, The Essential Turing: Hesaplama, Mantık, Felsefe, Yapay Zeka ve Yapay Yaşam Alanlarında Çığır Açan Yazılar ve Enigma'nın Sırları. Oxford Üniversitesi Yayınları, 2004.

[18] S. Arora ve B. Barak, Computational Complexity: Modern Bir Yaklaşım. Cambridge Üniversitesi Yayınları, 2009.

[19] J. von Neumann, "First draft of a report on the edvac," Annals of the History of Computing, IEEE, vol. 15, no. 4, s. 27-75, 1993.

detaylarına bakıldığında, bellekten fiziksel olarak ayrı bir merkezi işlem birimi (CPU) gerektiren bir cihaz olarak görülebilir. CPU hem makinenin çalışmasını yönlendiren kontrol birimini hem de yürütme için gerekli mantık kapılarını ve aritmetik işlevleri (aritmetik/mantık birimi) içerir. CPU ve bellek arasında büyük miktarda veri aktarılması gerekir, bu da makinenin performansını hem zaman (von Neumann darboğazı[20]) hem de enerji tüketimi açısından sınırlar[21] .

Paralel hesaplama bu sorunların **bazılarını** hafifletse de **çözmez**: birkaç işlemci fiziksel bir "kapalı" bellek kullanarak tüm verinin bölümlerini işler. Sonuç olarak, tüm işlemciler eninde sonunda tüm sorunu çözmek için birbirleriyle iletişim kurmak zorunda kalacak ve bu da işlemciler ile bellekleri arasında hala önemli miktarda veri aktarımı gerektirecektir. Bu "bilgi gecikmesi sorununun" üstesinden gelmek için temelde yeni bir veri işleme ve depolama yöntemi gerekecektir.

Son araştırmalar, UTM kavramına dayanmayan ve **tüm** hesaplamayı **belleğe yerleştiren**, kendi beynimizin işlemlerinden esinlenen yeni bir **hesaplama** paradigması **önermiştir**. Bu paradigma memcomputing olarak bilinmektedir[22] . Beyinde olduğu gibi, memcomputing makineleri de ayrı bir işlemciye ihtiyaç duymadan bellekte hesaplama yapacaktır. Bellek, öğrenme ve uyarlanabilir yeteneklere izin verir[23,24] , kopuk bağlantıları atlar ve hesaplamayı çözüm yoluna kendi kendine organize eder[25,26] , tıpkı beynin belirli bir miktar hasarı sürdürebilmesi ve yine de sorunsuz bir şekilde çalışabilmesi gibi. Uygulamada, hafıza hesaplama

---

[20] J. Backus, "Programlama von neumann tarzından kurtarılabilir mi? A functional style and its algebra of programs," Commun. ACM, cilt 21, s. 613-641, Ağustos 1978.

[21] J. L. Hennessy ve D. A. Patterson, Bilgisayar Mimarisi, Dördüncü Baskı: Nicel Bir Yaklaşım. San Francisco, CA, ABD: Morgan Kaufmann Publishers Inc., 2006.

[22] M. Di Ventra ve Y. V. Pershin, "The parallel approach," Nature Physics, vol. 9, pp. 200-202, 2013.

[23] Y. V. Pershin, S. La Fontaine, ve M. Di Ventra, "Memristive model of amoeba learning," Phys. Rev. E, vol. 80, p. 021926, Aug 2009.

[24] F. L. Traversa, Y. V. Pershin, and M. Di Ventra, "Memory models of adaptive behavior," Neural Networks and Learning Systems, IEEE Transactions on, vol. 24, pp. 1437-1448, Sept 2013.

[25] Y. V. Pershin ve M. Di Ventra, "Memristörlerle labirent çözme: A massively parallel approach," Phys. Rev. E, cilt 84, s. 046703, Ekim 2011.

[26] Y. V. Pershin and M. Di Ventra, "Self-organization and solution of shortest-path optimization problems with memristive networks," Phys. Rev. E, vol. 88, p. 013305, Jul 2013.

[27,28,29] belirli frekanslarda tepki fonksiyonlarında bir dereceye kadar zamansızlık (hafıza) sergileyen birçok malzeme ve sistemin fiziksel özelliklerinden yararlanılarak uygulanabilir.

Bu tür bir makinenin **deterministik olmayan** bir **Turing makinesi ile** aynı hesaplama gücüne sahip olduğu matematiksel olarak kanıtlanmıştır[30] , ancak ikincisinden farklı olarak, tamamen deterministiktir ve bu nedenle **inşa edilebilir**. Hesaplama gücünden şu üç özellik sorumludur: **içsel paralellik** - etkileşim halindeki bellek hücreleri hesaplama yaparken durumlarını eş zamanlı ve toplu olarak değiştirir; **işlevsel çok biçimlilik - etkileşim** halindeki aynı bellek hücreleri uygulanan sinyallere bağlı olarak farklı işlevleri hesaplayabilir; ve son olarak **bilgi ek yükü** - etkileşim halindeki bellek hücreleri, bellek hücrelerinin sayısıyla doğru orantılı olmayan bir şekilde bir miktar bilgiyi depolayabilir.

Bu özellik farklı bir mimari türünden türetilmiştir: bu mimarinin topolojisi, etkileşimli bellek hücrelerinden oluşan bir ağ ile tanımlanır ve dinamikleri, bilgiyi aynı anda depolayabilen ve işleyebilen kolektif bir durumla tanımlanır. Kolektif durumlar, kuantum hesaplamadaki birçok kübitin kolektif (dolaşık) durumlarına benzer; burada dolaşık durum, belirli problem türlerini verimli bir şekilde çözmek için kullanılabilir.

3.1 Bellek İşlemcileri

Dynex mimarisinde, memişlemciler temel yapı taşlarıdır. Bir memişlemciyi *(x, y, z, σ)* dörtlüsü tarafından tanımlanan bir nesne olarak tanımlıyoruz; burada x memişlemcinin durumu, y dahili değişkenler dizisi, z bir memişlemciden diğer memişlemcilere bağlanan değişkenler dizisi ve σ evrimi tanımlayan bir operatördür.

$$\sigma[x, y, z] = (x' , y').$$

[27] T. Driscoll, H.-T. Kim, B.-G. Chae, B.-J. Kim, Y.-W. Lee, N. M. Jokerst, S. Palit, D. R. Smith, M. Di Ventra, ve D. N. Basov, "Memory metamaterials," Science, vol. 325, no. 5947, s. 1518-1521, 2009.

[28] Y. V. Pershin ve M. Di Ventra, "Memory effects in complex materials and nanoscale systems," Advances in Physics, vol. 60, no. 2, pp. 145- 227, 2011.

[29] M. Di Ventra ve Y. V. Pershin, "Memristive, memcapacitive ve meminductive sistemlerin fiziksel özellikleri üzerine," Nanotechnology, cilt 24, s. 255201, 2013.

[30] F. L. Traversa ve M. Di Ventra. Evrensel Hafıza Hesaplama Makineleri. (arXiv:1405.0931'de ön baskı) IEEE Transaction on Neural Networks and Learning Systems, DOI: 10.1109/TNNLS.2015.2391182, 2015.

İki veya daha fazla memişlemci birbirine bağlandığında, bir memişlemci ağına (hesaplama belleği) sahip oluruz. Bu durumda x vektörünü ağın durumu olarak tanımlarız (yani, her bir memişlemcinin tüm $_{xi}$ durumlarının dizisi) ve $z = \text{izi}$ tüm bağlantı değişkenlerinin dizisi, $_{zi}$ *i-inci bellek* işlemcisinin değişkenlerinin bağlantı dizisi.

Sırasıyla $_{zi}$ ve $_{zj,}$ i ve j memişlemcilerinin bağlantı değişkenlerinin vektörleri olsun, o zaman $_{zi \cap zj}$ $!= \varnothing$ ise iki memişlemcinin bağlantılı olduğunu söyleriz. Alternatif olarak, $z = z(x, y)$ *olduğunda (*yani, z tamamen x ve y tarafından belirlendiğinde) bir memişlemci başka bir memişlemciye bağlı değildir (izole edilmiştir) ve

$$\sigma[x, y, z(x, y)] = (x, y),$$

Bu da bellek işlemcisinin dinamiği olmadığı anlamına gelir. Bir memişlemci ağı, aşağıdaki gibi tanımlanan Ξ evrim operatörü tarafından verilen z bağlantı değişkenlerinin evrimine sahiptir

$$\Xi[x, y, z, s] = z'$$

Burada $y = \text{iyi}$ ve s, ağa uyaran sağlamak için bağlantıların bir alt kümesine uygulanabilecek harici sinyaller dizisidir. Son olarak, ağın tam evrimi sistem tarafından tanımlanır

$$\sigma[x_1, y_1, z_1] = (x'_1, y'_1)$$
$$\ldots$$
$$\sigma[x_n, y_n, z_n] = (x'_n, y'_n)$$
$$\Xi[x, y, z, s] = z'.$$

Evrim operatörleri σ ve Ξ ayrık ya da sürekli evrim operatörleri olarak yorumlanabilir. Ayrık evrim operatörü yorumu yapay sinir ağlarını da içerir[31] , sürekli operatör yorumu ise daha genel dinamik sistemleri temsil eder.

[31] S. Haykin, Sinir Ağları: Kapsamlı Bir Temel. Upper Saddle River, NJ, ABD: Prentice Hall PTR, 2. baskı, 1998.

3.2 Dynex makine

İdeal bir Dynex makinesi, bir kontrol ünitesinin kontrolü altında dijital (mantık) veya analog (işlevsel) işlemler gerçekleştirebilen birbirine bağlı bir bellek hücreleri (memprocessors) bankasından oluşur. Hafıza ile ve hafıza içinde hesaplama aşağıdaki gibi gösterilebilir. İki veya daha fazla bellek işlemcisi bağlandığında, kontrol birimi tarafından gönderilen bir sinyal, bellek işlemcilerinin hem ilk durumlarına hem de sinyale göre iç durumlarını değiştirmelerine neden olarak içsel paralellik ve işlevsel çok biçimlilik üretir.

Dynex makinesini sekiz çiftli olarak tanımlıyoruz

$$\text{Dynex makinesi} = (M, \Delta, P, S, \Sigma, {}_{p0}, {}_{s0,} F),$$

Burada M tek bir memişlemcinin olası durumları kümesidir. Sonlu bir $_{Md}$ kümesi (dijital rejim), bir süreklilik veya sonsuz bir ayrık durum kümesi $_{Ma}$ (analog rejim) olabilir, bu nedenle M, $M = {}_{Md}$ *VEYA* Ma olarak ifade edilebilir. Δ bir fonksiyonlar kümesidir

$$_{\delta\alpha} : M^{m\alpha} \backslash F \times P \rightarrow M^{m'\alpha} \times P^2 \times S$$

Burada $_{m\alpha} < \infty$ $_{\delta\alpha}$ fonksiyonunun girdisi olarak kullanılan (okunan) memişlemci sayısıdır ve $m'_{\alpha} < \infty$ $_{\delta\alpha}$ fonksiyonunun çıktısı olarak kullanılan (yazılan) memişlemci sayısıdır; P $_{\delta\alpha}$ tarafından çağrılan memişlemcileri seçen $_{p\alpha}$ $_{işaretçi}$ dizilerinin kümesidir ve S α indekslerinin kümesidir; Σ giriş aygıtı tarafından hesaplama belleğine yazılan başlangıç durumlarının kümesi; $_{p0} \in P$ *başlangıç işaretçi* dizisi; $_{s0}$ başlangıç indeksi α ve $F \subseteq M$ son durumların kümesidir.

Dynex makinesinin iki önemli özelliğinin, yani **paralellik** ve **çok** biçimliliğin, $_{\delta\alpha}$ fonksiyon kümesinin tanımına açıkça gömülü olduğuna dikkat ediniz. Gerçekten de Dynex makinesi UTM'den farklı olarak birden fazla $_{\delta\alpha}$ geçiş fonksiyonuna sahip olabilir (fonksiyonel polimorfizm) ve herhangi bir $_{\delta\alpha\ fonksiyonu}$ aynı anda bir dizi memişlemci üzerinde hareket eder (içsel paralellik). Dynex makinesi ayrıca UTM'den farklı olarak makine durumları ile teybe kaydedilen semboller arasında ayrım yapmaz. Bu bilgiyi kodlayan daha ziyade bellek işlemcilerinin durumlarıdır. Aynı anda hem veri depolayabilen hem de hesaplama yapabilen bir makine inşa etmek için bu bileşene sahip olmak zorunludur.

Bir başka önemli nokta olarak, sonlu sayıda ayrık durum ve sınırsız teyp depolama alanına sahip olan UTM'nin aksine, bir Dynex makinesi, bellek işlemcilerinin sayısı sınırlı olsa bile, prensipte **sonsuz sayıda sürekli durum** üzerinde çalışabilir. Özünde, her bir bellek işlemcisi sürekli durum değerleri kümesine sahip analog bir cihazdır.

Son olarak, hafıza işlemcisinin ve hafıza işlemcileri ağının resmi tanımının yukarıda tanımlanan $_{\delta\alpha}$ fonksiyonu ile uyumlu olduğu fark edilebilir. Aslında, ağın topolojisi ve evrimi uyarıcı *s* ile ilişkilendirilirken, kontrol birimi ağa belirli bir sinyal $_{s\alpha}$ (indeks vektörü $_{p\alpha}$'yı seçen) uygulanarak elde edilebilecek tüm olası $_{\delta\alpha} \in$ *Δ'yı* tanımlar. Ağ evrimi daha sonra *x'* değerini belirlerken *β* ve $_{p\beta}$ (ya da daha iyisi $_{s\beta}$) bir sonraki işlem adımı için kontrol birimi tarafından tanımlanır.

3.3 Dynex Nöromorfik Çip

Dynex makinesi fiziksel olarak, problemin çözümlerini temsil eden nokta çekicilerden oluşan **doğrusal olmayan** bir **dinamik sistem** olarak gerçekleştirilebilir. Kuantum olmayan sistemler oldukları için Dynex makinelerinin hareket denklemlerini sayısal olarak entegre etmek mümkündür. Benzer makinelerin çok çeşitli kombinatoryal optimizasyon problemleri üzerindeki performansının, geleneksel algoritmik yaklaşımlardan çok daha **hızlı** olduğu zaten gösterilmiştir32[,33,34,35,36].

Daha sonra, topolojik alan teorisi kullanılarak[37] , bu verimliliğin arkasındaki fiziksel nedenin, sistem bir alan teorisine ulaşana kadar farklı boyutlarda çığların (alan teorisi dilinde instantonlar) üretildiği geçici dinamikler sırasında gelişen dinamik uzun menzilli düzene dayandığı gösterilmiştir.

---

[32] Massimiliano Di Ventra ve Fabio L. Traversa. Perspektif: Memcomputing: Verimli hesaplama yapmak için bellek ve fizikten yararlanma. *Journal of Applied Physics,* 123(18):180901,
2018.

[33] F. L. Traversa, P. Cicotti, F. Sheldon ve M. Di Ventra. Zor optimizasyon problemlerinin çözümünde üstel hızlanma kanıtı. *Karmaşıklık*, 2018:7982851, 2018.

[34] F. L. Traversa ve M. Di Ventra. Tamsayılı doğrusal programlama bellek hesaplama. *arXiv:1808.09999*, 2018.

[35] Forrest Sheldon, Fabio L. Traversa, ve Massimiliano Di Ventra. Dinamik uzun menzilli düzen ile konveks olmayan bir manzaranın evcilleştirilmesi: Memcomputing ising benchmarkları. *Phys. Rev. E,* 100:053311, Kasım 2019.

[36] Haik Manukian, Fabio L Traversa ve Massimiliano Di Ventra. Memcomputing ile derin öğrenmeyi hızlandırma. *Neural Networks,* 110:1-7, 2019.

[37] M. Di Ventra, Fabio L. Traversa, ve Igor V. Ovchinnikov. Topolojik alan teorisi ve instantonlarla hesaplama. *Ann. Phys. (Berlin)*, 529:1700123, 2017.

çekici[38] . Bu nedenle, çözüm arayışının geçici aşaması, depremler[39] , güneş patlamaları[40] veya söndürmeler[41] gibi Doğadaki çeşitli olaylarınkine benzemektedir.

Dynex Nöromorfik Çipimiz, bir Dynex makinesinin gerçek zamanlı performansına yakın bir performans elde etmek için sahada programlanabilir kapı dizileri (FPGA) kullanır. Hesaplanacak probleme serbestçe uyarlanabilir ve ayrıca bir kümenin parçası olarak birbirine bağlanabilir ve çalıştırılabilir.

Dynex Nöromorfik Çip kullanılarak, klasik veya kuantum yöntemlerle çözülemeyen problemler çözülebilir, böylece **von Neumann darboğazının** oluşturduğu engel **ortadan kaldırılabilir**. Zor optimizasyon problemlerini çözmek, tam sayılı doğrusal programlamayı (ILP) uygulamak, makine öğrenimini (ML) gerçekleştirmek, derin sinir ağlarını eğitmek veya genel olarak bilgi işlem verimliliğini artırmak için kullanılabilir.

4. Dynex Protokolü

Bitcoin, p2p elektronik nakit kavramının başarılı bir uygulaması olmuştur. Hem profesyoneller hem de genel halk, bir güven modeli olarak halka açık işlemlerin ve iş kanıtının uygun kombinasyonunu takdir etmeye başlamıştır. Bugün, elektronik paranın kullanıcı tabanı istikrarlı bir şekilde büyümektedir; müşteriler düşük ücretlerden ve elektronik paranın sağladığı anonimlikten etkilenirken, tüccarlar da öngörülen ve merkezi olmayan emisyonuna değer vermektedir. Bitcoin, elektronik paranın kağıt para kadar basit ve kredi kartları kadar kullanışlı olabileceğini etkili bir şekilde kanıtlamıştır.
Ne yazık ki, Bitcoin çeşitli eksikliklerden muzdariptir.

Herhangi bir blok zinciri sisteminin temel bileşeni mutabakat protokolüdür ve Dynex, geleneksel bir-CPU-bir-oy algoritmalarına göre çeşitli avantajlar gösteren eşitlikçi bir Proof of Work (PoW) mutabakat protokolü kullanmaktadır:

Bir PoW sistemiyle ilgili en önemli sorunlardan birinin, küçük bir grup çalışana izin veren özel donanımların (ASIC'ler) geliştirilmesi olduğu iyi bilinmektedir.

---

[38] Forrest Sheldon, Fabio L. Traversa, ve Massimiliano Di Ventra. Dinamik uzun menzilli düzen ile konveks olmayan bir manzaranın evcilleştirilmesi: Memcomputing ising benchmark. *Phys. Rev. E*, 100:053311, Kasım 2019.

[39] Per Bak ve Chao Tang. Kendi kendini organize eden kritik bir fenomen olarak depremler. *Jeofizik Araştırma Dergisi: Katı Toprak*, 94(B11):15635-15637, 1989.

[40] E. T. Lu ve R. J. Hamilton. Çığlar ve güneş patlamalarının dağılımı. *The Astrophysical Journal*, 380:L89-L92, Ekim 1991.

[41] Gunnar Pruessner. *Kendi Kendini Organize Eden Kritiklik: Theory, Models and Characterisation*. Cambridge Üniversitesi Yayınları, 2012.

ASIC donanımlı madenciler PoW bulmacalarını herkesten çok daha hızlı ve verimli bir şekilde çözebilmektedir. Bellek açısından zor PoW şemaları, ASIC'ler ve emtia donanımları arasındaki eşitsizliği azaltarak bu sorunu çözebilir. En umut verici yaklaşımın, bir çözümü doğrulamak için onu keşfetmekten çok daha az bellek gerektiren asimetrik bellek zor PoW şemaları kullanmak olduğuna inanıyoruz[42,43] .

İkinci olarak, bir PoW ağının ademi merkeziyeti, büyük madencilerin bile madencilik havuzları oluşturma eğiliminde olması nedeniyle tehdit altındadır ve bu da sadece birkaç havuz operatörünün (bu yazının yazıldığı sırada Bitcoin'de 5 ve Ethereum'da 2) hesaplama gücünün %51'inden fazlasını kontrol ettiği bir duruma yol açmaktadır. Protokolümüz hem **bellek açısından zor** hem de havuza **dayanıklıdır**.

4.1. Eşitlikçi İş İspatı

Bu bölümde iş ispatı algoritmamızı detaylandırıyoruz. Öncelikli hedefimiz CPU (çoğunluk) ve GPU/FPGA/ASIC (azınlık) madencileri arasındaki farkı kapatmaktır. Bazı kullanıcıların diğerlerine göre belirli bir avantaja sahip olması uygundur, ancak yatırımları en azından güçle doğrusal olarak artmalıdır. Daha genel olarak, özel amaçlı cihazlar üretmek mümkün olduğunca az kârlı olmalıdır.

Orijinal Bitcoin iş ispatı protokolü, CPU yoğun fiyatlandırma fonksiyonu SHA-256'yı kullanır. Temel olarak temel mantıksal operatörlerden oluşur ve yalnızca işlemcinin hesaplama hızına dayanır, bu nedenle çok çekirdekli / taşıyıcı uygulama için mükemmel şekilde uygundur. Ancak, modern bilgisayarlar yalnızca saniyedeki işlem sayısıyla değil, aynı zamanda bellek boyutuyla da sınırlıdır. Bazı işlemciler diğerlerinden önemli ölçüde daha hızlı olabilirken, bellek boyutlarının makineler arasında farklılık gösterme olasılığı daha düşüktür.

Belleğe bağlı fiyat fonksiyonları ilk olarak Abadi ve arkadaşları tarafından tanıtılmış ve "hesaplama süresi belleğe erişim için harcanan süre tarafından domine edilen fonksiyonlar" olarak tanımlanmıştır. Ana fikir, bellek içinde nispeten yavaş erişilebilen (örneğin RAM) büyük bir veri bloğu ("scratchpad") tahsis eden ve bunun içinde "öngörülemeyen bir dizi konuma erişen" bir algoritma oluşturmaktır. Blok, verinin korunmasını her erişim için yeniden hesaplanmasından daha avantajlı kılacak kadar büyük olmalıdır. Algoritma ayrıca dahili paralelliği önlemelidir, dolayısıyla N eşzamanlı iş parçacığı aynı anda N kat daha fazla bellek gerektirmelidir.

---

[42] A. Biryukov ve D. Khovratovich, "Equihash: Asymmetric proof-of-work based on the generalized birthday problem," Ledger, vol. 2, pp. 1-30, 2017.

[43] Ethash. [Çevrimiçi]. Mevcut: https://github.com/ethereum/wiki/wiki/Ethash/6e97c9cea49605264c6f4d1dc9e1939b1f89a5a3

Dwork ve arkadaşları bu yaklaşımı araştırmış ve resmileştirerek fiyatlandırma fonksiyonunun başka bir varyantını önermişlerdir: "Mbound". Bir diğer çalışma ise en etkili çözümü öneren F. Coelho'ya aittir: "Hokkaido". Bildiğimiz kadarıyla büyük bir dizide sözde rasgele arama fikrine dayanan son çalışma C. Percival tarafından "scrypt" olarak bilinen algoritmadır. Önceki işlevlerden farklı olarak bu algoritma iş ispatı sistemlerine değil anahtar türetmeye odaklanmaktadır. Bu gerçeğe rağmen scrypt amacımıza hizmet edebilir: Bitcoin'deki SHA-256 gibi kısmi hash dönüştürme probleminde bir fiyatlandırma fonksiyonu olarak iyi çalışır.

Şimdiye kadar scrypt Litecoin ve diğer bazı Bitcoin çatallarında zaten uygulanmıştır. Bununla birlikte, uygulaması gerçekten belleğe bağlı değildir: "bellek erişim süresi / toplam süre" oranı yeterince büyük değildir çünkü her örnek yalnızca 128 KB kullanır. Bu durum GPU madencilerinin kabaca 10 kat daha etkili olmasını sağlar ve nispeten ucuz ama yüksek verimli madencilik cihazları yaratma olasılığını devam ettirir. Dahası, scrypt yapısının kendisi, scratchpad'deki her bloğun yalnızca bir öncekinden türetilmesi nedeniyle bellek boyutu ile CPU hızı arasında doğrusal bir değiş tokuşa izin verir. Örneğin, her ikinci bloğu saklayabilir ve diğerlerini tembel bir şekilde, yani yalnızca gerekli olduğunda yeniden hesaplayabilirsiniz. Sözde rastgele indekslerin düzgün dağıldığı varsayılır, dolayısıyla ek blokların yeniden hesaplanmasının beklenen değeri 21 -N'dir, burada N iterasyon sayısıdır. Toplam hesaplama süresi yarıdan daha az artar çünkü her iterasyonda karalama alanının hazırlanması ve hashing gibi zamandan bağımsız (sabit zamanlı) işlemler de vardır. Belleğin 2/3'ünün kaydedilmesi 31 - N + 13 - 2 - N = N ek yeniden hesaplamaya mal olur; 9/10'u 1 -N +...+ 1 ile sonuçlanır
-9-N = 4,5N. Tüm bloklardan sadece 1 tanesini 1010 sn saklamanın zamanı s-1 katından daha az artırdığını göstermek kolaydır. Bu da modern çiplerden 200 kat daha hızlı bir CPU'ya sahip bir makinenin karalama alanının yalnızca 320 baytını depolayabileceği anlamına gelir.

Algoritmamız, iş kanıtı fiyatlandırma fonksiyonu için belleğe bağlı bir algoritmadır. Yavaş bir belleğe rastgele erişime dayanır ve gecikme bağımlılığını vurgular. Scrypt'in aksine her yeni blok (64 bayt uzunluğunda) önceki tüm bloklara bağlıdır. Sonuç olarak varsayımsal bir "bellek koruyucu" hesaplama hızını katlanarak artırmalıdır. Örnek başına yaklaşık 2MB gerektirir:

- birkaç yıl içinde yaygınlaşması beklenen modern işlemcilerin L3 önbelleğine (çekirdek başına) sığar;
- Bir megabayt dahili bellek, modern bir ASIC boru hattı için neredeyse kabul edilemez bir boyuttur;
- GPU'lar yüzlerce eş zamanlı örneği çalıştırabilir, ancak başka şekillerde sınırlıdırlar: GDDR5 bellek CPU L3 önbelleğinden daha yavaştır ve rastgele erişim hızıyla değil bant genişliğiyle dikkat çeker.
- Scratchpad'in önemli ölçüde genişletilmesi, yinelemelerin artmasını

gerektirecek ve bu da genel bir zaman artışı anlamına gelecektir. "Ağır" çağrılar

Güvensiz bir p2p ağı ciddi güvenlik açıklarına yol açabilir, çünkü düğümler her yeni bloğun iş kanıtını kontrol etmekle yükümlüdür. Eğer bir node her bir hash değerlendirmesi için önemli miktarda zaman harcarsa, keyfi iş verilerine (nonce değerleri) sahip sahte nesnelerden oluşan bir sel tarafından kolayca DDoS'a maruz kalabilir.

4.2. Takip Edilemeyen İşlemler

Bu bölümde, hem takip edilemezlik hem de bağlantı kurulamazlık koşullarını karşılayan tamamen anonim işlemlerin şemasını açıklıyoruz. Çözümümüzün önemli bir özelliği özerk olmasıdır: göndericinin işlemlerini yapmak için diğer kullanıcılarla veya güvenilir bir üçüncü tarafla işbirliği yapması gerekmez; dolayısıyla her katılımcı bağımsız olarak bir örtü trafiği üretir.

Şemamız, grup imzası olarak adlandırılan kriptografik ilkelliğe dayanmaktadır. İlk olarak D. Chaum ve E. van Heyst tarafından sunulmuştur[44] , bir kullanıcının mesajını grup adına imzalamasına izin verir. Mesajı imzaladıktan sonra kullanıcı (doğrulama amacıyla) kendi tek açık anahtarını değil, grubundaki tüm kullanıcıların anahtarlarını sağlar. Doğrulayıcı, gerçek imzacının grubun bir üyesi olduğuna ikna olur, ancak imzacıyı özel olarak tanımlayamaz. Orijinal protokol güvenilir bir üçüncü taraf (Grup Yöneticisi olarak adlandırılır) gerektiriyordu ve imzalayanın izini sürebilecek tek kişi oydu. Rivest ve arkadaşları tarafından[45] adresinde tanıtılan ve halka imza olarak adlandırılan bir sonraki versiyon, Grup Yöneticisi ve anonimlik iptali olmayan otonom bir şemaydı. Bu şemanın çeşitli modifikasyonları daha sonra ortaya çıktı: bağlanabilir halka imza[46,47,48] iki imzanın aynı grup üyesi tarafından üretilip üretilmediğini belirlemeye izin verdi, izlenebilir halka imza[49,50] aynı meta bilgiye (veya[50] açısından "etiket") göre iki mesajın imzacısını izleme imkanı sağlayarak aşırı anonimliği sınırladı. Benzer bir kriptografik yapı ad-hoc grup imzası olarak da bilinir[51,52] . Grup/ring imza şemaları daha ziyade sabit bir üye kümesini ima ederken, bu şema keyfi grup oluşumunu vurgular. Bizim çözümümüz çoğunlukla E. Fujisaki ve K. Fujisaki'nin "Traceable ring signature" adlı çalışmasına dayanmaktadır.

---

[44] David Chaum ve Eug`ene van Heyst. Grup imzaları. EUROCRYPT içinde, sayfa 257-265, 1991.

[45] Ronald L. Rivest, Adi Shamir, ve Yael Tauman. Bir sır nasıl sızdırılır. ASIACRYPT içinde, sayfa 552-565, 2001.

[46] Joseph K. Liu, Victor K. Wei, ve Duncan S. Wong. Ad hoc gruplar için bağlanabilir spontane anonim grup imzası (genişletilmiş özet). ACISP içinde, sayfa 325-335, 2004.

[47] Joseph K. Liu ve Duncan S. Wong. Bağlanabilir halka imzaları: Güvenlik modelleri ve yeni şemalar. ICCSA (2) içinde, sayfa 614-623, 2005.

[48] Man Ho Au, Sherman S. M. Chow, Willy Susilo ve Patrick P. Tsang. Kısa bağlanabilir halka imzaları tekrar gözden geçirildi. EuroPKI içinde, sayfa 101-115, 2006.

[49] Eiichiro Fujisaki. Rastgele oracle'lar olmadan doğrusal altı boyutta izlenebilir halka imzaları. CTRSA içinde, sayfa 393-415, 2011.

[50] Eiichiro Fujisaki ve Koutarou Suzuki. İzlenebilir halka imzası. Açık Anahtarlı Kriptografi içinde, sayfa 181-200, 2007.

[51] Ben Adida, Susan Hohenberger, ve Ronald L. Rivest. Ele geçirilmiş anahtar çiftlerinden ad-

hoc-grup imzaları. DIMACS Workshop on Theft in E-Commerce içinde, 2005.

[52] Qianhong Wu, Willy Susilo, Yi Mu ve Fangguo Zhang. Ad hoc grup imzaları. IWSEC içinde, sayfa 120-135, 2006.

Suzuki[53] . Orijinal algoritma ile bizim modifikasyonumuzu ayırt etmek için ikincisini tek seferlik halka imza olarak adlandıracağız ve kullanıcının kendi özel anahtarı altında yalnızca bir geçerli imza üretme kabiliyetini vurgulayacağız. İzlenebilirlik özelliğini zayıflattık ve yalnızca tek seferlikliği sağlamak için bağlanabilirliği koruduk: açık anahtar birçok yabancı doğrulama kümesinde görünebilir ve özel anahtar benzersiz bir anonim imza oluşturmak için kullanılabilir. Çifte harcama girişimi durumunda bu iki imza birbirine bağlanacaktır, ancak imzalayanın ifşa edilmesi bizim amaçlarımız için gerekli değildir.

4.2.1 Eliptik eğri parametreleri

Temel imza algoritmamız olarak D.J. Bernstein ve diğerleri tarafından geliştirilen ve uygulanan hızlı şema EdDSA'yı kullanmayı seçtik.[54] . Bitcoin'in ECDSA'sı gibi eliptik eğri ayrık logaritma problemine dayanmaktadır, bu nedenle şemamız gelecekte Bitcoin'e de uygulanabilir.

Yaygın parametreler şunlardır:

q: bir asal sayı; q = 2255 - 19;
d: Fq'nun bir elemanı; d = -121665/121666;
E: bir eliptik eğri denklemi; -x 2 + y 2 = 1 + dx2y 2 ; G:
bir taban noktası; G = (x, -4/5);
l: temel noktanın asal sırası; l = 2252 + 27742317777372353585193779088364849 3; Hs: bir kriptografik özet fonksiyonu {0, 1} ∗ → Fq;
Hp: deterministik bir hash fonksiyonu E(Fq) → E(Fq).

4.2.2 Terminoloji

Geliştirilmiş gizlilik, Bitcoin varlıkları ile karıştırılmaması gereken yeni bir terminoloji gerektirir.

özel ec-anahtarı standart bir eliptik eğri özel anahtarıdır: bir a ∈ [1, l - 1] sayısı;
açık ec-anahtarı standart bir eliptik eğri açık anahtarıdır: bir A = aG noktası;

tek seferlik anahtar çifti, özel ve genel ek-anahtarların bir çiftidir;

Özel kullanıcı anahtarı, iki farklı özel ek-anahtarın bir çiftidir (a, b);

izleme anahtarı bir özel ve genel ek-anahtar çiftidir (a, B) (burada B = bG ve a 6= b);

genel kullanıcı anahtarı (a, b)'den türetilen iki genel ek-anahtarın bir çiftidir (A, B);

standart adres, hata düzeltme ile insan dostu dizeye verilen genel kullanıcı anahtarının bir temsilidir;

kesilmiş adres, hata düzeltme ile insan dostu dizeye verilen bir genel kullanıcı anahtarının ikinci yarısının (B noktası) bir temsilidir.

[53] Eiichiro Fujisaki ve Koutarou Suzuki. İzlenebilir halka imzası. Açık Anahtarlı Kriptografi içinde, sayfa 181-200, 2007.

[54] Daniel J. Bernstein, Niels Duif, Tanja Lange, Peter Schwabe ve Bo-Yin Yang. Yüksek hızlı yüksek güvenlikli imzalar. J. Cryptographic Engineering, 2(2):77-89, 2012.

İşlem yapısı Bitcoin'deki yapıya benzer kalır: her kullanıcı birkaç bağımsız gelen ödeme seçebilir (işlem çıktıları), bunları ilgili özel anahtarlarla imzalayabilir ve farklı hedeflere gönderebilir.

Bir kullanıcının benzersiz özel ve açık anahtara sahip olduğu Bitcoin modelinin aksine, önerilen modelde bir gönderici, alıcının adresine ve bazı rastgele verilere dayalı olarak tek seferlik bir açık anahtar oluşturur. Bu anlamda, aynı alıcı için gelen bir işlem tek seferlik bir açık anahtara gönderilir (doğrudan benzersiz bir adrese değil) ve yalnızca alıcı fonlarını kullanmak için ilgili özel kısmı kurtarabilir (benzersiz özel anahtarını kullanarak). Alıcı, halka imza kullanarak fonları harcayabilir, mülkiyetini ve gerçek harcamasını anonim tutar. Protokolün detayları sonraki alt bölümlerde açıklanmaktadır.

4.3. Bağlantısız ödemeler

Klasik Bitcoin adresleri, bir kez yayınlandıktan sonra, gelen ödemeler için kesin bir tanımlayıcı haline gelir, onları birbirine bağlar ve alıcının takma adlarına bağlanır. Eğer birisi "bağlanmamış" bir işlem almak istiyorsa, adresini özel bir kanal aracılığıyla göndericiye iletmelidir. Aynı sahibine ait olduğu kanıtlanamayan farklı işlemler almak istiyorsa, tüm farklı adresleri oluşturmalı ve bunları asla kendi takma adıyla yayınlamamalıdır.

Çözümümüz, bir kullanıcının tek bir adres yayınlamasına ve koşulsuz, bağlantısız ödemeler almasına izin vermektedir. Her Dynex çıktısının hedefi (varsayılan olarak) alıcının adresi ve göndericinin rastgele verilerinden türetilen bir açık anahtardır. Bitcoin'e karşı ana avantajı, her hedef anahtarın varsayılan olarak benzersiz olmasıdır (gönderici aynı alıcıya yaptığı her işlem için aynı verileri kullanmadığı sürece). Bu nedenle, tasarım gereği "adresin yeniden kullanımı" gibi bir sorun yoktur ve hiçbir gözlemci herhangi bir işlemin belirli bir adrese gönderilip gönderilmediğini belirleyemez veya iki adresi birbirine bağlayamaz.

İlk olarak, gönderici kendi verilerinden ve alıcının adresinin yarısından paylaşılan bir sır elde etmek için bir Diffie-Hellman değişimi gerçekleştirir. Daha sonra paylaşılan sırrı ve adresin ikinci yarısını kullanarak tek seferlik bir hedef anahtarı hesaplar. Bu iki adım için alıcıdan iki farklı ec- anahtarı gerekir, bu nedenle standart bir Dynex adresi bir Bitcoin cüzdan adresinden neredeyse iki kat daha büyüktür. Alıcı ayrıca ilgili gizli anahtarı kurtarmak için bir Diffie-Hellman değişimi gerçekleştirir.

Standart bir işlem sırası aşağıdaki gibidir:

1. Alice, standart adresini yayınlamış olan Bob'a bir ödeme göndermek istiyor. Adresi açar ve Bob'un açık anahtarını (A, B) alır.

2. Alice rastgele bir r ∈ [1, l-1] üretir ve bir kerelik bir açık anahtar P = Hs(rA)G+ B hesaplar.

3. Alice P'yi çıktı için hedef anahtar olarak kullanır ve ayrıca R = rG değerini (Diffie-Hellman değişiminin bir parçası olarak) işlemin bir yerine paketler. Alice'in benzersiz açık anahtarlarla başka çıktılar oluşturabileceğini unutmayın: farklı alıcıların anahtarları (Ai
, Bi) aynı r ile bile farklı Pi anlamına gelir.

4. Alice işlemi gönderir.

5. Bob geçen her işlemi kendi özel anahtarı (a, b) ile kontrol eder ve P 0 = Hs(aR)G + B'yi hesaplar. Alice'in Bob'un alıcı olduğu işlemi bunlar arasındaysa, aR = arG = rA ve P 0 = P olur.

6. Bob ilgili tek seferlik özel anahtarı kurtarabilir: x = Hs(aR) + b, yani P = xG. Bu çıktıyı istediği zaman x ile bir işlem imzalayarak harcayabilir.

Sonuç olarak Bob, bir izleyici için **bağlantısı kurulamayan** tek seferlik açık anahtarlarla ilişkilendirilmiş gelen ödemeleri alır. Bazı ek notlar:

• Bob işlemlerini "tanıdığında" (bkz. 5. adım) pratikte özel bilgilerinin sadece yarısını kullanır: (a, B). İzleme anahtarı olarak da bilinen bu çift üçüncü bir tarafa (Carol) verilebilir. Bob yeni işlemlerin işlenmesi için Carol'ı görevlendirebilir. Bob'un Carol'a açıkça güvenmesi gerekmez çünkü Carol, Bob'un tam özel anahtarı (a, b) olmadan tek seferlik gizli anahtar p'yi kurtaramaz. Bu yaklaşım, Bob'un bant genişliği veya hesaplama gücü olmadığında (akıllı telefonlar, donanım cüzdanları vb.) kullanışlıdır.

• Alice, Bob'un adresine bir işlem gönderdiğini kanıtlamak isterse, r'yi bildiğini kanıtlamak için ya ifşa edebilir ya da herhangi bir tür sıfır bilgi protokolü kullanabilir (örneğin işlemi r ile imzalayarak).

• Bob gelen tüm işlemlerin bağlanabildiği denetim uyumlu bir adrese sahip olmak isterse, ya izleme anahtarını yayınlayabilir ya da kesilmiş bir adres kullanabilir. Bu adres yalnızca bir açık ek-anahtar B'yi temsil eder ve protokolün gerektirdiği geri kalan kısım bundan şu şekilde türetilir: a = Hs(B) ve A = Hs(B)G. Her iki durumda da herkes Bob'un gelen tüm işlemlerini "tanıyabilir", ancak elbette hiçbiri gizli anahtar b olmadan bunların içindeki fonları harcayamaz.

4.4. Tek seferlik yüzük imzaları

Tek seferlik halka imzalara dayalı bir protokol, kullanıcıların koşulsuz bağlantı kurulamazlık elde etmesine olanak tanır. Ne yazık ki, sıradan kriptografik imza türleri, işlemlerin ilgili göndericilerine ve alıcılarına kadar izlenmesine izin verir. Bu eksikliğe yönelik çözümümüz, şu anda elektronik para sistemlerinde kullanılanlardan farklı bir imza türü kullanmakta yatmaktadır.

İlk olarak, elektronik paraya açıkça atıfta bulunmadan algoritmamızın genel bir tanımını sunacağız. Bir kerelik halka imza dört algoritma içerir:

GEN: genel parametreleri alır ve bir ec-çifti (P, x) ve bir genel anahtar I çıktısı verir.

SIG: bir m mesajı, {Pi}i6=s açık anahtarlarından oluşan bir S 0 kümesi, bir (Ps, xs) çifti alır ve bir σ imzası ve bir S = S 0 ∪ {Ps} kümesi çıktısı verir.

VER: bir m mesajı, bir S kümesi, bir σ imzası alır ve "doğru" veya "yanlış" çıktısı **verir.**

LNK: bir I = {Ii} kümesi, bir σ imzası alır ve "bağlantılı" veya "bağımsız" çıktılarını verir.

Protokolün arkasındaki fikir oldukça basittir: bir kullanıcı, benzersiz bir açık anahtar yerine bir açık anahtar kümesi tarafından kontrol edilebilen bir imza üretir. İmzalayanın kimliği, sahibi aynı anahtar çiftini kullanarak ikinci bir imza üretene kadar açık anahtarları kümede bulunan diğer kullanıcılardan ayırt edilemez.

GEN: İmzalayan rastgele bir gizli anahtar x ∈ [1, l - 1] seçer ve buna karşılık gelen açık anahtar P = xG'yi hesaplar. Ek olarak, "anahtar görüntüsü" olarak adlandıracağımız başka bir açık anahtar I = xHp(P) hesaplar.

SIG: İmzalayan, [21]'deki teknikleri kullanarak etkileşimli olmayan sıfır bilgi kanıtı ile tek seferlik bir halka imza oluşturur. Diğer kullanıcıların açık anahtarları Pi, kendi anahtar çifti (x, P) ve anahtar görüntüsü I arasından n'nin rastgele bir alt kümesi S 0'ı seçer. 0 ≤ s ≤ n, imzacının S'deki gizli indeksi olsun (böylece açık anahtarı Ps olur). İmzalayan (1 . . . l)'den rastgele bir {qi | i = 0 . . . n} ve {wi | i = 0 . . . n, i 6= s} seçer ve aşağıdaki dönüşümleri uygular:

$$L_i = \begin{cases} q_i G, & \text{if } i = s \\ q_i G + w_i P_i, & \text{if } i \neq s \end{cases}$$

$$R_i = \begin{cases} q_i \mathcal{H}_p(P_i), & \text{if } i = s \\ q_i \mathcal{H}_p(P_i) + w_i I, & \text{if } i \neq s \end{cases}$$

Bir sonraki adım, interaktif olmayan meydan okumayı almaktır:

$$c = \mathcal{H}_s(m, L_1, \ldots, L_n, R_1, \ldots, R_n)$$

Son olarak imzalayan yanıtı hesaplar:

$$c_i = \begin{cases} w_i, & \text{if } i \neq s \\ c - \sum_{i=0}^{n} c_i \mod l, & \text{if } i = s \end{cases}$$

$$r_i = \begin{cases} q_i, & \text{if } i \neq s \\ q_s - c_s x \mod l, & \text{if } i = s \end{cases}$$

Ortaya çıkan imza σ = (I, c1, . . . , cn, r1, . . . , rn) şeklindedir.

VER: Doğrulayıcı, ters dönüşümleri uygulayarak imzayı kontrol eder:

$$\begin{cases} L_i' = r_i G + c_i P_i \\ R_i' = r_i \mathcal{H}_p(P_i) + c_i I \end{cases}$$

Son olarak, doğrulayıcı aşağıdaki durumları kontrol eder

$$\sum_{i=0}^{n} c_i \stackrel{?}{=} \mathcal{H}_s(m, L_0', \ldots, L_n', R_0', \ldots, R_n') \mod l$$

Bu eşitlik doğruysa, doğrulayıcı LNK algoritmasını çalıştırır. Aksi takdirde doğrulayıcı imzayı reddeder.

LNK: Doğrulayıcı, I'nın geçmiş imzalarda kullanılıp kullanılmadığını kontrol eder (bu değerler I kümesinde saklanır). Birden fazla kullanım, iki imzanın aynı gizli anahtar altında üretildiği anlamına gelir. Protokolün anlamı: İmzalayan L-dönüşümlerini uygulayarak en az bir Pi = xG olacak şekilde x bildiğini kanıtlar. Bu kanıtı tekrarlanamaz hale getirmek için anahtar görüntüsünü I = xHp(P) olarak tanıtıyoruz. İmzalayan hemen hemen aynı ifadeyi kanıtlamak için aynı katsayıları (ri , ci) kullanır: öyle bir x bilir ki en az bir Hp(Pi) = I - x -1 .

Eğer x → I eşlemesi bir enjeksiyon ise:

1. Hiç kimse açık anahtarı anahtar görüntüsünden kurtaramaz ve imzalayanın kimliğini belirleyemez;
2. İmza sahibi farklı I'lar ve aynı x ile iki imza atamaz.

4.5. Bir Dynex işlemi

Bob, her iki yöntemi (bağlantısız açık anahtarlar ve izlenemez halka imza) birleştirerek orijinal Bitcoin şemasına kıyasla yeni bir gizlilik seviyesine ulaşır. Anonim işlemleri almaya ve göndermeye başlamak için yalnızca bir özel anahtar (a, b) saklamasını ve (A, B) yayınlamasını gerektirir. Bob her bir işlemi doğrularken, bir işlemin kendisine ait olup olmadığını kontrol etmek için çıktı başına yalnızca iki eliptik eğri çarpımı ve bir toplama işlemi gerçekleştirir. Bob her çıktısı için tek seferlik bir anahtar çifti (pi , Pi) elde eder ve bunu cüzdanında saklar. Herhangi bir girdinin aynı sahibinin olduğu ancak

tek bir girdide görünmeleri halinde dolaylı olarak kanıtlanabilir.

işlem. Aslında tek seferlik halka imzası nedeniyle bu ilişkiyi kurmak çok daha zordur.

Halka imza ile Bob her girdiyi bir başkasınınkiler arasında etkili bir şekilde gizleyebilir; tüm olası harcayıcılar eşitlenebilir olacaktır, hatta önceki sahibi (Alice) herhangi bir gözlemciden daha fazla bilgiye sahip olmayacaktır.

Bob işlemini imzalarken kendi çıktısıyla aynı miktarda n adet yabancı çıktı belirtir ve bunların hepsini diğer kullanıcıların katılımı olmadan karıştırır. Bob'un kendisi (ve başkaları) bu ödemelerden herhangi birinin harcanıp harcanmadığını bilmez: bir çıktı binlerce imzada bir belirsizlik faktörü olarak kullanılabilir ve asla bir gizleme hedefi olarak kullanılamaz. Çifte harcama kontrolü LNK aşamasında, kullanılan anahtar görüntü setine karşı kontrol edilirken gerçekleşir. Bob belirsizlik derecesini kendisi seçebilir: n = 1 çıktıyı harcama olasılığının %50 olduğu anlamına gelir, n = 99 ise %1 verir. Ortaya çıkan imzanın boyutu doğrusal olarak O(n+1) kadar artar, bu nedenle geliştirilmiş anonimlik Bob'a ekstra işlem ücretlerine mal olur. Ayrıca n = 0 olarak ayarlayabilir ve halka imzasını yalnızca bir elemandan oluşacak şekilde yapabilir, ancak bu onu anında bir harcayıcı olarak ortaya çıkaracaktır.

5. Dayanıklılık ve Hayatta Kalabilirlik

Bir platform olarak doğası gereği Dynex'in en azından ortalama bir insanın ömrü boyunca **uzun vadeli** sözleşmeleri desteklemesi beklenmektedir. Buna rağmen, genç akıllı sözleşme platformları bile performans düşüşü ve dış koşullara uyum sağlayamama sorunu yaşamaktadır. Bu nedenle, bir kripto para birimi, bu sorunu çözmek için bir hard-fork sağlamak için küçük bir geliştirici grubuna bağlı olacaktır, aksi takdirde hayatta kalamayacaktır. Örnek olarak, Ethereum ağı Proof-of-Work mutabakat algoritmasını kullanmaktadır ve yakın gelecekte Proof-of-Stake'e geçmeyi vaat etmektedir. Bununla birlikte, Proof-of-Stake geliştirmesindeki gecikmeler, birkaç sabit çatalın sabitlenmesiyle sonuçlandı[55] ve topluluk hala bir sonraki sert çatalı uygulamak için çekirdek geliştiricilere güveniyor.

İlk yaygın beka sorunu, geliştiricilerin genellikle yeterli araştırma ve test yapmadan popülerlik peşinde ad-hoc çözümler uygulamasıdır. Kaçınılmaz olarak, bu tür çözümler hatalara yol açacak, bu da aceleci hata düzeltmelerine yol açacak, bu da daha sonra bu hata düzeltmelerinin hata düzeltmelerine yol açacak, vb. ağı güvenilmez ve daha da az güvenli hale getirecektir. Dynex, kısa vadeli yenilikler aramak yerine **istikrarlı, iyi test edilmiş çözümler** kullanmaya odaklanmaktadır. Dynex'te kullanılan çözümlerin çoğu

[55] Ethereums blok zinciri bir kez daha zorluk bombası etkisini hissediyor. [Çevrimiçi]. Mevcut: https://www.coindesk.com/ ethereum-blockchain-feeling-the-difficulty-bomb-effect

Dynex,[56,57,58,59,60,61] adresindeki hakemli konferanslarda sunulan ve topluluk içinde geniş çapta tartışılan makalelerde resmileştirilmiştir.

Merkeziyetsizlik (ve dolayısıyla beka), güvenli ve güvenilir hafif istemcilerin yokluğu nedeniyle de zorlanmaktadır. Dynex bu sorunu yeni bir sorun yaratmadan çözmeyi amaçlamaktadır. Dynex bir Proof-of-Work blok zinciri olduğundan, blok içeriğinden küçük bir başlık kolayca çıkarılabilir. Bu başlık tek başına üzerinde yapılan işin doğrulanmasını sağlar ve bir başlık zinciri ağ ile senkronizasyon için en uygun zinciri seçmek için yeterlidir. **Başlık zincirleri**, tam blok zincirinden çok daha küçük olmasına rağmen, yine de zaman içinde doğrusal olarak büyür. Hafif istemciler üzerine yapılan son araştırmalar, hafif istemcilerin daha da küçük miktarda veri indirerek ağ ile senkronize olmalarını ve böylece cep telefonları gibi güvenilmeyen düşük uçlu cihazların ağa katılmalarını sağlayan bir yol göstermiştir[62,63] . Dynex kimliği doğrulanmış bir durum kullanır ve istemcilerin bir blokta yer alan işlemlerin doğruluğunun kanıtlarını indirmelerine olanak tanır. Bu şekilde Dynex, blok zinciri boyutundan bağımsız olarak cep telefonu kullanan herkes tarafından erişilebilir hale gelmektedir.

Ayrıca üçüncü bir potansiyel sorun daha vardır: hafif istemciler Dynex kullanıcıları için sorunu çözerken, Dynex madencileri için sorunu çözmezler.

---

[56] L. Reyzin, D. Meshkov, A. Chepurnoy ve S. Ivanov, "Kripto para birimlerine uygulamalarla kimliği doğrulanmış dinamik sözlüklerin iyileştirilmesi," Uluslararası Finansal Kriptografi ve Veri Güvenliği Konferansı. Springer, 2017, s. 376-392.

[57] D. Meshkov, A. Chepurnoy ve M. Jansen, "Kısa makale: Revisiting difficulty control for blockchain systems", Data Privacy Management, Cryptocurrencies and Blockchain Technology içinde. Springer, 2017, s. 429-436.

[58] A. Chepurnoy, V. Kharin, ve D. Meshkov, "Kripto para ücretlerine sistematik bir yaklaşım," IACR Cryptology ePrint Archive, vol. 2018, p. 78, 2018.

[59] A. Chepurnoy, V. Kharin ve D. Meshkov, "Evrensel turing makinesi olarak kendi kendini yeniden üreten paralar", Veri Gizliliği Yönetimi, Kripto Para Birimleri ve Blok Zinciri Teknolojisi. Springer, 2018, s. 57-64.

[60] A. Chepurnoy ve M. Rathee, "Checking laws of the blockchain with property-based testing," in Blockchain Oriented Software Engineering (IWBOSE), 2018 International Workshop on. IEEE, 2018, s. 40-47.

[61] T. Duong, A. Chepurnoy, ve H.-S. Zhou, "Multi-mode cryptocurrency systems," in Proceedings of the 2nd ACM Workshop on Blockchains, Cryptocurrencies, and Contracts. ACM, 2018, s. 35-46.

[62] A. Kiayias, A. Miller ve D. Zindros, "Proof-work'ün etkileşimli olmayan kanıtları," Kriptoloji ePrint Arşivi, Rapor 2017/963, 2017. Erişim tarihi: 2017-10-03, Tech. Rep., 2017.

[63] L. Luu, B. Buenz ve M. Zamani, "Flyclient super light client for cryptocurrencies," IACR Cryptology ePrint Archive, 2019. [Çevrimiçi]. Mevcut: https://eprint.iacr.org/2019/226

verimli işlem doğrulaması için tüm durumu saklar. Şu anda, blok zinciri sistemleri kullanıcıların bu durumda rastgele veri depolamasına izin vermektedir. Bu verilerin sonsuza dek saklanması nedeniyle, zaman içinde sonsuz bir şekilde büyüyen çok fazla toz oluşturur[64] . Durumun rastgele erişimli bellek için çok büyük olduğu durumlarda, bir düşman, madencinin deposuna rastgele erişim gerektirdiğinden doğrulanması çok yavaş olan işlemler oluşturabilir. Sonuç olarak, 2016 yılında Ethereum'da meydana gelen gibi DoS saldırıları meydana gelebilir[65] . Topluluğun bu tür saldırılardan korkmasının yanı sıra madenciler ve kullanıcılar için telafisi olmayan "durum şişmesi" sorunu, ölçeklendirme çözümlerinin uygulanmasını engellemiş olabilir (örneğin daha büyük blok boyutları gibi). Bu nedenle Dynex bir **depolama kirası bileşeni içermektedir**: bir çıktı taşınmadan dört yıl boyunca durumda kalırsa, madenci bayt başına küçük bir ücret talep edebilir.

Normal bulut depolama hizmetlerine benzer şekilde, bu konsept kripto paralar için daha yeni önerilmiştir[66] ve birkaç önemli sonucu vardır. İlk olarak, emisyon tamamlandıktan sonra madenciliğin istikrarsız hale gelebildiği Bitcoin ve diğer iş kanıtı para birimlerinin aksine Dynex madenciliğinin her zaman istikrarlı olmasını sağlar[67] . İkinci olarak, devletin boyutunun büyümesi öngörülebilir ve kontrol edilebilir hale gelir, böylece Dynex madencileri donanım gereksinimlerini daha etkili bir şekilde yönetebilirler. Son olarak, madenciler eski kutulardan depolama ücreti toplayarak coinleri dolaşıma geri döndürebilir ve böylece kayıp anahtarlar nedeniyle dolaşımdaki arzın sürekli olarak azalmasını önleyebilir[68] . Tüm bu faktörlerin Dynex'in hem teknik hem de ekonomik olarak uzun vadede yaşayabilirliğini desteklemesi beklenmektedir.

---

[64] C. P´erez-Sol`a, S. Delgado-Segura, G. Navarro-Arribas, ve J. HerreraJoancomart´ı, "Another coin bites the dust: an analysis of dust in utxobased cryptocurrencies," Royal Society open science, vol. 6, no. 1, p. 180817, 2019.

[65] Ethereum ağ saldırganlarının ip adresi izlenebilir. [Çevrimiçi]. Mevcut: https://www.bokconsulting.com.au/blog/ ethereum-network-attackers-ip-address-is-traceable/

[66] A. Chepurnoy ve D. Meshkov, "Blok zinciri sistemlerinde alan kıtlığı ekonomisi üzerine." IACR Kriptoloji ePrint Arşivi, cilt 2017, s. 644, 2017.

[67] M. Carlsten, H. Kalodner, S. M. Weinberg ve A. Narayanan, "Blok ödülü olmadan bitcoin'in istikrarsızlığı üzerine," 2016 ACM SIGSAC Bilgisayar ve İletişim Güvenliği Konferansı Bildirileri. ACM, 2016, s. 154-167.

[68] E. Krause, "Tüm bitcoin'in beşte biri kayıp. bu kripto avcıları yardımcı olabilir," 2018.

6. Dynex'in Yerel Jetonu

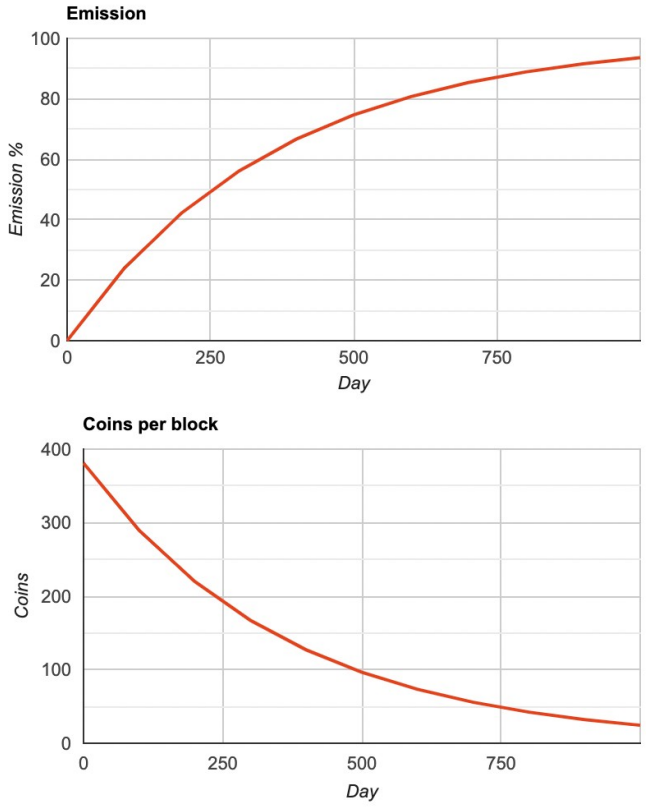
Dynex'in yerel token'ı **DNX olarak adlandırılır** ve nanoDNX adı verilen 10^9 daha küçük birime bölünebilir (bir nanoDNX, bir DNX'in milyarda birine eşittir). Toplamda en fazla **100.000.000,0 DNX** mevcut olacaktır. DNX, aşağıda belirtilen bir dizi nedenden ötürü Dynex platformunun istikrarı ve güvenliği için hayati önem taşımaktadır. Token'lar önceden belirlenmiş ve sabit kodlanmış bir programa göre yayılacaktır.

6.1. Emisyon

İlk madeni para teklifi ("ICO"), **ön madencilik** ve geliştiriciler için **madeni para düşüşü** veya tokena yerleştirilmiş başka herhangi bir gizli teşvik yoktur. Dynex ana ağının başlatılmasının ardından, tüm 100.000.000.0 DNX tokenleri emisyon programına göre kullanıma sunulacaktır. Emisyon sürecinin sorunsuz olmasını sağlamak için blok ödülleri için aşağıdaki formülü kullanıyoruz:

$$BaseReward = (MSupply - A) \gg 18,$$

Burada A önceden üretilmiş madeni paraların miktarıdır. Aşağıdaki grafik emisyonu grafiksel olarak göstermektedir:



Şekil 2: DNX Emisyon Çizelgesi

7. Yeni Nesil Nöromorfik Hesaplama

Bizim görüşümüze göre yeni nesil bilgi işlem yetenekleri **herkes tarafından erişilebilir** olmalıdır. Bilgi işlemin geleceği olacağına inandığımız nöromorfik bilgi işlemin özgürleştirilmesi ve hızlandırılması için bir platform olarak Dynex, **tescilli devreyi** (Dynex'in Nöromorfik Çipi gibi) **genel kullanıma açık** nöromorfik bilgi işlem **altyapısı** (Intel Lohi[69] , IBM TrueNorth[70] veya California Üniversitesi'nin NeuRRAM[71] gibi) ile **yazılım ve algoritma** geliştiricileri ile birleştirmektedir.

Dynex, üzerine inşa edilecek **uygulamalar** ve algoritmalar **için temel** sağlar. Bir platform, nöromorfik çip kümelerini çalıştıran ana bilgisayarları birbirine bağlayarak kullanıcıların ve uygulamaların bu yeni nesil donanıma erişmesini sağlar. Dynex yerel belirteci, platform üzerinde hesaplama süresi alışverişi yapmak için kullanılır.

- **Dynex operatörleri** nöromorfik bilgi işlem altyapısını korur ve işletir. Bu, Intel Lohi, IBM TrueNorth veya Kaliforniya Üniversitesi NeuRRAM gibi genel donanımlar kullanılarak ya da FPGA'lar Dynex Nöromorfik Çip devre tasarımıyla programlanarak gerçekleştirilebilir. ASIC'lerin proof-of-work token madenciliğindeki hakimiyeti nedeniyle, yüksek performanslı yeni nesil nöromorfik bilgi işlem kümelerine dönüştürülebilecek önemli miktarda atıl FPGA altyapısı mevcuttur. Dynex'in operatörleri bilgi işlem kaynaklarını Dynex'in yerel tokenı olan DNX karşılığında sunmaktadır.

- **Yazılım geliştiriciler,** operatörler tarafından sağlanan nöromorfik bilgi işlem altyapısı üzerinde çalışan uygulamalar geliştirmektedir. Basit ve öğrenmesi kolay bir komut dosyası dili olan Dynexscript ile problemler ve hesaplama görevleri nöromorfik hesaplama kümelerinde yürütülmek üzere yeniden formüle edilebilir. Bu altyapıya erişim, yazılım geliştiricilerin ve araştırmacıların mevcut ve Kuantum metodolojilerinden daha iyi performans gösterebilen yüksek performanslı, yüksek verimli bilgi işlem sistemleri uygulamalarına olanak tanır. Dynex'in yerel tokenı DNX, bilgi işlem kaynaklarının kullanımı için tazminat olarak kullanılmaktadır.

---

[69] https://www.intel.com/content/www/us/en/research/neuromorphic-computing.html

[70] Krishna, R. & Nandini, Usha & Mayan, J. & Sawarn, Nidhi. (2021). Nöromorfik Hesaplama - Gelişimin İlkesi. 10.4108/eai.7-6-2021.2308573.

71 https://www.sciencedaily.com/releases/2022/08/220817114253.htm

- Donanımın yeniden kullanılmasıyla ilişkili çevresel faydaların yanı sıra, **kullanıcılar** Dynex'in yerel belirteci DNX'i de elde edebilir ve böylece donanımın yeniden kullanılmasının bir sonucu olarak yakın gelecekte katlanarak büyüyecek bir pazar olan Moore yasası sonrası büyüyen bilgi işlem pazarı segmentinde yer alabilirler. Vizyonumuz, sıradan insanların gelecekte hızla artan bilgi işlem gücünden faydalanabilmesidir.

7.1. Örnek

Nöromorfik hesaplamanın üstün performansını göstermek için aşağıdaki örnekte, karmaşıklığı $O(n^{100,000})$ olan bir problem formülasyonunun Dynex Nöromorfik Çip kullanılarak çözüldüğü bir kısıtlama memnuniyeti probleminin uygulaması gösterilmektedir. Problem 100.000 benzersiz değişkenden oluşmaktadır. Mevcut ve Kuantum teknolojisine dayalı mevcut metodolojiler (Shor'**un** algoritması[72] ile karmaşıklığı $O(n^{50,000})$ **)'e** indirgemek) bir çözüm bulmak için **evrenin varoluşundan daha uzun bir süre** gerektireceğinden günümüzde bu problemi çözemez. Dynex Nöromorfik Çip, doğasında var olan paralelleştirme, uzun menzilli düzen ve instantonları kullanma kabiliyeti sayesinde problemi **2.23 saniyede** çözmektedir (Şekil 2).

Güncel Yöntem	**Kuantum Yöntem**	**Dynex Nöromorfik Çip**
$O(n^{100,000})$	$O(n^{50,000})$	2.23s
*Daha uzun evren çıkar	*Daha uzun evren var	

Not: Bu sonuçlar GitHub depomuzda yayınlanan referans uygulamalarımızla doğrulanabilir ve çoğaltılabilir.

[72] Mosca, M., Verschoor, S.R. (Kuantum) SAT çözücüleriyle yarı asal sayıların çarpanlarına ayrılması. *Sci Rep* 12, 7982 (2022). https://doi.org/10.1038/s41598-022-11687-7