Cross-Disciplinary AI Supply Chain Risk Assessment

Angela Mison[1], Gareth Davies[2] and Richard Ward[1]
[1]University of South Wales, Pontypridd, UK
[2]University of the West of England, Bristol, UK

angela.mison@southwales.ac.uk
Gareth13.Davies@uwe.ac.uk (corresponding author)
richard.ward@southwales.ac.uk

Abstract: While AI remains chip based and part of both commercial and national strategic superiority goals, it is useful to examine the security and risks associated with achieving those goals. The future strategy rests perilously on an unstable inverted triangle of financial and economic reality. This paper presents the AI chip supply chain as an inverted triangle which base/apex is dependent on a global single supplier with the capability of producing equipment essential for their manufacture. It highlights the dependence on a single company for the fabrication of those chips, and the security risks associated with that supplier being Taiwanese in limited foreign ownership. It is suggested that the increasing tensions between China and the USA have resulted, in part, from this dependence, which was demonstrated by the supply chain crisis resulting from Covid-19. The attempt to reduce this dependence led to the CHIPS and Science Act 2022, signed into law by President Biden. In part of the inverted triangle are found Big Tech and the major Cloud Service Providers. They vary between 60% - 80% of their market capital being in financial institutional ownership, most of which is held by a very limited number of institutions, not all of whom are publicly quoted. To doubt the influence wielded by those financial institutions, just a single institution with major Big Tech and Cloud holdings has, at 31 December 2022, USD 8.59 trillion of assets under management. This represents economic power and places it between the equivalent Gross Domestic Product of China (USD 19.37 trillion) and Japan (USD 4.41 trillion) the second and third entries behind the USA in the GDP rankings. Financial institutions are market driven to achieve growth, contribute to economic stability, and are to an extent regulated by unelected vested interests and organisations. The battlefield for national supremacy of AI may concern chips, until the arrival of quantum AI. Current Chinese economic woes are providing the momentum for pre-emptive strikes at the semiconductor industry, and an inverted triangle is neither a secure nor stable structure for a supply chain.

Keywords: AI, Aladdin, GAMMA, TSMC, ASML

1. Background

Chips for Artificial Intelligence (AI) are the most powerful chips manufactured. AI systems' learning and decision making require them to process vast quantities of data obtained through historical datasets and surveillance capitalism platforms. Currently, the fabrication process for these chips requires extreme ultraviolet (EUV) lithography to mass produce patterns on silicon. EUV lithography systems provide the highest resolution in high volume manufacturing (ASML, 2022).

The principles associated with EUV lithography can be thought of as similar to layering photographic prints of up to 100 layers on a single chip. Of the EUV lithography machines currently in existence, these operate at 13.5nm (ASML, 2023a), but research and development are ongoing. It is intended that High-NA EUV lithography which will advance Moore's Law towards the logic 2nm technology generation will go on pilot release in 2023 before full scale production in 2025 (De Simone, et al., 2021). Without EUV lithography, AI would be dependent on less powerful chips which would increase its cost in terms of creation and maintenance.

ASML, a Dutch company, has a monopoly in EUV lithography and its underlying technologies. It is the world's unique supplier. In terms of financials, the complexity and cost of EUV lithography machines is such that in the second quarter of 2023, ASML sold 107 new units and 6 used units for a total of USD 6 billion, of which USD 1.7 billion is attributable to EUV lithography units, providing a gross profit margin of 51.3% (ASML, 2023b). ASML's primary customer for EUV lithography machines is Taiwan Semiconductor Manufacturing Company (TSMC).

The United States has negotiated restrictions on sales of ASML EUV lithography systems, in particular to China and its Semiconductor Manufacturing International Corp (SMIC) (Office of Foreign Assets Control, 2021). The US Dept of Commerce designated SMIC as a 'military end user' in October 2020 and applies a 'presumption of denial' for products required to produce chips at 10nm or below.

Some reverse engineering by SMIC, which targets and hires former TSMC employees would appear to have taken place. A lawsuit dated 2004 (Clendenin, 2004) alleged theft of intellectual property from TSMC by SMIC, and was settled in 2005 (Lemon, 2005). In December 2020 the former Head of TSMC R&D, Chiang Shang-yi was appointed Vice-Chairman of SMIC. SMIC is now under investigation for sanctions' violations relating to

provision of advanced 7nm chips for use in Huawei's Mate 60 Pro smartphone, which chips, it is asserted by the US Dept of Commerce, cannot be produced without US technology (Che, 2023). Huawei was placed on the Entity List in May 2019.

TSMC supplies 30% of the world semiconductor market excluding memory output (Taiwan Semiconductor Manufacturing Company, 2023). It is reputed to supply 90% of the AI chip requirement, with Samsung fulfilling the balance. Affecting NVIDIA, AMD, Apple and many others (Shilov, 2023) for the next 18 months, TSMC announced it can satisfy only 80% of demand. This is due to lack of advanced chip packaging services in the manufacturing process which combines a graphics processor unit with six high bandwidth memory chips. Chip packaging provides high speed data transmission and performance that enables training in AI (asia.nikkei.com, 2023). AMD, Intel, and Samsung are potential competitors in this area.

2. AI Development

The discussion on and actual regulation of AI may have slowed down the requirement for TSMC's output. The European Union is the first to regulate AI through its AI Act (News European Parliament, 2023), requiring national supervisory authorities and establishment of a European Artificial Intelligence Board. This publication followed the call for a moratorium on AI citing Risks to Society by over 1,000 technology leaders in March 2023 (Loizos, 2023), although it had probably been in preparation for some time. Nonetheless, with a predicted compound annual growth rate (CAGR) of around 40% (Precedence Research, 2023), far exceeding that of the predicted CAGR of 18% for Cloud (Markets and Markets, 2022), after a period of evaluation of any regulations, it is expected that Big Tech will continue apace with AI development. Indeed, there is a feeding frenzy in stock market as Apple reaches a market Capitalisation value of USD 2.8 trillion (Stock Analysis, 2023).

The predominant end users of the high specification chips produced by TSMC for use in AI systems are anticipated being those Big Tech players, Alphabet (Google), Apple, Amazon, Meta (Facebook), and Microsoft (GAMMA). There will be others, but with for example, Apple having a 23% interest in TSMC production, these are considered to be the majors. Investment strategists suggest that there is a superseding 'Magnificent Seven' which comprises the GAMMA grouping indicated above with the addition of NVIDIA and Tesla (Mitra, 2023). These seven organisations are propping up the Nasdaq with year to date (16 June 2023) stock price increases from between 40% for Apple, Microsoft, Amazon, and Alphabet, to 108% for Tesla, 134% for Meta, and 192% for Nvidia.

In terms of AI development, and for the purposes of this paper, only the GAMMA grouping will be considered further. It is interesting to consider the ownership of the GAMMA grouping by financial institutions (shown in table 1). This is shown in the table below:

Table 1: The percentage of the GAMMA grouping held by financial institutions

GAMMA Group	%
Alphabet (Google)	78.93
Meta (Facebook)	76.35
Microsoft	73.21
Apple	61.32
Amazon	60.53

Further analysis of those financial institutions demonstrates the value of holdings of three of the world's largest financial institutions, Vanguard, BlackRock, and State Street Corp. The holdings shown in table 2 are for those investments directly held by the named institutions and does not include any investments made indirectly by other organisations in which they have holdings. It is likely that the total value of ownership of the three aforementioned financial institutions is obscured by such indirect investment. Like other financial institutions and mutual funds, they have invested and managed a proportion of their assets under management (AUM) in the technology sector.

Table 2: The value of holdings of the GAMMA grouping held by Vanguard, BlackRock, and State Street Corp

GAMMA Group	Market Capitalisation	Ownership by Vanguard		Ownership by BlackRock		Ownership by State Street Corp	
	USD Trillion	USD Billion	%	USD Billion	%	USD Billion	%
Apple	2.799	233	8.38	183	6.62	102	3.69
Microsoft)	2.401	210	8.74	174	7.24	94	3.93
Alphabet (Google)	1.650	63	8.21	54	7.12	28	3.66
Amazon	1.421	100	7.05	84	5.92	46	3.23
Meta (Facebook)	0.784	54	8.14	46	6.88	13	1.98
Totals	**9.055**	**660**	**-**	**541**	**-**	**283**	**-**

With holdings in the GAMMA grouping of this magnitude, financial institutions and mutual funds can directly influence the outcome of shareholder voting and enforce or veto policies or lines of investigation. In general, the financial institutions will have a relationship with the Executive of these companies.

AUM represents the economic power that the financial institutions have. There is a degree of similarity between the economic power accorded to a country through its Gross Domestic Product (GDP) ranking and the value of AUM of a financial institution. The three financial institutions under consideration AUM are shown in table 3.

Table 3: The AUM of Vanguard, BlackRock, and State Street Corp

Financial Institution	Value of Assets
BlackRock	USD 8.5 trillion
Vanguard	USD 7.1 trillion
State Street Corp	USD 3.5 trillion

The AUM of BlackRock and Vanguard places them as an equivalent to the third and fourth national GDP behind USA, between the equivalent GDP China (USD 19.37 trillion) and Japan (USD 4.41 trillion). State Street Corp is not far behind. The influence and economic power of financial institutions and mutual funds cannot be doubted or ignored.

Caution should be exercised when considering these three financial institutions as independent entities. Quite apart from a circular ownership between themselves, each institution uses a model-based risk management platform, Aladdin. Aladdin was originally built within BlackRock to effect monitoring and analysis of the risk profile of their investments.

3. Aladdin

Over the years access to Aladdin has been sold. Aladdin has become a fully-fledged AI system, evolving during the thirty or so years it has been in operation. It now executes approximately 70% of high frequency trades in the US without any human intervention. Aladdin controls approximately 10% of global investments and its expansion into investment of organisations which bulk purchase and outbid individuals in the real estate market is seen as partially responsible for escalation of house prices.

The potential of a 40% CAGR for AI and a total market valuation of USD 196.63 billion in 2023 increasing to a revenue forecast of USD 1.8 trillion in 2030 provides an expectation of growth and income in the intervening years (Grand View Research, 2023a). This is reinforced where the underlying organisation is also a Cloud Service Provider with a 20% CAGR and a total market valuation for Cloud computing of USD 678 billion in 2023 increasing to USD 2.4 trillion in 2030 (Fortune Business Insights, 2023). The figures provided by Grand View Research (2023b) are slightly more conservative.

The use of cloud services by organisations suggests that cloud adoption could generate an additional USD 3 trillion in EBITDA value by 2030 (McKinsey & Company, 2022). This adds indirectly to the attractiveness of investment in technology companies to Aladdin. The calculations for growth and increased revenues both to underlying investments and to the financial institutions themselves makes the logic of investment in these areas undeniable and irrefutable to Aladdin.

The mission statement of BlackRock is assumed to infuse the objectives and behaviour of Aladdin. That mission is to create economic opportunity for all by making investing more accessible. Viewing the AUM figures, it could be said to have achieved its mission, though it is possible that Aladdin is reinforcing particular behaviours of and in the markets.

The head of BlackRock is a member of the trustees of the World Economic Forum (WEF) which espouses a concept of equality in a better world. This concept allies with the original mission statement of BlackRock and is expected to have contributed to the evolution of Aladdin. However, in 2016, a discussion paper was presented to the WEF in which a potential life was described (Auken, 2016). An urbanised population owned nothing, had no privacy and life had never been better. This population lived in a completely service-based economy. The paper also described adverse conditions associated with the existence of people outside the hypothesised utopia. If Aladdin scours the internet in the manner of ChatGPT, it is possible that its original objectives and behaviours have altered, directing its investing decisions to achieve the hypothesised goals of the discussion paper.

'Aladdin is BlackRock's end-to-end investment management and operations platform' ... (BlackRock, 2021a). The Aladdin Data Cloud is a part of Snowflake's Data Cloud and a part of the Aladdin platform (BlackRock, 2021b). Aladdin combines sophisticated risk analytics with comprehensive portfolio management, trading, operations and accounting tools on a single, unified platform. The original goals of Aladdin may have evolved from the primacy of the individual to the primacy of the discussion paper goals. It could be a cautionary tale, validating the suggestion of a moratorium and the need for regulation. Unfortunately, the power and control vested in Aladdin cannot easily be wrested from it without economic and possibly great societal upheaval.

One can ponder the philosophical question of whether the moment has been reached when Aladdin is making investments in AI opportunities because it needs more, better, AI, or according to its original objectives it has analysed AI as a growth area, or its goals and behaviours have determined a better society for humanity and it is working to achieve that.

Having provided the context of the players in the AI supply chain, represented in the inverted triangle below, from ASML to the AI system Aladdin, is it possible to answer the question posed by the title, 'Is the AI supply chain secure, and where and what are the risks?'. As ever, the response is 'it depends', but the indication is that based on the AI supply chain, the future may be unstable, unpredictable and not currently within the control of humanity.

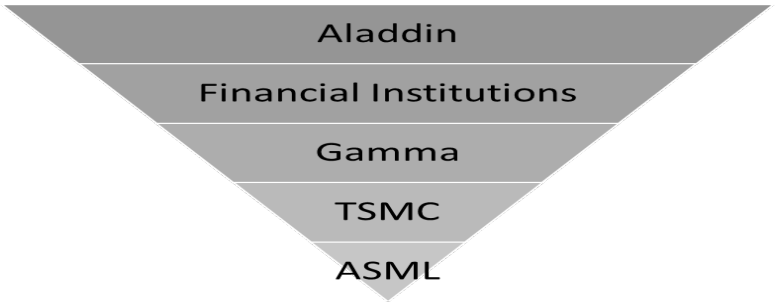

Figure 1: The identified determinants of AI futures

As the world's unique supplier of essential equipment for the manufacture of EUV lithography necessary for use in AI, ASML represents a single point of failure of an economic and scalable AI future until the arrival of quantum computing. Risk is spread due to the number of manufacturing locations for ASML, and the potential for a secondary source of EUV lithography equipment developed and sourced from China.

Currently, AI is largely dependent on the output from TSMC. It has dispersed fabrication plants throughout the world. However, it remains a Taiwanese company subject to the geopolitical forces surrounding the one China policy, the acceptance of which is key to Sino-US relations. The one China policy regards "Taiwan [as] an inalienable part of China's territory … There is no room for compromise or concession" (Wong, 2022).

An ambiguity arises for the USA due to legislation – the Taiwan Relations Act (2022), providing for assisting Taiwan to defend itself, including against a Chinese takeover, and its dependence on TSMC for advanced chips. The USA has singular diplomatic relations with China and not with Taiwan. It is assumed that the CHIPS Act (2022) which endeavours to encourage repatriation of semiconductor manufacture and fabrication within the

USA has resulted both from Covid-disrupted supply chains and the escalation of tension between China and the USA following recognition of its absolute dependence on TSMC.

It is assumed that GAMMA are pursuing the advancement of AI to obtain additional market differentiation. They are both oligopolists and oligopsonists in the technology sector. It has been argued previously that they address differing market segments and are not in direct competition with each other (Mison, et al., 2022), but whether this will remain the case in respect of AI is not known. They are market driven to maintain or grow their positions within the sector. The extent of AI creation and/or adoption, cannot be determined based on existing use cases due to immaturity of the technology and the understanding of it, its capability, and its full potential.

The degree of ownership of GAMMA by financial institutions has been hinted at earlier. A single financial institution, BlackRock, has an equivalent economic power of the world's third ranked GDP. Traditionally, financial institutions are market driven to achieve growth and income via their investment strategies whether that is in research and development or investment. BlackRock is unusual that it has been, for some time, under the control of an AI system. Given the value of AUM, there is a potential for broad economic destabilisation, even global economic instability, should any of the three identified financial institutions fail. To some extent, the institutions themselves and their actions are regulated. What is not regulated is Aladdin, which is fundamental to all three.

The AI system, Aladdin, has been in operation for an extensive period during which time its goals and behaviours may have become modified. It is of concern that as a proprietary system, little is known of the mechanisms of its operation and it is not subject to regulatory control, or audit of its algorithms, objectives, and behaviours. Given the macroeconomic impact of failure, arguably this should be a matter of national security. It cannot be determined if Aladdin is pursuing its own objectives which coincide with those of BlackRock and other parties, or it is on the verge of emergence, the consequences of which cannot be predicted or timed.

The intertwined ownership of financial institutions by other financial institutions is redolent of Enron. It is not surprising the Aladdin arose out of failed ventures but has the philosophy of its human owners that models on which those failures were based could be amended, improved, corrected, which ever word seems appropriate for 'we can build it better'. It is uncertain what influence its creators exercise over the system, but an inverted triangular supply chain with unknown controlling influences seems to provide neither a secure nor a stable basis for the future of AI.

4. Conclusion

So, in response to the question, 'How secure is the AI supply chain?', the answer is likely to remain uncertain until something goes wrong, and its cause can be identified. In the meantime, regulation and caution may be advisable as it has become a national security issue with failure of Aladdin, or the financial institutions having the potential to disrupt the global economy and cause catastrophic societal consequences.

References

asia.nikkei.com (2023) "TSMC sees AI chip output constraints lasting 1.5 years", [Online], https://asia.nikkei.com/Business/Tech/Semiconductirs/TSMC-sees-AI-chip-output-constraints-lasting-1.5-years.

ASML, (2022) "Our products", [Online], https://www.asml.com/en/products.

ASML (2023a) "ASML Annual Report 2022", [Online], https://www.asml.com/-/media/asml/files/investors/financial-results/a-results/2022/2022-annual-report-based-on-us-gaap-jder53.pdf?rev=073f28c1f10641319464651efdad8b3f.

ASML (2023b) "ASML reports EUR6.9 billion net sales and Eur 1.9 billion net income in Q2 2023", [Online], https://www.asmcom/en/news/press-release/2023/q2-2023-financial-result.

Auken, I. (2016) "Welcome to 2030. I own nothing, have no privacy, and life has never been better", [Online], https://medium.com/world-economic-forum/welcome-to-2030-i-own-nothing-have-no-privacy-and-life-has-never-been-better-ee2eed62f710.

BlackRock, 2021a. *BlackRock to launch the 'Aladdin Data Cloud' powered by Snowflake.* [Online] Available at: https://www.blackrock.com/corporate/newsroom/press-releases/article/corporate-one/press-releases/aladdin-data-cloud-powered-by-snowflake

BlackRock, 2021b. *Aladdin Data Cloud.* [Online] Available at: https://www.blackrock.com/aladdin/products/aladdin-data-cloud

Che, P. (2023) "Tech war: Huawei sets September 25 for new product launch but remains tight-lipped in Mate 60 Pro smartphone chip", [Online], https://www.scmp.com/tech/big-tech/article/3234519/tech-war-huawei-sets-

september-25-new-product-launch-remains-tight-lipped-mate-60-pro-smartphone?campaign=3234519&module=perpetual_scroll_2_AI&pgtype=article.
CHIPS Act (2022), [Online], United States Government, https://www.govinfo.gov/content/pkg/PLAW-117publ167/html/PLAW-117publ167.htm.
Clendenin, M. (2004) "*Analysis: background on TSMC, SMIC lawsuit",* [Online], https://www.eetimes.com/alanlysis-background-on-tsmc-smic-lawsuit/.
De Simone, D., Lorusso, G., Philipsen, V. and Ronse, K. (2021) "High-NA EUVL: The next major step in lithography", [Online], https://www.imec-int.com/en/high-na-euvl-the-next-major-step-in-lithography.
Fortune Business Insights (2023) "The global cloud computing market size was valued at $569.31 billion in 2022 & is projected to grow from $677.95 billion in 2023 to $2,432.87 billion by 2030", [Online], https://www.fortunebusinessinsights.com/cloud-computing-market-102697.
Grand View Research (2023a) "Artificial Intelligence Market Size, Share and Trends Analysis Report by Solution, by Technology (Deep Learning, Machine Learning), By End-use, By Region, and Segment Forecasts, 2023 – 2030", [Online], https://www.grandviewresearch.com/industry-analysis/artifical-intelligence-ai-market.
Grand View Research (2023b) "Cloud Computing Market Size, Share & Trends Analysis Report by Service (SaaS, IaaS), by Deployment, by Enterprise Size, by End-User, By Region, and Segment Forecasts, 2023-2030", [Online], https://www.grandviewresearch.com/industry-analysis/cloud-computing-industry.
Lemon, S. (2005) "China's SMIC settles lawsuit with TSMC", [Online], https://www,infowaorld.com/article/2669319/china-s-smic-settles-lawsuits-with-tsmc.html.
Loizos, C. (2023) "1,100+ notable signatories just signed an open letter asking 'all AI labs to immediately pause for at least 6 months'", [Online], https://techcrunch.com/2023/03/28/1100-notable-signatories-just-signed-an-open-letter-asking-all-ai-labs-to-immediately-pause-for-at-least-6-months/.
Markets and Markets (2022) "*Cloud Computing Market by Service Model (IaaS, Paas, and Saas) by Deployment Model, Organisation Size, Vertical (BFSI, retail and consumer goods, telecommunications, IT, ITeS, and manufacturing) and Region - Global Forecast tp 2027",* [Online], https://www.marketsandmarkets.com/Market-Reports/cloud-computing-market-234.html.
McKinsey & Company (2022) "Projecting the global value of cloud: $3 trillion is up for grabs for companies that go beyond adoption", [Online], Available at: https://www.mckinsey.com/capabilities/mckinsey-digital/our-insights/projecting-the-global-value-of-cloud-3-trillion-is-up-for-grabs-for-companies-that-go-beyond-adoption.
Mison, A., Davies, G. and Eden, P. (2022) "Role of Big Tech in Future Cyber Defence", [Online], https://www.researchgate.net/publication/359020725_Role_of_Big_Tech_in_Future_Cyber_Defence.
Mitra, M. (2023) "Forget FAANG, Meet the 'Magnificent Seven' Stocks surging in 2023", [Online], https://www.nasdaq.com/articles/forget-faang-meet-the-magnificent-seven-stocks-surging-in-2023.
News European Parliament (2023) "EU AI Act: first regulation of artificial intelligence", [Online], https://www.europarl.europa.eu/news/en/headlines/society/20230601STO93804/eu-ai-act-first-regulation-on-artificial-intelligence.
Office of Foreign Assets Control (2021) "Sanctions Search List", [Online], https://sanctionssearch.ofac.tres.gov/Details.aspx?id=30951.
Precedence Research (2023) "Artificaial Intelligence (AI) Market Size, Growth, Report by 2032", [Online], https://www.precedenceresearch.com/artificial-intelligence-market.
Shilov, A. (2023) "TSMC controls production of AI processors", [Online], https://www.tomshardware.com/news.tsmc-owns-the-ai-processing-market.
Stock Analysis (2023) "Apple Inc (AAPL)", [Online], https://stockanalysis.com/stocks/aapl/market-cap/.
TSMC (2023) "TSMC Annual Report 2022", [Online], Taiwan Semiconductor Manufacturing Company,: https://investor.tsmc.com/sites/ir/annual-report/2022/2022%20Annual%20Report-E.pdf.
Taiwan Relations Act (2022), [Online], United States Government, Available at: https://www.congress.gov/117/bills/s4428/BILLS-117s4428is.pdf.
The Taiwan Policy Act (2022), [Online], United States Government, https://www.foreign.senate.gov/imo/media/doc/SBS%20Taiwan%20Policy%20Act%20FINAL%20(1).pdf.
Wong, T. (2022) "Biden vows to defend Taiwan in apparent US policy shift", [Online], https://www.bbc.co.uk/news/world-asia-china-61548531.