Representation of the People Bill

Written evidence submitted by the Centre for Finance & Security at RUSI

Point of contact: Eliza Lockhart, CFS Research Fellow, ElizaL@rusi.org

At the Centre for Finance and Security at the Royal United Services Institute (RUSI), we examine how finance is used to destabilise democracies around the world. We have advised domestic and international public and private partners on a complex spectrum of foreign financial interference threats, including on deployment to Romania, Moldova, Armenia and Ukraine. CFS has given evidence on the financial dimension of political interference at the Council of Europe and the European Parliament, as well as at a recent meeting of the Joint Committee on the National Security Strategy (JCNSS). Further details of the CFS programme and activities can be found at the end of this evidence.

Our current research project on **Cryptocurrencies in UK Politics**, funded by the Joseph Rowntree Reform Trust, combines CFS's expertise in financial regulation, fintech, national security and electoral law to examine the risk of opaque, foreign or malign finance entering UK politics via cryptocurrencies. We would welcome the opportunity to provide further written or oral evidence to the Committee on these issues to enable a deeper understanding of these critical legal, political and security risks.

I. Cryptocurrencies as a political money laundering accelerant

Cryptocurrency donations to UK political parties present an urgent and under-addressed challenge to the UK's electoral integrity and, by extension, to its national security. CFS's work in financial foreign interference in domestic and international politics has revealed that: 'foreign powers have learned that submitting a well-timed donation or funding an effective influence campaign can achieve what tanks and missiles cannot'. If malign actors can covertly finance political campaigns, or distort the political process through opaque financial channels, the legitimacy of democratic governance is undermined. This, in turn, weakens public confidence in government institutions and exposes the UK to hostile influence.

The Representation of the People Bill contains important proposals to strengthen transparency around political donations and prevent foreign actors from funding domestic politics. However, the Bill does not mention cryptocurrencies. Instead, it treats cryptocurrency donations as equivalent to fiat contributions and expects the same tracing and compliance rules to apply. This leaves a critical gap in our foreign interference defences as the pseudonymous, cross-border and decentralised features of crypto enable it to be used as a political money laundering accelerant, which cannot be effectively monitored or regulated under frameworks designed for fiat currencies. This has already been acknowledged by the government, which has tasked the Financial Conduct Authority (FCA) with designing a new cryptoasset regime to regulate crypto firms that provide financial services in the UK, to come into force in October 2027.

The Royal United Services Institute
61 Whitehall, London
SW1A 2ET
United Kingdom

+44 (0)207 747 2600
enquiries@rusi.org
rusi.org
@RUSI_org

II. Crypto Ban or Moratorium?

It is due to these security concerns that some are advocating for a complete ban on crypto donations. However, our research indicates that a ban offers less protection than it appears and that a moratorium, to be lifted once an appropriate regulatory regime has been designed, is the best way to futureproof our political finance system against undue influence and foreign inference. This is for three key reasons:

1. **Legal Risks**
   It is commonly argued that a ban is needed to protect our system against a future, pro-crypto government because a ban is more permanent than a moratorium. But no Parliament can effectively bind its successor. A future government could reverse a ban through primary legislation just as it could lift a moratorium through affirmative resolution. However, the process to lift a moratorium can include various strengthening procedures, such as the approval of a regulatory regime by the Electoral Commission, that would make the process more robust than repealing a ban via primary statute.

2. **Political Risks**
   Markets do not stand still. As crypto adoption grows, and other regulatory regimes are implemented – such as the FCA's forthcoming cryptoasset regime – a blanket ban is likely to erode under political and commercial pressure. The strategic choice we must make is whether to use this opportunity to design safeguards now, while the risks are still emerging, or leave the shape of the system to a future government at a potentially more geopolitically unstable time.

   A moratorium would pause our immediate exposure to critical security risks while creating a defined window before the next election to build a credible verification system through regulated intermediaries and strengthen the capacity of regulators and law enforcement agencies to investigate these activities. Once a functioning regulatory architecture exists, dismantling it becomes far harder than overturning a prohibition that never built the underlying safeguards.

   Moreover, with the growing influence of technology and fintech platforms in international politics, we are seeing the increased weaponisation of free speech and political participation arguments to push back against legitimate attempts to regulate political finance. It is much easier to paint a blanket ban, which provides no roadmap for the future, as stifling technological innovation or as an act of politically motivated censorship, than a moratorium that provides the space to consult and design a robust and evidenced-based regulatory regime.

3. **Security Risks**
   Finally, and most importantly, a ban would create a false sense of security because it does nothing to prevent the risks from crypto being moved upstream or offshore. A ban only deals with the 'direct' use of crypto, where a political party or candidate receives a donation in cryptocurrency.

The Royal United Services Institute
61 Whitehall, London
SW1A 2ET
United Kingdom

+44 (0)207 747 2600
enquiries@rusi.org
rusi.org
@RUSI_org

The more significant and underestimated risk is the 'indirect' use of crypto. This refers to the use of crypto earlier in the transaction history of a donation to obscure the fund's origin – essentially, it is the use of crypto to make an illegal or foreign donation appear to come from a permissible donor.

At a 13 January 2026 Foreign Affairs Committee evidence session, the Electoral Commission's Chief Executive, Vijay Rangarajan, indicated that this is already happening: 'We have seen, in some of our investigations, money flowing internationally through crypto exchanges and ending up in British bank accounts'. Regulators and law enforcement agencies do not currently have the specialist skills or technical resources to police crypto-to-fiat laundering effectively. As Rangarajan commented at that same Foreign Affairs Committee session: '[crypto] could in the end be quite a major part of the financial system. The issue we see is that it is very hard to know through some of the crypto providers who the ultimate donor is. As a mechanism to obfuscate where the money is coming from, crypto can be very good'.

The Bill's proposed control of political donation safeguards, including the donation risk assessment, does not contemplate the complex capacities required to identify and mitigate the upstream use of crypto. If a blanket ban is implemented, with no accompanying timeline to design a comprehensive regulatory regime and increase enforcement capacity, direct risks would be mitigated but the much more insidious risks from the indirect use of crypto will continue to evolve untouched. This is why CFS Director Tom Keatinge, at a 12 January 2026 JCNSS evidence session said: 'a ban risks missing the wood for the trees … What we need is a moratorium until such time as we are sure that we have the right checks and balances in place to deal with the incremental risk that comes from the inclusion of cryptocurrency [in politics]'.

III. Conclusion

Legislative opportunities to strengthen political finance regulation are rare and this one has come at a critical time. The UK is increasingly the target of malign financial interference by foreign state and private-sector actors intent on disrupting and undermining democratic decision making. Therefore, there is a narrowing window of opportunity to strengthen defences against this threat to our sovereignty and stability.

With the FCA currently designing a regulatory regime for crypto firms that provide financial services in the UK, now is the perfect time to prepare a complementary regime for the unique and complex security risks involved in the direct and indirect use of crypto in political finance. A moratorium would pause our current risk exposure and provide the space to create this robust regulatory framework, which in turn would provide the impetus to increase the investigative capacities of the relevant regulators and law enforcement agencies. This is not an impossible task, on the contrary, it is an imperative if we are to safeguard our democracy against escalating foreign interference threats.

The Royal United Services Institute
61 Whitehall, London
SW1A 2ET
United Kingdom

+44 (0)207 747 2600
enquiries@rusi.org
rusi.org
@RUSI_org

IV. About CFS

Since its formation in 2014, CFS has focused on matters at the intersection of finance and security. CFS uses its evidence-based research and convening power to support policymakers, operational agencies and the private sector across the globe, as well as undertaking extensive engagement with multilateral bodies. CFS conducts work across a range of topics relevant to the UK's national security and foreign financial interference, including the development and implementation of anti-financial crime policies and how finance is used to destabilise democracies around the world. Our current project on Cryptocurrencies in UK Politics combines our expertise in financial regulation, fintech, national security and electoral law to examine the risk of opaque, foreign or malign finance entering UK politics via crypto.

Other CFS projects examine:

- How cryptocurrencies have fundamentally changed the ways in which criminals, terrorists and hostile states operate and the need for policymakers, regulators, law enforcement and the private sector to keep pace with developments to understand the security risks and seek mitigations.
- The financial dimension of state threats (what we term 'active financial measures'), including building stronger responses to counter terrorist financing, the growing threat of Russian sabotage attacks, and the malign use of finance to disrupt elections, create undue political influence and undermine democratic decision-making.
- The intersection of illicit finance and serious and organised crime, for example, the national security implications of the online fraud epidemic and the role of money mules, the effectiveness of sanctions regimes, and the threat posed to the UK by Chinese and Russian professional money laundering networks.

This submission is made by CFS at RUSI and it represents the views of the research team members who have contributed their expertise as relates to the themes covered by the Bill. It does not represent the views of RUSI itself.

The Royal United Services Institute
61 Whitehall, London
SW1A 2ET
United Kingdom

+44 (0)207 747 2600
enquiries@rusi.org
rusi.org
@RUSI_org