Decentralized Open Network Services for a Resillient Economy and Free Society

Christian Grothoff
Free Secure Network Systems Group
Technische Universität München
Email: grothoff@net.in.tum.de

***Abstract*—Starting from a pessimistic perspective on the global economic future and current technological trends, this position paper derives the need for technologies to build a new open platform for secure networking that liberates users from the client-server paradigm and its hidden costs. We then sketch some of the major challenges and possible research directions towards reaching this goal.**

I. What is changing?

The International Energy Agency (IEA)'s World Energy Outlook 2010 says production of conventional crude oil peaked in 2006 at 70 million barrels per day and is expected to stay on a plateau for a few years until its inevitable decline. The resulting market turmoil, which is not limited to oil but also impacts other resources and currencies, can be expected to continue and worsen. We predict a destruction of global markets resulting in a relocalization of most economic activity.

Data-driven businesses, being more independent of transport and raw materials, will be the exception to the general force towards localization and continue to grow, resulting in a continued reduction in vendor diversity. At the same time, optimizing the transport of people and goods using network-based platforms will become critical for cost control, paving the way for the adaptation of network-based logistics-support applications by individual citizens. A lack of competition, the existing technical ability to control user access to hardware [1] and commercial incentives set the stage for most users loosing complete control over their systems and lifes. This threatens not only the freedoms of citizens but also limits the ability of cooperations to be profitable or governments to rule should they allow themselves to become dependent on closed platforms.

Energy consumption will continue to be a concern for battery-operated devices; for power-line supplied devices the possibility of interruptions in the energy supply due to resource shortages or supply chain problems [2] is expected to be a more serious issue.

II. What is our vision?

We envision a system based on open standards and free (as in freedom [3]) software and hardware that provides a range of completely decentralized distributed services. Given the importance of these services to daily life, no party should be able to monitor or exercise control over transactions it is not involved in. Furthermore, proper economic incentives (ideally without the ability to monitor or control) should be available for third parties that facilitate others. The system should enable users to control their own data, including access control, repudiation and persistence. Decentralization should be used to address the failure of individual systems and not be a burden to performance, scalability or usability. Communication in the system is envisioned to be diverse, using both short-range [4] and medium-distance wireless technologies [5] in concert with existing IP-based networks. Implementations should select communication mechanisms based on availability, resource constraints, cost and quality of service.

The envisioned system uses an extensible, standards-based open platform as the foundation for service development. Sandboxing is used to isolate services and the platform should provide strict bounds on the impact of malicious software or operators. Services are able to evolve without compromising active transactions, voiding persistence guarantees or requiring developers to maintain a growing body of code for legacy compatibility.

Specific benefits of the envisioned system are tied to the availablilty of the respective specific service. Moving existing legacy services for communication or collaboration to such a platform would have benefits in terms of cost, security and privacy; more significant benefits would come from new services, especially in the areas of decentralized markets [6], peer-assisted logistics and cooperative event signalling.

The openness of the platform would ensure competition, cost-effectiveness and user freedom; combined with decentralized operation, the system should be robust to external pressures. By having participants act not as clients and servers but as peers, the system becomes more adaptive: currently, virtualization enables server operators to migrate services to data centers with better availability or locality [7]; in the future, services could migrate all the way to the user's device(s). Caching static content is a well-known optimization even for embedded systems [8]. Recently, techniques for predictive caching for phones with variable connectivity have been proposed [9]. Clearly, moving from caching static content to migrating dynamic services would be another major step forward. Furthermore, instead of relying on an Internet service provider (ISP) or mobile network operator hierarchy for connectivity, the network could often route cooperatively. Such cooperative action would improve robustness, reduce costs [10] and eliminate control problems.

III. What are the challenges?

One challenge will be how to address legitimate state control desires, especially those that would arise with the integration of financial services into fully decentralized systems, such as taxation or mechanisms against money laundering. Peer-to-Peer markets seem to be just as incompatible with enforced taxation as censorship-resistence [11] is incompatible with copyright enforcement.

On the technical side, the main challenge is making it *easy* to develop fully-decentralized secure services. Only if the architecture (including design, engineering principles, platform and tool-support, validation mechanisms, etc.) makes it easy to develop and evolve services there is hope that those services can provide the necessary level of security. Existing methodologies for the development of parallel, distributed or even decentralized applications rarely result in the timely development of correct and secure implementations.

Finally, for a decentralized system to be widely adopted, it must not suffer from serious drawbacks in comparisson to centralized competitors. Resource consumption and performance in general are obvious areas of concern, especially for certain problem domains, such as search. An even bigger challenge is usability with respect to installation and system maintenance. Here, centralized solutions have the advantage of paid (and "trusted") engineers; we need to develop the ability to avoid individual responsibility for system maintenance without having maintainers that could assume control over private data or impact system availability.

IV. What could be a solution?

The productive development of decentralized systems can be accelerated by providing developers with appropriate languages that facilitate parallel composition. Approaches based on systems that interact using data streams currently seem to be the most promising, combining modular design, development and testing with natural, scaleable and powerful composition while being suitable for distribution using networks [12]. Existing designs often focus on parallel and distributed settings and need to be extended to work for decentralized systems that have additional requirements, especially in terms of fault-tolerance and security.

Debugging is another major contributor to low productivity in the development of distributed systems. However, since debugging often largely consists of repetitive application of the same basic techniques [13], [14] to narrow down the problem, it should be possible to develop an expert system that automates this large part of the debugging process [15]. Such an automated debugger, providing comprehensive diagnostics, would also be a first step towards maintenance-free distributed systems.

Finally, most of the freedoms of free software and the possible security advantages are currently meaningless to most users since they are unable to read or modify software. However, giving users control over their data implies that they should not have to trust the developer of a service. Having functional specifications that capture key data flow properties and can on the one hand be converted to understandable human-readable descriptions (for example, "Your birthday will be made known to your friends.") and on the other hand be used to validate relevant properties of the executable details (for example, this value is never exposed in plaintext beyond this set of users) would dramatically reduce the scope of a user's trust base.

V. Conclusion

When single institutions are too big to ~~fail~~ bail and too powerful to control, decentralization is a key strategy for maintaining stability. The philosophical ideas behind the vision presented in this position paper are widely appreciated [16], [17]; however, decentralized approaches must address a range of performance, usability and security challenges in order to compete with centralized solutions *prior* to the eventual systemic failure of a centralized monoculture.

References

[1] F. von Lohmann, "Lift the hood, go to jail?" netWorker, vol. 13, pp. 16–17, September 2009.

[2] S. Weinberger, "Powerless in gaza," IEEE Spectr., vol. 46, pp. 36–41, December 2009.

[3] R. M. Stallman, Free Software, Free Society: Selected Essays of Richard M. Stallman, 2nd ed., J. Gay, Ed. GNU Press, 2004.

[4] S. Farahani, ZigBee Wireless Networks and Transceivers. Newton, MA, USA: Newnes, 2008.

[5] "Ieee standard for information technology-telecommunications and information exchange between systems-local and metropolitan area networks-specific requirements - part 11: Wireless lan medium access control (mac) and physical layer (phy) specifications," IEEE Std 802.11-2007 (Revision of IEEE Std 802.11-1999), pp. C1–1184, 12 2007.

[6] R. Brunner and F. Freitag, "Elaborating a decentralized market information system," in Proceedings of the 2007 OTM confederated international conference on On the move to meaningful internet systems - Volume Part I, ser. OTM'07. Berlin, Heidelberg: Springer-Verlag, 2007, pp. 245–254.

[7] M. Armbrust, A. Fox, R. Griffith, A. D. Joseph, R. H. Katz, A. Konwinski, G. Lee, D. A. Patterson, A. Rabkin, I. Stoica, and M. Zaharia, "Above the clouds: A berkeley view of cloud computing," EECS Department, University of California, Berkeley, Tech. Rep. UCB/EECS-2009-28, Feb 2009.

[8] R. Shinkuma, S. Jain, and R. Yates, in 2009 IEEE 20th International Symposium on Personal, Indoor and Mobile Radio Communications.

[9] P. Lungaro, Z. Segall, and J. Zander, "Predictive and context-aware multimedia content delivery for future cellular networks," in Vehicular Technology Conference (VTC 2010-Spring), 2010 IEEE 71st, May 2010, pp. 1 –5.

[10] "Open peering initiative," http://www.openpeering.nl/, January 2011.

[11] G. Perng, L. Tong, and C. Wang, "Censorship resistance revisited," in Information Hiding, 2005, pp. 62–76.

[12] K. C. Bader, T. Eißler, N. Evans, C. GauthierDickey, C. Grothoff, K. Grothoff, H. Meier, C. Ritzdorf, and M. J. Rutherford, "Dup: A distributed stream processing language," in Proceedings of the IFIP International Conference on Network and Parallel Computing (NPC 2010), ser. LNCS 6289, 2010, pp. 232–246.

[13] C. E. McDowell and D. P. Helmbold, "Debugging concurrent programs," ACM Comput. Surv., vol. 21, pp. 593–622, December 1989.

[14] M. Weiser, "Programmers use slices when debugging," Commun. ACM, vol. 25, pp. 446–452, July 1982.

[15] H. Agrawal, R. A. Demillo, and E. H. Spafford, "Debugging with dynamic slicing and backtracking," Software: Practice and Experience, vol. 23, pp. 589–616, 1993.

[16] E. Moglen, "Freedom in the cloud," February 2010. [Online]. Available: http://www.youtube.com/watch?v=QOEMv0S8AcA

[17] K. Wuestefeld, "Sovereign computing," November 2004. [Online]. Available: http://www.advogato.org/article/808.html