Is a private blockchain more secure due to its private nature?

A private blockchain seems at first glance to be more secure, since one might ask: how can you hack a private blockchain which is "locked away" and only accessible for authorized participants?

Ho ver, this assumption does not take into considerations that employees including suppliers, consultants and contractors are the top source of security incidents[3] and also that hackers have already demonstrated the capability to successfully intrude networks (see for instance the "Cloud Hopper Attacks"[4]).

Would it not be better to rely on a public blockchain and its globally distributed community, where different parties with different backgrounds, experiences, and expertise are using and testing the public blockchain on a day-to-day basis and announcing and fixing security weaknesses in case they detect one?

In addition, the source code of most public blockchains is publicly available and can be reviewed by anybody. This concept of open source software is popular and widely adopted by a vast amount of applications but as well as by operating systems (e.g. Linux or Android). A main advantage of open source is that everybody is invited to inspect the code for understanding and verification of functionality and security. Thereby, no faith is required in a company or sub contractor that they correctly and timely implement or fix security critical functionality. To compare it to the previously mentioned analogy of the internet vs. intranets, more innovation can take place on public blockchains as they are open and accessible for anyone to tinker with.

What type of blockchain will most likely be used in the long run?

With recent developments in encryption and privacy technologies (e.g. zero knowledge proof techniques), public blockchains are able to overcome some of the concerns many companies often have, especially when it comes to privacy and confidentiality. In addition, so-called layer 2 scaling technologies for blockchains, such as Plasma (Marigold on Tezos) or Lightning foster faster and more scalable public blockchains. As a result, common reasons to implement a private blockchain are vanishing as recent tech developments make them irrelevant.

Using a public blockchain instead of a private blockchain can also help companies to save costs since they are not responsible for running and maintaining the entire blockchain network and can instead focus on the integration of their use cases into the blockchain and further innovation. Also, the difference of blockchain types between open and closed will disappear due to some of the technological improvements mentioned above, but this type definition will be still valid to characterize use cases.

Furthermore, we predict that public blockchains and their usage will go through a similar development cycle like the internet. In the past, at a very early stage of the internet, companies were running their own networks (Intranets) with dozens of servers hosting their required applications. Today, a lot of companies obtain their applications directly from the internet ("cloud") and thus costs for running and maintaining internal networks and application systems are replaced by paying the access to the internet via a local internet provider.

Finally, blockchains will only succeed if they create value. Much like the internet, value from blockchains relies on connectivity and network effects, which accrue on public chains and are fragmented on private ones. For example, tokenized assets such as digital stocks or bonds cannot pass between private chains, meaning that to own a digital security tokenized on a private chain, one would have to be a member of the consortium governing the private chain - given the size and scale of private and public capital markets, it would be virtually impossible to bring all participants onto one private chain network, and value would be destroyed because of fragmentation rather than created. With public chains, more market participants can engage, enabling greater connectivity and exchange of value, thereby providing additional value to all participants. As public chain technology continues to advance, the fundamentally superior economics of public chains will inevitably lead to an obsolescence of private chains and a robust digital economy based on public blockchains.

[3] https://www.pwc.com/us/en/services/consulting/cybersecurity/library/information-security-survey.html
[4] https://www.schneier.com/blog/archives/2019/07/details_of_the_2.html